Asia Pacific Journal of Information Systems
Vol. 31 No. 3 (September 2021), 257-276

ISSN 2288-5404 (Print) / ISSN 2288-6818 (Online)
https://doi.org/10.14329/apjis.2021.31.3.257

Mobile Payment Use in Light of Privacy Protection and Provider's Market Control

Mohammad Bakhsh[a,*], Hyein Jeong[b], Lingyu Zhao[c], One-Ki Daniel Lee[d]

[a] *Ph.D. Candidate, University of Massachusetts Boston, USA*
[b] *Ph.D. Candidate, University of Massachusetts Boston, USA*
[c] *Ph.D. Candidate, University of Massachusetts Boston, USA*
[d] *Associate Professor, University of Massachusetts Boston, USA*

A B S T R A C T

This study investigates the factors that facilitate or hinder people to use mobile payment, especially drawing upon the theoretical perspectives on individual's privacy protection motivation and perceived market condition. Survey data (n = 200) were collected through a web-based platform and used to test a theoretical model. The results show that one's privacy protection power is formed by various individual and technological factors (i.e., perceived data exposure, self-efficacy, and response efficacy), and in turn it determines his/her intention to use mobile payment. Moreover, the relationship between privacy protection power and mobile payment use is conditional on the perceived market control by the service provider – with a perception of the high level of provider's market control, one uses mobile payment regardless of his/her privacy protection power, while under the low level of provider's market control, the decision depends on the degree of privacy protection power. The findings would help our understanding of why some people are more susceptible to mobile payment and others are not.

Keywords: Mobile Payment, Privacy Protection, Data Exposure, Market Control, Personal Data

Ⅰ. Introduction

During the last several years, major technology companies such as Apple, Samsung, and Amazon have competitively expanded their business into FinTech, especially mobile payment services. FinTech, as its name implies, is an integration of financial and technological services (Kim et al., 2010). This new way of making end-user financial transactions has great potential due to today's pervasive usage of mobile devices such as smartphones in our daily life. Regardless of its great potential and benefits like improving transaction speed and management and reducing financial fraud, however, some people

*Corresponding Author. E-mail: mohammad.bakhsh001@umb.edu

still hesitate to adopt and use mobile payment services for various reasons (Ernst and Young, 2019; Kim et al., 2010). However, what makes certain people more susceptible or open to the use of mobile payment services than others have been ill-understood in the literature, which is the motivation of this study.

Due to the popularity of smartphones flowing in the market, it seems reasonable to posit that more people are willing to use mobile payment services. However, some researchers have argued that the high mobility of smartphones is not a strong determinant of mobile payment use (Kock, 2015). Similarly, an industry report about payment methods of online shoppers in 2017 reveals that mobile payment only has 14% of the market share while credit card payment has the largest one (42%) (Statista, 2017). Hence, why people hesitate to use mobile payment regardless of its significant benefits will be a salient question to both academics and practitioners.

Privacy concern has been frequently recognized as a significant barrier in consumer electronic commerce (Tsai et al., 2011; Van Slyke et al., 2006). In the context of mobile payment, Yang et al. (2012) has also found that privacy concern indirectly affects people's intention of mobile payment use through trust. Since mobile payment transactions usually involve various personal information, many people may have concerns about leaking their personal information to unforeseen parties. Hence, such privacy concerns should be further scrutinized regarding mobile payment use.

In addition, several researchers have highlighted the role of mobile payment service providers regarding individual's mobile payment use (Arvidsson, 2014; Lowry et al., 2016; Yang et al., 2012). For example, Chandra et al. (2010) have investigated the characteristics of mobile service providers and showed that their reputation and structural assurance have positive effects on consumer trust in mobile payment and thus indirectly affect an individual's mobile payment adoption. Hence, it will be important to consider the role of service providers in mobile payment user behaviors as an environmental factor. However, extant studies have seldom examined how this environmental factor interplays with the privacy concerns of users (as an individual factor) in shaping individual users' mobile payment use behavior. Particularly, this study focuses on the degree of service provider's market control as a salient environmental factor. Within a high degree of service provider's control on market, individuals may feel limited in their choices for their mobile payment use. Thus, the perceived provider market control should also affect the mobile payment use of individuals. Moreover, like other socio-technical systems, mobile payment will also involve technological factors that affect its user behaviors (Kankanhalli et al., 2011).

To investigate the impacts of the individual, environmental, and technological factors on mobile payment use, this study reviews the relevant theoretical perspectives on individual data protection (for the technological and individual factors) and provider's market control (for the environmental factor). Drawing upon the theoretical perspective on an individual's protection motivation (Boss et al., 2015), particularly, we investigate an individual's coping appraisal for personal data protection in terms of personal data exposure (as a potential threat) and protection power. In addition, drawing upon the market oligopoly and customer choice perspective, we investigate how users' perception of provider's market control affects their appraisal process for mobile payment service use. Through this study, therefore, we aim to answer the following questions:

RQ1: What is the role of an individual's perceived power

for privacy protection in his/her use of mobile payment services?

RQ2: How does the perceived mobile payment service environment, especially the degree of provider's market control, affect the role of privacy protection power in mobile payment use?

To have a better understanding of the phenomena, we began by interviewing several active and potential users of mobile payment services, as a focus group. Based on the findings from the focus group analysis and a literature review on the relevant topics such as privacy and market choice, a theoretical model was proposed. A survey was conducted to test the proposed model. The findings of this research would help both academics and practitioners better understand how technological, individual, and environmental factors shape one's decision to use mobile payment services.

Ⅱ. Theoretical Backgrounds

This study is grounded on the following literature areas: 1) mobile payment, 2) privacy and protection motivation, and 3) provider control and cognitive dissonance.

2.1. Mobile Payment

As a form of FinTech services, mobile payment is an innovative payment method between payers and receivers via electronic devices. Compared to the conventional payment methods (e.g., using cash, check, debit, or credit card), mobile payment provides various benefits likes fast and safe transaction and convenience in management to both payers and receivers (Eze et al., 2008; Zhou, 2013). In addition to these benefits, the high volume of mobile phones and handheld devices drives the development of mobile payment (Eze et al., 2008). The prevailing applications of mobile payment include Google Pay, Apple Pay, Samsung pay, Alipay, and WeChat Pay, which are developed and serviced mostly by software companies. In addition, online payments and money transfers are frequently used through mobile payment brokers like PayPal and TransferWise. Crowdfunding, peer-to-peer lending, and stock trading are also often supported by mobile payment services. Due to this emergence of mobile payment services in various areas, recently mobile payment has drowned researcher's great attention (Chen, 2008; Slade et al., 2015; Zhou, 2013).

