6-22-2020

Facial Payment Use in China: An Integrated View of Privacy Concerns and Perceived Benefits

Chenglong Li
University of Turku, chenglong.li@utu.fi

Hongxiu Li
Tampere University, hongxiu.li@tuni.fi

Ping Wang
Wuhan University, wangping@whu.edu.cn

Facial Payment Use in China: An Integrated View of Privacy Concerns and Perceived Benefits

Research-in-Progress

Chenglong Li
University of Turku
Turku, Finland
chenglong.li@utu.fi

Hongxiu Li
Tampere University
Tampere, Finland
hongxiu.li@tuni.fi

Ping Wang
Wuhan University
Wuhan, China
wangping@whu.edu.cn

Abstract

This paper presents a study design intended to investigate the privacy concerns and benefits related to the adoption of facial payment technology from a privacy calculus perspective. In the proposed research model, relative advantages, including convenience, availability, and security, are considered as perceived benefits in facial payment adoption and assumed to exert a positive influence on the adoption of facial payment. The privacy concern, involving threat appraisal (perceived severity and vulnerability) and coping appraisals (response efficacy and self-efficacy), are articulated as perceived risks. Threat appraisals negatively affect people's intention to use facial payment technology, whereas coping appraisals positively influence their usage. Based on privacy calculus framework, the benefit-risk analysis shapes people's adoption behavior of facial payment technology. In addition, personal innovativeness is set as moderators in the proposed model. This research might contribute to literature on privacy concerns and facial payment technology use, and offer practical implications for facial payment providers.

Keywords: Privacy concerns, facial payment, privacy calculus, protection motivation theory, benefits, risks

Introduction

Along with the rapid development of face recognition technology, the application of facial payment (FP) has been popular in China. FP provides consumers with a hassle-free payment experience as consumers can pay with the presence of their faces to devices once they have bound their facial information and payment accounts. In China, Alipay and WeChat, the two leaders in online and mobile payments in China, have been powering the trend with FP devices already in hundreds of cities (Agence France-Presse 2019). According to the report released by iiMedia, the number of Chinese users of facial payment in 2018 was 61 million, and the user population was estimated to exceed 760 million in 2022 (iiMedia Report 2019). FP could be more convenient than mobile payment as the systems do not require entering a password or placing a finger on a scanner (Zhang and Kang 2019). Additionally, FP has been suggested to be with high security as it requires high accuracy with users' facial information and accounts, and the recognition rate of FP has also reported to be quite high and accurate (Lin 2000; Vazquez-Fernandez and Gonzalez-Jimenez 2016).

Despite the advantages of FP, its penetration and adoption still face the great challenge of users' concerns about privacy. Since FP collects the facial biometric information of users, many users worry about the potential misuse and the possible invasions to their privacy (Carpenter, McLeod, Hicks and

Maasberg 2018; Miltgen, Popovič and Oliveira 2013; Oh, Lee and Lee 2019). For instance, users' biometric information related to their faces in database could be stolen and misused by hackers (Vazquez-Fernandez and Gonzalez-Jimenez 2016). But users could not make changes of their facial information like changing their passwords in case of user information misuse or leak. Users' perception of privacy concerns might impede their adoption of FP, which may further lead to the failure of FP (Pons and Polak 2008). Thus, it is important to investigate both the underlying drivers of users' adoption of FP as well as their privacy concerns in FP usage in order to get a comprehensive understanding of users' adoption of FP.

Prior literature on innovative payment research has mainly focused on investigating new payment technologies like mobile payment (e.g., Gong, Zhang, Chen, Cheung and Lee 2019; Gong, Zhang, Chen, Cheung and Lee 2020; Silic, Barlow and Back 2018), but research on FP has been rare. FP has its uniqueness. As an automatic method of individual recognition based on biometric information, FP is capable to identify and track people without consumers' consent, which may raise greater privacy concerns than other payment methods (Prabhakar, Pankanti and Jain 2003). Pons and Polak (2008) argued that sensitive biometric information could increase users' perceived risks and decrease the use intention. On the other side, although FP users concern about their privacy in FP use, they could also benefit from using FP as the payment technology is easier, smoother, and safer than mobile payment (Zhang and Kang 2019). Therefore, it is necessary to examine users' adoption of FP with an integrated view of the potential risks (i.e., privacy concern) and benefits in FP use.