Over the past few years, researchers have investigated serval drivers and inhibitors about the mobile payment of consumers. For example, Choi et al. (2019) used social representation to investigate FinTech and payment from the perspective of financial authorities, financial companies, and IT firms. Moon (2020) also explored the enabler factors for the adoption of mobile banking from economic, psychological, and social perspectives. Moreover, the role of trust has been frequently investigated as a driver of consumers' use of mobile payment for their e-commerce transactions (Chandra et al., 2010; Gao and Waechter, 2017). They have attested that trust is playing a vital role and is positively associated with mobile payment intention to use. In addition, earlier research conducted by Kim et al. (2010) found that perceived ease of use and perceived usefulness are strong drivers of mobile payment intention to use. The combination of behavioral beliefs, social influences, and personal traits are also very important drivers from the point of view of customers. In recent years, convenience has been discussed to help accel-

erate the speed of mobile payment use for customers (Yang et al., 2012). On the other hand, some inhibiting factors have also been discussed. In particular, Johnson et al. (2018) examined the negative effect of a privacy risk as one of the limitations to prevent the expansion of mobile payment services. Even though these prior studies have helped researchers and practitioners recognize the development of mobile payment, however, the intermediating and conditional effects regarding the mobile payment user behavior have barely been studied yet.[1)]

2.2. Privacy and Protection Motivation

According to Anderson (2001), privacy can be defined as the "ability and/or right to protect our personal secrets, the ability and/or right to prevent invading our personal space" (p. 612). As one's ability or right, privacy is relatively evaluated. Therefore, people have a different level of cognition and treatment which is the foundation of an individual's privacy protection. For example, when one uses mobile payment for online shopping, one's private information can be exposed to other parties. To avoid this situation and improve their privacy protection, some people use technologies that enable them to protect their data and privacy (Senicar et al., 2003). Floyd et al. (2000) define this protection motivation as "any threat for which there is an effective recommended response that can be carried out by the individual" (p. 409).

Protection motivation theory (PMT) is a leading theoretical foundation used in privacy research (Boss et al., 2015). PMT was developed by Rogers (1975) to describe how individuals understand fear, cope with it, and are motivated to react in a self-protective way. Boss et al. (2015) applied this theoretical perspective on information systems and security. The main components of PMT are fear appeal, threat appraisal, coping appraisal, protection motivation, and security-related behaviors. The PMT process starts with a fear appeal, a stimulus that triggers both the threat-appraisal and coping-appraisal processes. In the threat-appraisal process, a protection motivation response occurs when the threat is greater than the rewards. In the coping-appraisal process, a protection motivation response occurs when response efficacy and self-efficacy outweigh the response costs (Boss et al., 2015).

This study adopts the theoretical perspective of PMT and investigates perceived data exposure, self-efficacy, and response efficacy as the drivers of an individual's appraisal toward mobile payment use. Perceived data exposure can be defined as the users' recognition of the wide usage of their personal data (Liang and Xue, 2009). Under PMT, perceived data exposure relates to threat appraisal – the process when threat or fear are first generated in which it inspires protection motivation to be weighted. On the other side, self-efficacy and response efficacy relate to PMT's coping appraisal when one outweighs the response costs for engaging in the protection motivation. According to Floyd et al. (2000), response efficacy can be defined as "the degree to which a person believes that the recommended response will be effective" while self-efficacy refers to "the degree to which an individual believes that he or she has the capability to perform what is required to avert the threat" (p. 411).

Protection motivation assesses one's intention to protect oneself from the danger raised in the fear appeal (Liang and Xue, 2009). Choi et al. (2019)'s

1) A couple of researchers have discussed the conditional effects of only some personal demographics such as age (Liébana-Cabanillas et al., 2014) and gender differences (Jaradat and Faqih, 2014).

study on FinTech used the term self-protection. Choi and Jung (2019) also investigated the role of privacy cynicism in online users' privacy behaviors toward privacy protection. Similar to other online payments, the privacy concerns in mobile payment (i.e., fear) will include a collection of personal information, unauthorized secondary use of personal information, errors in personal information, and improper access to personal information (Tsai et al., 2011). Hence, mobile payment users also try to protect themselves from these potential fears of losing privacy. To investigate the degree to which an individual feels how much he/she can protect personal data, this study conceptualizes perceived privacy protection power (PPP) as one's belief in the power to safeguard personal data against collection, access, usage of personal information by service providers, to refuse the consent form of collecting personal data, and to protect personal data from being linked and used across different platforms (Hoffmann et al., 2016). Unlike prior studies investigating the intention to protect personal information (e.g., Liang and Xue, 2009), this study focuses on an individual's perceived power of privacy protection as an important determinant of mobile payment use.

2.3. Provider's Market Control

Market conditions significantly affect consumer behaviors as an environmental factor in general, and thus will do the same in the context of mobile payment services (Ernst and Young, 2019; Hasan et al., 2019; R and Rathi, 2019). For this environmental factor, this study focuses on the degree of provider's market control. Provider control refers to that one or few product or service provider has the power to control the market. The high-level provider control of the mobile payment market occurs when a few large companies or agencies collect and systematically analyze large datasets for resale or other for-profit activities (Avital et al., 2007). However, studies on the impact of provider control as a factor on the use of new technologies are very limited.

Hasan et al. (2019), for example, investigated the environment of market and information opaqueness in their study of mobile payment adoption from the bottom-of-the-pyramid (BOP) context, which refers to the socio-economic development that is still at a very beginning stage (Prahalad and Hart, 2002). They conclude that provider control and information opaqueness hinder mobile payment adoption in the BOP context, which means that under a high provider control environment, people are less likely to adopt mobile payment services. They also discussed other factors, such as a corporation's reputation, integrity, trust, reliability, and recognition, as the ways that may increase adoption of mobile payment in the BOP context. However, extant studies failed to explain why people still adopt mobile payment in a highly-controlled market like China (Ernst and Young, 2019; Hoffmann et al., 2016; R and Rathi, 2019).[2] Hence, we need to further investigate the role of provider's market control in shaping an individual's mobile payment use behavior.

2.4. Cognitive Dissonance

Cognitive dissonance theory states that people generally seek consistency in their beliefs and behaviors, and when one faces two contradictory beliefs at the same time, or when one engages in behavior that

2) China, which scored first on the global FinTech mobile payment adoption index in 2019 (Ernst and Young, 2019), has only two dominant mobile payment platforms, WeChat Pay and Alipay, in which they hold about 92% of the market share in the country (R and Rathi, 2019).

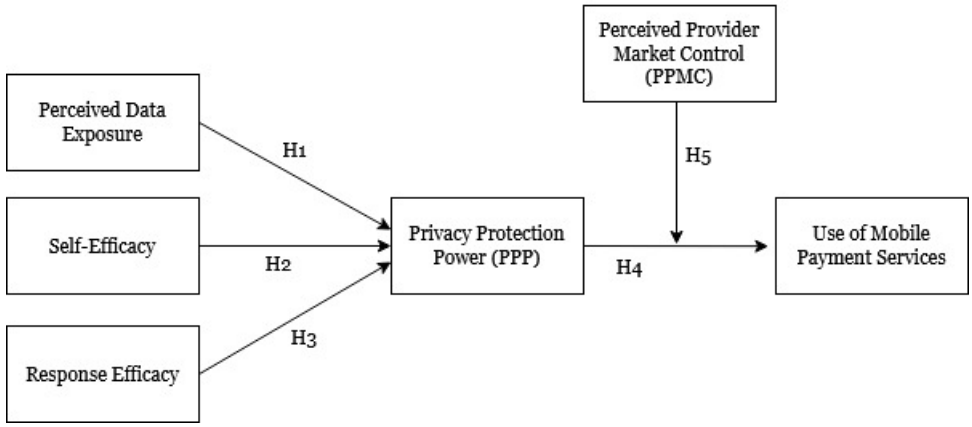
contradicts with one's beliefs, one feels a sense of discomfort – known as cognitive dissonance. To eliminate this dissonance condition and bring back balance, one has three options: changing the belief(s), changing the behavior, or trivializing the inconsistency (Epstein and Kopylov, 2005). In our mobile payment case, when a user has a high privacy concern but doesn't act to generate enough corresponding level of privacy protection behavior, this apparent discrepancy between attitudes and actual behavior creates a cognitive dissonance, which has been discussed as "privacy paradox." Hoffmann et al. (2016) introduce the term "privacy cynicism" to explain the situation when individuals make extensive use of online services while avoiding privacy protection behavior despite their significant privacy concerns. It allows fearful, low-skilled users to take advantage of the desired online services without cognitive dissonance since privacy protection behavior can be rationalized as useless or ineffective. We believe such privacy paradox or cynicism applies to the mobile payment use behaviors especially when they recognize limited choices to them. According to Hoffmann et al. (2016), privacy cynicism corresponds with four recurring elements: uncertainty and insecurity, loss of control/ powerlessness, mistrust, and resignation. Among the four elements, this study focuses on the loss of control/ powerlessness as the most relevant environmental intervention for individuals' cognition of their privacy protection power in mobile payment use.

In the other case of the privacy paradox, even though a user has concerns about personal data exposure by the service provider, the user is willing to provide their information. Ghosh and Singh (2017) examined this privacy paradox by focusing on individual justification based on the cognitive dissonance theory. They found that users are aware of their information being exposed and, therefore, perceive the consequences of using or not using services as similar. Therefore, users were seeking higher benefit choices using an external justification such as checking the information that the service was collecting. That is, if mobile payment users perceive data exposure, their privacy protection power would be justified to a higher level in order to avoid dissonance. However, they also found that this behavior consequently contributes to encouraging individuals to share their information for more benefit. Therefore, the users justified the data is being used to provide services to the same individual. In other words, individuals are willing to lose some of their privacy protection power. Thus, this study focuses on the final justification of privacy behavior as users' perception of privacy protection power on the data exposure in mobile payment use.

Ⅲ. Research Model and Hypotheses

<Figure 1> shows our theory-based model. In this section, each of the proposed links will be developed as a hypothesis to be tested.

First, a high level of perceived data exposure means that users perceive a high amount of personal data is collected by service providers, where their personal data can be easily accessible by service providers and moreover their data can be linked and used across different platforms (Boss et al., 2015; Liang and Xue, 2009). PMT suggests a negative relationship between perceived threat and protection motivation. Likewise, we propose that based on the perceived level of data exposure, users would perceive different levels of privacy protection power (PPP) and needed efforts to safeguard their personal data. A user with high data exposure would perceive a different power



<Figure 1> Research Model

than a user with low data exposure: i.e., a perception of high data exposure would lead to a perception of low privacy protection power, while a perception of low data exposure would lead to a perception of high privacy protection power. Hence, the perceived level of data exposure would negatively affect one's feelings and perceptions of how much power to protect his/her privacy an individual has. Based on these arguments, our first hypothesis is developed as follows:

H1: Perceived data exposure is negatively associated with privacy protection power.

Second, self-efficacy and response efficacy have been frequently discussed in PMT-based studies especially for the appraisal coping relationship (Beaudry and Pinsonneault, 2005). Self-efficacy describes the degree to which an individual believes that he/she can perform what is required to avert the threat (Boss et al., 2015). From the perspective of IT adoption and use, self-efficacy affects the user's perception of what IT features to use (Liang and Xue, 2009). PMT suggests a positive relationship between self-efficacy and protection motivation. Hence, we propose that the higher the perceived self-efficacy, the higher the perceived privacy protection power. Based on these arguments, our second hypothesis is developed as follows:

H2: Perceived self-efficacy is positively associated with privacy protection power.

Third, response efficacy describes the degree to which a person believes the recommended response will be effective (Boss et al., 2015). According to Boss et al. (2015), response efficacy works as a belief about the system to adapt mobile payment. If a user believes that he/she knows the system's reputation or pros and cons, the user believes to have more capability to adapt the mobile payment service. In other words, if a user has knowledge of a specific mobile payment system especially regarding the system's security or data protection policy, the user would develop a higher belief in his/her capacity to adapt to the particular mobile payment service. Hence, we propose that the higher the perceived response efficacy, the higher the perceived privacy protection power. Based on these arguments, our third hypothesis is developed as follows:

H3: Perceived response efficacy is positively associated with privacy protection power.

Fourth, a user's high privacy protection power indicates his/her belief to safeguard the access and use of personal data from other firms and thus to safeguard personal data from being accessed and utilized across different parties (Hoffmann et al., 2016; Liang and Xue, 2009). When a user believes he/she has a high level of protection power, the user will recognize the low-level privacy risk, which leads to more chances of use of mobile payment services (Johnston et al., 2018). Hence, we propose that a high level of privacy protection power would indicate a high level of intention to use a mobile payment service. Based on these arguments, our fourth hypothesis is developed as follows:

H4: Perceived privacy protection power is positively associated with the intention to use mobile payment services