In addition, prior literature has researched on biometric technology adoption from a standpoint of privacy concerns. For instance, in the work of Miltgen et al. (2013), users' perceived risks have been found to exert a negative effect on intention to accept a biometric system. Carpenter et al. (2018) also found that privacy concerns on biometric technology (i.e., perceived accountability and perceived vulnerability) negatively affect an employee's attitude toward using biometric technology in workplace. Prior research has highlighted the privacy risks in using biometric technology, but ignored how users could cope with privacy concerns in biometric technology. According to protection motivation theory (PMT) (Rogers 1975), such as in FP context, when users are aware of potential risks to their privacy, they can develop adaptive responses for mitigating such privacy threats (Boss, Galletta, Lowry, Moody and Polak 2015). Thus, it is essential to take both perceived privacy threats and perceived privacy control into consideration when examining privacy concerns in FP use in order to obtain a more comprehensive insight into privacy concerns in FP adoption.

Third, previous research suggest that personal characteristics (i.e., personal innovativeness) can moderate the relationships between IS adoption and its antecedents (Sun 2012). However, little research has studied the moderating effect of personal innovativeness in IT (PIIT) on FP adoption. Considering that FP is a new innovative payment technology, therefore, it is necessary to investigate how the PIIT strengthens or suppresses the influences of perceived benefits and privacy concerns on FP adoption.

To address the above research gaps, this paper aims to build a framework based on the privacy calculus theory (Culnan and Armstrong 1999) and PMT (Rogers 1975) to investigate the FP adoption by the means of risk-benefit analysis. Following privacy calculus theory, the intention to use FP is based on the trade-off between the perceived risks and perceived benefits (Xu, Teo, Tan and Agarwal 2009; Zhang et al. 2018). Such as the relative advantages of FP reflect the perceived benefits in using FP, while privacy concerns refer to the perceived risks. Further, in order to obtain a nuanced picture of privacy concerns, we specify the components for threat appraisals and coping appraisals related to privacy concerns based on PMT. Furthermore, this study also considers PIIT as a moderator of the relationships of the antecedents and FP adoption intention.

The rest of this paper is structured as follows: first, we begin a literature review that informs our study. Then, we propose the research model and hypotheses. Third, we present the research methods that will be applied in this study. Finally, we discuss the expected outcomes and potential contributions.

Literature Review

Advantages of Facial Payment

FP relies on the face recognition technology (Zhang and Kang 2019). FP connects users' facial information with the payment systems. In terms of its implementation, it compares users' face image captured by a camera with the users' biometric information related to face stored in the database to complete the authentication (Zhang and Kang 2019). When two faces match and are verified to belong to the same person, the payment will be confirmed (Zhang and Kang 2019). As a new form of payment, compared with other payment methods, FP has been argued to have relative advantages, such as in the dimensions of security, convenience, and availability (Vazquez-Fernandez and Gonzalez-Jimenez 2016).

Security. FP is more secure when compared with other traditional payment methods, such as password, and credit card. Facial features of individuals are hard to copy, imitate, or lose (Zhang and Kang 2019). And users need not worry about their accounts being stolen. Additionally, compared to other biometric payment technologies, like fingerprint or iris recognition, current face recognition technology offers both high accuracy and low intrusiveness (Lin 2000; Vazquez-Fernandez and Gonzalez-Jimenez 2016; Zhang and Kang 2019). Along with the development of face recognition technology, such as using 3D light cameras and artificial intelligence algorithms, the safety of FP can be even further improved.

Convenience. FP is much easier to operate than mobile payment. When purchasing, users of FP only need to look at digital cameras of their smartphones or face-scan devices launched by merchants in stores. Particularly, FP is more convenient for the senior people, since FP does not require them to operate with additional devices such as QR code or fingerprint scanners. Also, FP can reduce transaction times as its recognition process only needs a few seconds (Zhang and Kang 2019).