Fifth, while the relationship between privacy protection power and the use of mobile payment services would be positive as discussed above, we argue that perceived provider market control would negatively moderate their relationship. Particularly, when one perceives a low level of provider's market control – meaning a high level of customer choice, one would trust his/her perceived power to decide to use a mobile payment (Hasan et al., 2019). However, we see situations where users would use mobile payment even though they perceive a low level of privacy protection power under certain market conditions. For example, a repeating phenomenon occurs when a person, mostly young, frequently uses a new mobile payment service, and when asked if afraid or concerned about such a decision to reveal his/her personal data, the explanation goes that there is nothing left of personal data to hide (Pingitore et al., 2017). Hoffmann et al. (2016) describe this situation using the concept of privacy cynicism and its connection with privacy paradox and cognitive dissonance. This phenomenon may lessen as the person perceives a low level of provider market control – meaning more choices to the person. These examples indicate that the perceived provider market control affects the relationship between privacy protection power and an individual's decision to use the mobile payment service. Hence, it is important and useful to investigate how users behave under their different perceptions of market control conditions. In particular, in a low PPMC market, an individual's privacy protection power and intention to use mobile payment services (PPP to UMSP) has a positive relationship, confirming the same results of prior studies (Hasan et al., 2019). However, in a high PPMC market, there would be a high use of mobile payment services regardless of the level of the privacy protection power. This suggests investigating the role of one's perception of the market environment in making a decision to use mobile payment services. Because the effect of one variable (PPP to UMSP) differs depending on the level of a second variable (PPMC) there would be a moderation effect. It's a negative, not positive, moderating effect because the more positive PPMC is, the more negative the effect of PPP to UMSP becomes (or alternatively, the more negative PPMC is, the more positive effect PPP to UMSP becomes). Based on these arguments, our fifth hypothesis is developed as follows:

H5: The relationship between privacy protection power and the intention to use mobile payment services is negatively moderated by the perceived provider market control (PPMC).

Ⅳ. Research Methods

This research was conducted through the following steps. After developing the hypotheses, we developed the associated measurements to create a survey questionnaire regarding our research constructs. A field survey was conducted using a well-known online survey platform, Amazon Mechanical Turk (AMT) which has been increasingly used for academic surveys (Steelman et al., 2014; Syed et al., 2019). Compared to a paper-based survey, an online survey is known to be more effective in terms of time, cost, flexibility, and anonymity (Goodman et al., 2013; Lowry et al., 2016). To improve the quality of the collected data, we applied some constraints for survey participation, which were believed necessary for the contexts of this study. Specifically, we limited the survey to only those in the United States to minimize potential compounding effects by different levels of economic status and different cultural backgrounds among samples. Also, we limited taking the survey only for 18 years or older people as potential mobile payment users.

We had two pilots before collecting the final sample data. The purpose of pilot trials was to ensure that the survey has no errors for our main data collection. Through the pilots, we revised and updated our survey. For our main survey, we also used multiple countermeasures, such as fake questions and reverse-scale questions, to filter out unconscious responses. After excluding some data based on the embedded fake questions and reverse-scale questions, we achieved a total of 200 final samples, and they were analyzed using a structural equation modeling (SEM) technique[3].

The final data show that respondents are from different states and regions in the United States, additionally confirming the unbiased of our data. 44% of the final samples were female and 55% were male. Their ages were well ranged from 18 to over 63 while 28-32 (18%) and 32-37 (18.5%) were the largest groups. 45.5% had a bachelor's degree, and 41% reported 50-100K as their annual income.

For construct operationalization of this study, most of our constructs – self-efficacy, response efficacy, and mobile payment use intention – were from previous literature (Beaudry and Pinsonneault, 2005; Chandra et al., 2010; Johnston and Warkentin, 2010), while other constructs were adapted from some relevant studies (Avital et al., 2007; Hoffmann et al., 2016; Johnston and Warkentin, 2010). For control variables, we included four variables from the collected demographics information of the final samples, including mobile phone operating system, gender, age, and household income. <Appendix A> provides the full lists of measurement items used for the research constructs development. <Table 1> provides the measurement descriptions of our research constructs with their sources.

Ⅴ. Results and Analyses

The data were analyzed by applying the partial least squares (PLS) SEM technique using SmartPLS version 3.2.8. We first checked the validity of our measurements and constructs and then analyzed the structural model to see how our proposed model

3) The first pilot was conducted from Nov 9, 2019 to Nov 14, 2019 and received a total of 18 responses. The second pilot was conducted on Nov 16, 2019 and received a total of 10 responses. Then the main survey was conducted from Nov 17, 2019 to Nov 21, 2019 and received a total of 250 responses. Through the online survey platform, Amazon Mechanical Turk (AMT), we limited the distribution to these numbers and then screened them as discussed above.

<Table 1> Measurement Items and Sources

Constructs	Measurement Descriptions	Sources
Perceived Data Exposure	Measured in terms of the perceived degree of collection and access of users' personal data by service providers such as Amazon, Apple, and Samsung, and the link and usage of the personal data across different service providers	Liang and Xue (2009)
Self-Efficacy	Measured in terms of the belief on the privacy and security protection, the possibility of protection, and the knowledge about how to protect privacy and security in a dangerous situation or when it necessary	Beaudry and Pinsonneault (2005)
Response Efficacy	Measured in terms of the belief on the advised and recommended action for protecting personal data and privacy when using mobile payment services	Johnston and Warkentin (2010)
Privacy Protection Power	Measured in terms of the belief in the power to safeguard personal data against collection, access, usage of personal information by service providers, to refuse on the consent form of collecting personal data, and to protect personal data from being linked and used across different platforms	Hoffmann et al. (2016)
Perceived Provider Market Control	Measured in terms of the perception of service provider's control over the market in general and the critical resources or technologies in the market	Avital et al. (2007)
Use of Mobile Payment Services	Measured in terms of the intention to use mobile payment service within next six months for processing payments, tracking transactions, and other purposes, and as a wallet	Chandra et al. (2010)

Note: We used a seven-point Likert scale (1 = strongly disagree, 7 = strongly agree) for the measurements under each construct.

can explain the behavioral intention of mobile payment service use.

5.1. Measurement Model Analysis

For measurement validation, the PLS measurement model links each construct to questions that measure their latent construct. The strength of the measurement model was established in terms of convergent validity and discriminant validity (Hair, 1998). For convergent validity, we examined the reliability of items, composite reliability of constructs, Cronbach's Alpha, and average variance extracted (AVE) of research constructs. We used a reliability score of 0.7 or more for the reliability of reflective items, and Cronbach's alpha of 0.7 or more for the reliability of the constructs (Hair, 1998). To verify a proper convergent validity of constructs, we maintained an AVE of higher than 0.5. We also checked the variance inflation factor (VIF) score of each construct to validate and avoid any possibility of multicollinearity problem in our measurement model. During this process, we had to remove a couple of measurement items to improve the validity of our measurement model. Common method biases were examined through a full collinearity assessment approach (Kock, 2015). Our results show that all VIF values were higher than the required threshold (3.3), which indicates that our measurement model is free from the common method bias (Kock, 2015). As shown in <Table 2>, our final measurement model satisfies the required standard of convergent validity.

We also tested discriminant validity by examining the AVE of a construct and its correlations with other research constructs (Fornell and Larcker, 1981). According to this approach, the discriminant validity is established when the square root of AVE of each construct is higher than its correlations with other constructs. As shown in <Table 3>, our results confirm that all constructs meet this requirement and

<Table 2> Results of Convergent Validity Test for Reflective Constructs

	Items #	Item Reliability	Composite Reliability	Cronbach's Alpha	AVE
Perceived Data Exposure (PED)	PED1 PED2 PED3 PED4	0.757 0.820 0.766 0.832	0.872	0.814	0.631
Self-Efficacy (SEFF)	SEFF1 SEFF2 SEFF3	0.894 0.925 0.894	0.931	0.889	0.818
Response Efficacy (REFF)	REFF1 REFF2 REFF3 REFF4	0.815 0.889 0.897 0.871	0.925	0.891	0.754
Privacy Protection Power (PPP)	PPP1 PPP2 PPP3	0.89 0.836 0.935	0.919	0.869	0.792
Perceived Provider Market Control (PPMC)	PPMC1 PPMC2	0.954 0.879	0.914	0.821	0.842
Use of Mobile Payment Services (UMPS)	UMPS1 UMPS2 UMPS3	0.922 0.752 0.787	0.862	0.768	0.678

<Table 3> Results of Discriminant Validity Test for Research Constructs

	PDE	SEFF	REFF	PPP	PPMC	UMPS
Perceived Data Exposure (PDE)	**0.794**					
Self-efficacy (SEFF)	-0.069	**0.904**				
Response Efficacy (REFF)	-0.242	0.520	**0.868**			
Privacy Protection Power (PPP)	-0.480	0.529	0.559	**0.890**		
Perceived Provider Market Control (PPMC)	0.257	0.121	0.112	0.075	**0.917**	
Use of Mobile Payment Service (UMPS)	0.054	0.277	0.194	0.171	0.216	**0.824**

Note: The bolded numbers on the diagonal are the square root of the AVE of research constructs (reflective).

thus the discriminant validity of our measurement model was verified.

We also tested the Heterotrait-Monotrait Ratio of correlations (HTMT) as a more accurate measure of discriminant validity for reflective constructs (Henseler et al., 2015). According to <Table 4>, all of the HTMT ratios of our research constructs are lower than the threshold value (.85). HTMT values supporting discriminant validity should be lower than 0.85 if constructs are conceptually different (Henseler et al., 2015). Together, therefore, these results confirm that our measurement model demonstrated adequate discriminant validity.

We Further conducted supplemental analyses to address potential multicollinearity and common method bias (CMB) issues. To test multicollinearity,

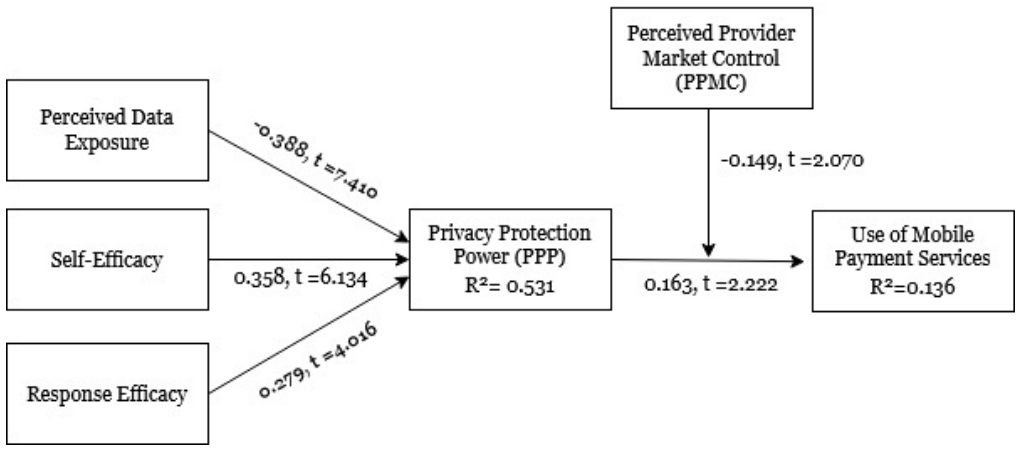
<Table 4> Results of Heterotrait-Monotrait Ratio (HTMT) Test

	PDE	SEFF	REFF	PPP	PPMC	UMPS
Perceived Data Exposure (PDE)						
Self-efficacy (SEFF)	0.137					
Response Efficacy (REFF)	0.234	0.582				
Privacy Protection Power (PPP)	0.509	0.604	0.626			
Perceived Provider Market Control (PPMC)	0.333	0.140	0.131	0.095		
Use of Mobile Payment Service (UMPS)	0.142	0.309	0.233	0.207	0.230	

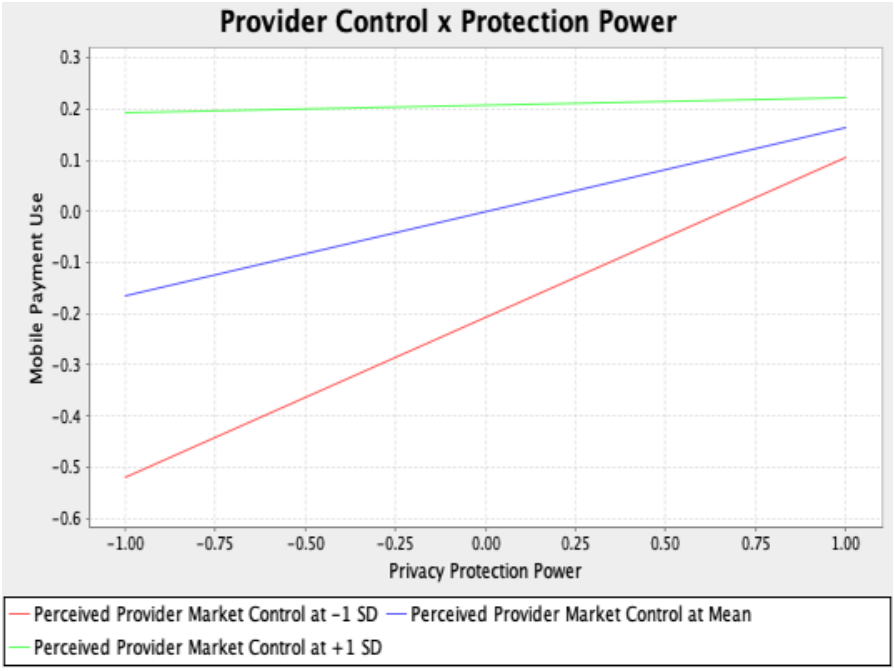
first, we used the variance inflation factor (VIF). We regressed all variables to each other and found that VIF scores of all constructs were between 1.057 and 2.160, which are lower than 3.3 (Kock, 2015). Second, we tested any possibility of CMB using Harman's single-factor test. The results showed that each of the six principal components explained similar amounts of the total variance of 58.4%, ranging from 6.13% to 14.94%. The results indicate that CMB is unlikely to be a serious concern in our study. Therefore, we conclude that our model is free from the multicollinearity concern.