Availability. FP can be usable anywhere and at any time for several reasons. Due to the ubiquity of smartphones, FP can take advantage of the integrated cameras in smartphones (Vazquez-Fernandez and Gonzalez-Jimenez 2016). FP users can utilize the cameras in their smartphones to recognize their faces at anytime and anywhere. Meanwhile, Alipay and WeChat have launched the face recognition machines in quite many stores in hundreds of cities in China to promote the FP, and the number of FP applications is continuously increasing in China (Agence France-Presse 2019; iiMedia Report 2019). It means that for people without smartphones or in case of smartphones out of power, uses also can use FP in the stores when face recognition machines are available.

Privacy Concerns

Privacy concerns refer to "subjects' concerns with their privacy over the Internet" (Hui, Teo and Lee 2007). As FP gathers and stores personal facial biometric information, users may worry about the disclosure of such sensitive biometric information. They may fear the privacy invasion related to facial data collection and misuse by FP providers. For instance, face biometric information stolen by hackers, unwanted identifications, recognition without awareness, and the lack of secrecy (Prabhakar et al. 2003). Though users are aware of the benefits of using FP, such as a higher level of convenience, they will often weigh both the risks and benefits when making decisions on FP use.

Privacy calculus theory assumes that when individuals face a privacy threat, they would like to conduct a risk-benefit analysis before deciding whether to offer private information (Culnan and Armstrong 1999). This theory has been employed to investigate individuals' behavior with regard to privacy issues in various contexts, such as information disclosure in online health communities (Zhang et al. 2018), information sharing in sharing economy (Teubner and Flath 2019), and adoption of healthcare wearable devices (Li, Wu, Gao and Shi 2016). It provides an appropriate research framework for explaining FP adoption. FP users have to agree that FP providers capture their facial biometric information and store such private information in databases in order to benefit them from using this new technology. Their adoption might be affected by the perceived balance between the perceived risks and benefits if allowing FP providers to collect their biometric information. Thus, this study applies privacy calculus theory as a research framework to investigate FP adoption.

In terms of privacy risk calculus, few studies have investigated the antecedents of privacy concerns related to FP. The PMT has been widely employed in the literature to explain individuals' protection motivation related to privacy threat in IS field (e.g., Boss et al. 2015; Zhang et al. 2018). It assumes that individuals would assess privacy threats and their capability to alleviate such threats before performing protection behavior (Boss et al. 2015; Rogers 1975). PMT illustrates two dimensions of privacy concerns: (1) threat appraisal, which includes evaluating the perceived severity and perceived vulnerability to privacy threats, and (2) coping appraisal, which comprises response efficacy and self-efficacy related to take protective actions. PMT provides a framework to examine users' perceptions of privacy threats and their ability to reduce such threats. Thus, PMT was integrated into the proposed research model based on privacy calculus theory to disentangle the antecedents of FP use.

The Research Model and Hypotheses

The Proposed Research Model

In our proposed research model, the privacy calculus theory offers the framework for understanding adoption of FP from the view of benefit-risk analysis. Following the related research on relative advantages of FP, we argue that convenience, availability, and security are the core benefits for FP users. For privacy risks, following PMT, we assume that users' privacy concerns are determined jointly by their appraisals of the privacy threats (i.e., perceived severity and vulnerability) and their appraisals of coping behavior (i.e., response efficacy and self-efficacy). Users' adoption of FP should be shaped by their analysis of perceived benefits (relative advantages) and perceived risks (privacy concerns) related to FP. Figure 1 presents our research model, and Table 1 introduces the construct included in the proposed research model.