5.2. Structural Model Analysis

For the analysis of our structural model, we used the path analysis and bootstrapping mechanisms that allow testing the statistical significance of various PLS-SEM results, such as path coefficients, t-statistics, and R^2 values. <Figure 2> illustrates the final statistical significance of the proposed relationships in the model. The results show that all of our hypotheses were statistically supported (at least at the 0.05 level), including both the direct and moderation effects. In particular, our model explained 53.1% of the variance of the privacy protection power and 13.6% of the intention to use mobile payment. For our hypotheses, the negative relationship between perceived data exposure and privacy protection power (H1) was statistically supported at the 0.01 level of significance. Also, the positive relationships between self-efficacy and response efficacy toward privacy



<Figure 2> Research Model Results



<Figure 3> Slope Analysis for the Moderating Effect of PPMC

protection power (H2 and H3, respectively) were statistically significant at the 0.01 level of significance. In addition, the results indicate that the positive relationship between privacy protection power and the intention to use mobile payment (H4) was significantly supported at the 0.05 level of significance.

Finally, our results reveal the negative moderating effect of the perceived level of provider market control (PPMC) on the relationship between the privacy protection power and the intention to use mobile payment, which statically supports our final hypothesis (H5) at the 0.05 level of significance. To better understand this moderation effect, we conducted a simple slope analysis as shown in <Figure 3>. The slope analysis result indicates that in a low level of PPMC, meaning a higher level of customer choice, an individual's privacy protection power and intention to use mobile payment services has a positive relationship, which confirms the same results of prior studies (Hasan et al., 2019). However, under a high level of PPMC, meaning a lower level of customer choice, the results suggest overall high use of mobile payment services regardless of the level of the privacy protection power, which is a very interesting and novel finding regarding the role of one's perception of the market environment in making a decision to use mobile payment services.

VI. Discussion

This study aims to answer two questions: 1) about the role of perceived power for personal data (privacy) protection in the mobile payment service use; 2) about the role of mobile payment service environment, especially the level of provider's market control, in the privacy protection and service use relationship. To answer these questions, we developed a theo-

ry-based model drawing upon the theoretical perspectives on protection motivation, provider market control, and cognitive dissonance. Our theoretical model and empirical test results of the model using a set of survey data allows a better understanding of an individual's mobile payment service use.

First, our findings provide additional insights to the PMT by highlighting an individual's attention to his/her perceived personal data exposure and privacy protection power. According to our model and results, when an individual makes a decision to use a mobile payment service, his/her use decision is not only impacted by what he/she perceives will happen in the future upon the use (e.g., my personal data will be accessed by other firms), but also by what a user perceives in the current situation (e.g., my personal data is already exposed). When considering the recent massive increase of personal data collection and usage by service providers, it is timely and useful to examine the impact of user's perception of personal data exposure on individual's adoption and use decisions of mobile payment services.

Second, our findings indicate the importance of understanding the privacy protection power as a mediating factor - an important stage that occurs before developing an intention to use mobile payment. This finding would provide a new understanding of the phenomenon from a new perspective on perceived power.

Third, this study examined the conditional effects of the perceived level of provider market control (PPMC) on the relationship between privacy protection power and the intention to use mobile payment. Especially, our results confirmed the proposed role of PPMC, i.e., its negative moderation effect that has not been discussed in the market monopoly literature. For example, Hasan et al. (2019) argued a hindrance in the role of provider control on the use of mobile payment services, which is also a negative moderation effect. In our study, however, we found an alternative phenomenon of the high use rates of the mobile payment services even when the perceived provider market control is high – a different form of negative moderation effects by PPMC. Hence, it would provide a novel explanation for the high use in places where users perceive a high level of PPMC compared with other places where users perceive a low level of PPMC in light of privacy protection power. This finding would highlight new interesting areas for future research such as cross-market analysis.

The findings of this study also would be helpful to practitioners, especially the mobile payment companies (both startups and large companies), to understand additional measures needed to increase the mobile payment service use by their current or future users. Likewise, this study would benefit technology companies in general by putting stress on the potential importance of data privacy on end-users' technology use, particularly about users' perception of their power for data safeguarding especially when they have more market choices. For instance, for marketing teams in mobile payment companies, marketing communications would not be the same in the high PPMC market versus the low PPMC market. In the low PPMC market, marketing communication would need to consider topics such as data privacy and reinforce that a user has the expected privacy protection power as switching to other mobile payment providers would be easier if these expectations are not met. On the other side, in the high PPMC market, marketing communications wouldn't need to worry as much as in the low PPMC market and would instead focus on other mobile payment features as data privacy and privacy protection power would not be a large concern for users in this type of market.

In addition, this study would benefit investors and their investment decisions as mobile payment usage and adoption would be higher in the high PPMC market than in the low PPMC market, and thus mobile payment companies in the high PPMC market would grow at a higher rate than in the low PPMC market. Similarly, the findings of this study would benefit policymakers in both the low and high PPMC markets in which policymakers would have a better understanding of the potential factors that could impact the growth of mobile payment services in particular markets and therefore make appropriate policies e.g., ease or toughen data handling policies.

From a technical perspective, the implications of these findings would benefit the development and improvement of features on mobile payment applications. Our findings indicate that the required application features would not be the same in both high PPMC and low PPMC markets. In the low PPMC market, the features of mobile payment applications should include data privacy elements such as storing, accessing, and linking data, and reinforce that a user has the expected privacy protection power as switching to other mobile payment providers would be easier if these expectations are not met. On the other side, in the high PPMC market, data privacy and privacy protection power would not be a significant concern for users in this type of market and therefore the needed features would instead focus more on other mobile payment features such as speed and convenience of mobile transactions.

The theoretical and practical implications, however, need to be considered in light of the limitations of this study. First, data were collected using a web-based survey platform, Amazon Mechanical Turk (AMT) that distributes survey questions to subscribed respondents. Although the pool of respondents is large and their backgrounds vary, there is a possibility that some respondents' answers may not truly reflect a random, unbiased sampling. Hence, a more sophisticated approach to achieve an unbiased sampling, like collecting data from different age groups and geographic locations would be helpful in our future research. Second, this study collected data only from the United State. For more generalizable findings, future research may extend the analysis beyond this regional constraint and focus comparisons with other regions. With this extension, we can investigate more objective differences in user perception on market conditions to where each sample belongs. Along with the regional differences, the role of cultural uniqueness can be investigated to find further insights. Third, the model test in this study was done using 200 samples. Although this number would be sufficient for the current explorative purpose of this study, future research may expand the sample size to test more complex research models. Fourth, since existing relevant research shows that different age groups have different use behaviors (Chandra et al., 2010), future research can extend this study to compare the use behaviors in different age or social groups. Lastly, future research can incorporate alternative perspectives to the proposed research model. Instead of using privacy protection power, for example, future research can study one's intention or motivation to protect personal information. Interestingly, an increase in the degree of exposure of personal information can either decrease or increase one's intention or motivation to protect personal information. On one hand, increased personal information exposure can make an individual feel exhausted on personal information protection (i.e., privacy fatigue) and thus decreases his/her intention to protect personal information. On the other hand, an increase in personal information exposure can also increase the user's psy-

chological ownership of personal information, which in turn can maximize personal information protection behavior. Thus, future research would investigate these conflicting perspectives on the impacts of personal information exposure on the intention to protect personal information, especially from the market contingency perspective (i.e., the moderation role of market control on these conflicting perspectives).

Ⅶ. Conclusion

In this study, we examined the use of mobile payment services in light of privacy protection power and provider market control. Our results reveal that self-efficacy, response efficacy, perceived data exposure, and privacy protection power have important roles in determining the intention to use mobile payment. In this study, we combined two different theoretical perspectives and found significance in the intention to use mobile payment services by self-efficacy (positive), response efficacy (positive), and perceived data exposure (negative) through the privacy protection power (positive). Furthermore, through a moderation effect test, we found very interesting conditional effects of the perceived level of provider market control (PPMC) on the relationship between the privacy protection power and the intention to use mobile payment: i.e., with a perception of high PPMC, people use the mobile payment regardless of their privacy protection power, while with a perception of low PPMC, their decision to use mobile payment services depends on the degree of perceived privacy protection power that they have. These findings through this study would help both academics and practitioners, such as mobile payment companies and technology companies, to better understand the user behavior of mobile payment services and to find more opportunities in both future research and business.

<References>

[1] Anderson, R. (2001). *Security engineering: A guide to building dependable distributed system.* Wiley Computer Publishing, New York.

[2] Arvidsson, N. (2014). Consumer attitudes on mobile payment services – results from a proof-of-concept test. *International Journal of Bank Marketing, 13*(2), 150-170.

[3] Avital, M., Sawyer, S., Kraemer, K., Sambamurthy, V., Lyytinen, K., and Iacono, C. S. (2007). Data rich and data poor scholarship: Where does IS research stand? *International Conference on Information Systems (ICIS) Proceedings*.

[4] Beaudry, A., and Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaptation. *MIS Quarterly, 29*(3), 493-524.

[5] Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., and Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837-864.

[6] Chandra, S., Srivastava, S. C., and Theng, Y. L. (2010). Evaluating the role of trust in consumer adoption of mobile payment systems: An empirical analysis. *Communications of the Association for Information Systems, 27*(29), 561-588.

[7] Chen, L. D. (2008). A model of consumer acceptance of mobile payment. *International Journal of Mobile Communications, 6*(1), 32-52.

[8] Choi, H., and Jung, Y. (2019). Online users' cynical attitudes towards privacy protection: Examining privacy cynicism. *Asia Pacific Journal of Information*

Systems, 30(3), 547-567.

[9] Choi, H., Jung, Y., and Choi, Y. (2019). Understanding of the fintech phenomenon in the beholder's eyes in South Korea. *Asia Pacific Journal of Information Systems, 29*(1), 117-143.

[10] Epstein, L. G. and Kopylov, I. (2005). Cognitive dissonance and choice. *Working Paper*, University of Rochester.

[11] Ernst and Young (2019). *Global FinTech adoption index 2019*. Retrieved from https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-fintech-adoption-index.pdf.

[12] Eze, U. C., Gan, G. G. G., Ademu, J., and Tella, S. A. (2008). Modelling user trust and mobile payment adoption: A conceptual framework. *Communications of the IBIMA, 3*(29), 224-231.

[13] Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407-429.

[14] Fornell, C., and Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement Error. *Journal of Marketing Research, 18*(1), 39-50.

[15] Gao, L., and Waechter, K. (2017). Examining the role of initial trust in user adoption of mobile payment services: An empirical investigation. *Information Systems Frontiers, 19*(3), 525-548.

[16] Ghosh, I., & Singh, V. (2017). Using cognitive dissonance theory to understand privacy behavior. *Proceedings of the Association for Information Science and Technology, 54*(1), 679-681.

[17] Goodman, J. K., Cryder, C. E., and Cheema, A. (2013). Data collection in a flat world: The strengths and weaknesses of mechanical turk samples. *Journal of Behavioral Decision Making, 26*(3), 213-224.

[18] Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., and Tatham, R. L. (1998). *Multivariate data analysis*. Upper Saddle River, NJ: Prentice hall.

[19] Hasan, R., Liu, Y., Kitchen, P. J., and Rahman, M. (2019). Exploring consumer mobile payment adoption in the bottom of the pyramid context: A qualitative study. *Strategic Change, 28*(5), 345-353.

[20] Henseler, J., Ringle, C. M., and Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115-135.

[21] Hoffmann, C. P., Lutz, C., and Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10*(4), Article 7.

[22] Jaradat, M. I. R. M., and Faqih, K. M. (2014). Investigating the moderating effects of gender and self-efficacy in the context of mobile payment adoption: A developing country perspective. *International Journal of Business and Management, 9*(11), 147-169.

[23] Johnston, A. C., and Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly 34*(3), 549-566.

[24] Johnston, V. L., Kiser, A., Washington, R., and Torres, R. (2018). Limitations to the rapid adoption of m-payment services: Understanding the impact of privacy risk on M-payment services. *Computers in Human Behavior, 79*, 111-122.

[25] Kankanhalli, A., Lee, O. K. D., and Lim, K.H. (2011). Knowledge reuse through electronic repositories: A study in the context of customer service support. *Information & Management, 48*(2-3), 106-113.

[26] Kim, S., Mirusmonov, M., and Lee, I. (2010). An empirical examination of factors influencing the intention to use mobile payment. *Computers in Human Behavior, 26*(3), 310-322.

[27] Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration, 11*(4), 1-10.

[28] Liang, H., and Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71-90.

[29] Liébana-Cabanillas, F, Sánchez-Fernández, J., and Muñoz-Leiva, F. (2014). Antecedents of the adoption of the new mobile payment systems: The moderating

effect of age. *Computers in Human Behavior, 35*, 464-478.