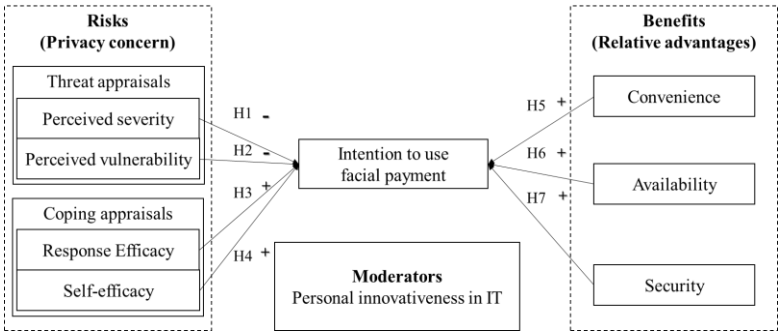

Figure 1. The Proposed Research Model

Table 1. The Key Concepts in the Proposed Model

Concept	Definition
Perceived severity	The degree to which a user believes that a privacy threat will cause consequential harm (Boss et al. 2015).
Perceived vulnerability	The degree to which a user believes that a privacy threat will occur (Boss et al. 2015).
Response efficacy	The degree to which a user believes that the recommended response to a privacy threat will be effective (Boss et al. 2015).
Self-efficacy	The degree to which a user believes that s/he has the capability to perform a recommended response to a privacy threat (Boss et al. 2015).
Convenience	A user's perception of the efficiency of FP, such as the time and effort required to use FP (Choudhury and Karahanna 2008).
Availability	A user's perception that FP services can be pervasive and prompt (Hong and Tam 2006)
Security	A user's perception of the security of technical information, such as privacy leakage (Zhang and Kang 2019)
Intention to use	An individual's intention to use FP (Venkatesh, Morris, Davis and Davis 2003).
Personal innovativeness in IT (PIIT)	An individual trait reflecting one's willingness to try out any new technology (Agarwal and Karahanna 2000)

The Proposed Hypotheses

Perceived severity refers to subjects' evaluation of the severity of consequences caused by a privacy threat (Boss et al. 2015). When people feel threatened, they will often adjust their behavior based on the perceived risk level. On the one hand, when they perceive a high level of severity, they would like to perform preventive responses. On the other hand, when the risk is perceived to be lower, there will be less possibility for them to undertake coping behavior (Herath et al. 2014). Perceived severity has been found to positively affect protection motivation (Boss et al. 2015). Perceived severity has also been uncovered to positively influence individuals' privacy concerns, which, in turn, lead to decreased intention to disclose information in online health communities (Zhang et al. 2018). Likewise, individuals might consider the potential negative dimensions in using FP, such as identity theft and undesired recognition, which could decrease their intention to use FP. When individuals perceive serious consequences as a result of losing privacy through using FP, they are less likely to try the new technology. Therefore, we propose the following hypothesis:

H1: Perceived severity is negatively associated with individuals' intention to use FP.

Perceived vulnerability describes the possibility that a privacy threat will happen (Boss et al. 2015). Once individuals perceive themselves as more vulnerable to privacy risks, they are more likely to carry out protective actions (Boss et al. 2015; Zhang et al. 2018). Previous research has found that perceived vulnerability exerts positive effects on privacy concerns in online health communities (Zhang et al. 2018), and motivation of defense (Boss et al. 2015). As current face technology is capable to capture human face information through digital cameras without consent. Thus, we assume that users' perceptions of vulnerability may also raise their motivation of defense in FP, and thus, negatively affect their intention to adopt FP, Therefore, the following hypothesis is suggested:

H2: Perceived vulnerability us negatively associated with individuals' intention to use FP.

Response efficacy assesses how effective a coping response provided by FP providers can alleviate a privacy risk (Boss et al. 2015). Given that an individual's face information is easy to be collected via cameras, response efficacy is necessary and important to be provided by FP providers in order to protect users' privacy. If individuals feel that their privacy can be effectively protected, they are more likely to lower their privacy concerns and protection motivation (Boss et al. 2015; Johnston and Warkentin 2010). Response efficacy has been found to positively impact users' behavioral intentions to comply with recommended security actions (Johnston and Warkentin 2010). Likewise, FP providers often develop strategies and mechanisms to improve the effectiveness of privacy protection, for instance, updating a privacy-enhanced face recognition system (Erkin et al. 2009). This could result in fewer concerns about the collection of their face information, and lead to their intention to use FP. Thus, we hypothesis accordingly:

H3: Response efficacy is positively associated with individuals' intention to use FP.