[30] Lowry, P. B., D'Arcy, J., Hammer, B., and Moody, G. D. (2016). "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of cata collection, including mechanical turk and online panels. *The Journal of Strategic Information Systems, 25*(3), 232-240.

[31] Moon, Y. (2020). Enablers of the adoption of mobile banking: From economic-psychological-social perspectives. *Asia Pacific Journal of Information Systems, 30*(1), 72-93.

[32] Pingitore, G., Rao, V., Dwivedi, K., and Cavallaro, K. (2017). To share or not to share. *Deloitte Insights*, Retrieved from https://www2.deloitte.com/insights/us/en/industry/retail-distribution/sharing-personal-information-consumer-privacy-concerns.html.

[33] Prahalad, C. K., and Hart, S. L. (2002). Strategy and business. *The Fortune at the Bottom of the Pyramid, 26*, 2-14.

[34] R, N., and Rathi, R. (2019). *Mobile payments: Comparison of two powerhouses of the world*. Retrieved from https://gomedici.com/medici_ltp_articles/5558.

[35] Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

[36] Senicar, V., Jerman-Blazic, B., and Klobucar, T. (2003). Privacy-enhancing technologies-approaches and development. *Computer Standards & Interfaces, 25*, 147-158.

[37] Slade, E., Willams, M., Dwivedi, Y., and Piercy, N. (2015). Exploring consumer adoption of proximity mobile payments. *Journal of Strategic Marketing, 23*(3), 209-223.

[38] Statista (2017). *Preferred payment methods of online shoppers worldwide as of March 2017*. Retrieved from -https://www.statista.com/statistics/508988/preferred-payment-methods-of-online-shoppers-worldwide/

[39] Steelman, Z. R., Hammer, B. I., and Limayem, M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *Journal of Consumer Psychology, 23*(2), 212-219.

[40] Syed, R., Dhillon, G., and Merrick, J. (2019). The identity management value model: A design science approach to assess value gaps on social media. *Decision Sciences, 50*(3), 498-536.

[41] Tsai, J. Y., Egelman, S., Cranor, L., and Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research, 22*(2), 254-268.

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

[43] Yang, S., Lu, Y., Gupta, S., Cao, Y., and Zhang, R. (2012). Mobile payment services adoption across time: An empirical study of the effects of behavioral beliefs, social influences, and personal traits. *Computers in Human Behavior, 28*(1), 129-142.

[44] Zhou, T. (2013). An empirical examination of continuance intention of mobile payment services. *Decision Support Systems, 54*(2), 1085-1091.

<Appendix A>

<Table 5> Measurement Items

Construct	ID	Survey Statement
Self-Efficacy (SEFF)	SEFF1	▪ I can figure out how to protect my privacy if I try my best.
	SEFF2	▪ It is important to protect my personal data.
	SEFF3	▪ In danger or suspicious situations, I know how to protect my personal data.
	SEFF4	▪ I know how to protect most of the data that I need to protect my privacy and security.
Response Efficacy (REFF)	REFF1	▪ I believe that advised actions (e.g., strong password) would be sufficient to protect my personal data.
	REFF2	▪ I believe that recommended responses (e.g., confirming your identity) would solve my concerns about my personal data.
	REFF3	▪ I perceive that advised actions would be very helpful to solve my privacy problems.
	REFF4	▪ Recommended responses will help me find privacy issues early.
Perceived Data Exposure (PED)	PED1	▪ A large amount of my personal data is already collected by firms such as Amazon, Apple, and Samsung.
	PED2	▪ My personal data can be easily accessible by FinTech service providers.
	PED3	▪ Some personal data is collected without my consent.
	PED4	▪ My personal data can be linked and used across different service providers.
Privacy Protection Power (PPP)	PPP1	▪ I have the power to safeguard my personal data collected by mobile FinTech payment providers.
	PPP2	▪ I have the power to safeguard the access and use of my personal data from other firms.
	PPP3	▪ When I give consent to collect my personal data, I have the power to revoke it.
	PPP4	▪ I have the power to safeguard my personal data from being linked and used across different platforms.
Perceived Provider Market Control (PPMC)	PPMC1	▪ There are few FinTech service providers.
	PPMC2	▪ FinTech service providers have strong control over the FinTech market.
	PPMC3	▪ The FinTech service providers have strong control of critical resources/technologies of the FinTech market.
	PPMC4	▪ Barriers to entry for new FinTech service providers are very high.
Use of Mobile Payment Services (UMPS)	UMPS1	▪ I frequently use mobile FinTech payment services to process payments.
	UMPS2	▪ I frequently use mobile FinTech as a wallet.
	UMPS3	▪ I frequently use mobile FinTech to track my transactions.
	UMPS4	▪ I frequently use mobile FinTech payment services for other purposes.

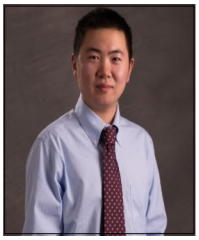
◆ About the Authors ◆

Mohammad Bakhsh

Mohammad Bakhsh is a Ph.D. Candidate in Business with focus on Information Systems for Data Science at the University of Massachusetts Boston. He has a BSc in operations from Northumbria University, England, and an MBA from San Francisco State University. His research interests include text analysis, spatial data and network optimization.

Hyein Jeong

Hyein Jeong is a Ph.D. Candidate in Business with focus on Information Systems for Data Science at the University of Massachusetts Boston. She has a bachelor's degree in Business Administration from University at Albany, State University of New York (SUNY) and worked as research assistant for the business plan project in University at Albany, SUNY and Pratt Institute. Her research interests include IT capabilities and management information system.



Lingyu Zhao

Lingyu Zhao is a Ph.D. Candidate in Business with focus on Information Systems for Data Science at the University of Massachusetts Boston. He has a master's degree in Computer Science from Boston University. His research interests include management information system.

One-Ki Daniel Lee

One-Ki Daniel Lee is an Associate Professor of the Department of Management Science and Information Systems at the University of Massachusetts Boston. He received his Ph.D. from the City University of Hong Kong and his Master's degree from the Korea Advanced Institute of Science & Technology (KAIST). His research interests include IT-enable dynamic capabilities (e.g., agility and KM capability), ambidextrous IT management and strategies, IT-enabled agile crisis management, and global IT project and risk management. His work has appeared in leading IS journals such as *Information Systems Research, Information & Management, IEEE Transactions on Engineering Management, Communications of the ACM, Communications of the AIS, Journal of Global Information Management*, and *Asia Pacific Journal of Information Systems.*

Submitted: March 24, 2021; 1st Revision: June 10, 2021; Accepted: June 22, 2021