Self-efficacy refers to the beliefs of individuals' capabilities to undertake an adaptive behavior (Boss et al. 2015; Zhang et al. 2018). Even though protection has been provided to against privacy threats, people have to know when and how to utilize it (Zhang et al. 2018). Such protection often involves in laws, polices, and regulations regarding privacy, which are somewhat difficult to understand for laymen. Those who are more confident about their ability to manage their privacy problems can have fewer privacy concerns and protection desires. Prior studies have found that self-efficacy has negative influences on privacy concerns and protection intentions (Boss et al. 2015; Johnston and Warkentin 2010; Zhang et al. 2018). Thus, it is reasonable to assume that those with high self-efficacy are more likely to adopt FP. Therefore, we suggest the following hypothesis:

H4: Self-efficacy is positively associated with individuals' intention to use FP.

Convenience is one of the distinguished benefits of using FP. Like mobile payment, FP provides consumers with a wallet-free experience, they do not need to bring any wallets or credit cards when shopping (Agence France-Presse 2019; Zhang and Kang 2019). In stores with face recognition devices available, users even do not need a smartphone. In addition, FP can minimize users' time and efforts for transaction as FP only requires users to present their faces to digital cameras in seconds (Zhang and

Kang 2019). When FP is perceived to be easier, faster, and effortless than other methods, it is more likely to be accepted by users. Previous research has found that convenience affects adoption of new technologies positively, like electronic channels (Choudhury and Karahanna 2008), and NFC-based mobile payment (Ozturk, Bilgihan, Salehi-Esfahani and Hua 2017). Based on the above discussion, it is reasonable to assume that convenience in FP will affect users' intention to use FP positively, and we offer the following hypothesis:

H5: Convenience is positively associated with individuals' intention to use FP.

Availability refers to the ubiquity of FP (Vazquez-Fernandez and Gonzalez-Jimenez 2016). Due to the popularity of smartphones and the wide spread of face recognition devices in China, FP is capable to offer pervasive and timely services (Agence France-Presse 2019; iiMedia Report 2019; Vazquez-Fernandez and Gonzalez-Jimenez 2016). Users believe that FP can be used at any time and from anywhere, which might provide them with a great desire to adopt FP. Previous research has suggested that availability of multipurpose information appliances positively affects perceived usefulness (PU), which leads to adoption intention (Hong and Tam 2006). Thus, we assume that availability will also impact users' intention to use FP, and we hypothesize accordingly:

H6: Availability is positively associated with individuals' intention to use FP.

Face recognition technology evolves rapidly along with the development of deep learning and 3D cameras, current FP technology has been demonstrated to be with high security in use (Lin 2000; Vazquez-Fernandez and Gonzalez-Jimenez 2016; Zhang and Kang 2019). Prior research of Zhang and Kang (2019) points out that security is a key driver of users' adoption of FP. In other words, the higher level of security of FP, the more likely for users to adopt FP. Therefore, we state the following hypothesis:

H7: Security is positively associated with individuals' intention to use FP.

Sun (2012) has found that PIIT moderates the relationships between determinants and adaptive system use (ASU), such as people with a high level of PIIT are more likely to use a new technology in different ways. Following the prior literature, this study considers PIIT as a moderator. We assume that people with high PIIT are more likely to value the benefits of FP, and tolerate the privacy risks, which will substantially make them more likely to use FP. Additionally, this study takes a couple of demographic variables (i.e., age, gender, and education) as control variables since these variables have been posited to affect users' intention to use new innovative technologies (Venkatesh, Thong and Xu 2012).

Methods

Data Collection Plan

This study is designed to collect data through online surveys in China. Alipay and WeChat, the two popular payment platforms that have applied FP, will be employed as the research context in this study. The target respondents of the online survey are the current Alipay or WeChat users. Specifically, we plan to post the questionnaire survey on a popular survey platform in China called Sojump, which has millions of registered sample resources.

Measurement Development

All measurement items for the constructs included in the proposed research model were taken from validated instruments in previous literature, ranging from "1 = strongly disagree" to "7 = strongly agree". Specifically, the items of four constructs regarding privacy concerns, including perceived severity, perceived vulnerability, response efficacy, and self-efficacy, were adopted from the work of Boss et al. (2015). The measures for personal innovativeness in IT were adapted from Agarwal and Karahanna (2000) and Sun (2012). The items measuring security were taken from Zhang and Kang (2019). The convenience measurements were adapted from Choudhury and Karahanna (2008) and Ozturk et al. (2017). The measures of availability were taken from the work of Hong and Tam (2006). The items for the adoption intention came from Venkatesh et al. (2003). All items will be reworded to fit the research context of FP.

Expected Research Results and Limitations

This study may offer several theoretical contributions to the literature. First, this study attempts to investigate adoption of FP via disentangling the components of privacy concerns and relative advantages of FP. The findings could potentially enrich the FP literature by highlighting privacy issue related to FP from a risk-benefit perspective. Second, the proposed research model opens the box of privacy concerns with a threat-coping angle. The findings could add new insights into privacy research in the FP context from not only the standpoint of potential privacy risks but also the point of coping response to perceived threats, which might explain the mechanism in dealing with privacy issues in FP. Third, the identified benefits of using FP in the research model could deepen our understanding of motivations of FP adoption. Finally, the suggested moderating effect of PIIT could add to the IS adoption research by identifying differences between different user groups.

This study may also provide several practical implications. First, the findings on the antecedents of FP adoption could assist FP providers to identify the key drivers and develop strategies to promote the adoption. Meanwhile, the findings on privacy concerns could also provide valuable suggestions to FP providers on how to migrate privacy worries related to FP. Third, the findings on moderators also could aid FP suppliers to identify different user groups and create personalized approaches for target groups.

There are certain limitations to this research. Firstly, as FP adoption is a new phenomenon, the data collected via the survey may not add great depth for understanding of the complex and nuanced features of privacy concerns related to FP. Thus, there are possibilities for us to consider mixed methods (i.e., qualitative and quantitative methods) in the future to enrich the findings. Second, we plan to collect data in China. This could limit our findings into certain countries, future research may consider collecting data from various nations to generalize our findings to FP adoption and compare the cultural differences.

Acknowledgments

The National Natural Science Foundation of China (No. 71774121) supports this study.

References

Agarwal, R., and Karahanna, E. 2000. "Time Flies When You're Having Fun: Cognitive Absorption and Beliefs About Information Technology Usage," *MIS Quarterly* (24:4), pp. 665-694.

Agence France-Presse. 2019. "Smile-to-Pay: Chinese Shoppers Turn to Facial Payment Technology." *The Guardian.* Retrieved from https://www.theguardian.com/world/2019/sep/04/smile-to-pay-chinese-shoppers-turn-to-facial-payment-technology

Boss, S. R., Galletta, D. F., 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), pp. 837-864.

Carpenter, D., McLeod, A., Hicks, C., and Maasberg, M. 2018. "Privacy and Biometrics: An Empirical Examination of Employee Concerns," *Information Systems Frontiers* (20:1), pp. 91-110.

Choudhury, V., and Karahanna, E. 2008. "The Relative Advantage of Electronic Channels: A Multidimensional View," *MIS Quarterly* (32:1), pp. 179-200.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115.

Erkin, Z., Franz, M., Guajardo, J., Katzenbeisser, S., Lagendijk, I., and Toft, T. 2009. "Privacy-Preserving Face Recognition," *International symposium on privacy enhancing technologies symposium*: Springer, pp. 235-253.

Gong, X., Zhang, K. Z. K., Chen, C., Cheung, C. M. K., and Lee, M. K. O. 2019. "What Drives Trust Transfer from Web to Mobile Payment Services? The Dual Effects of Perceived Entitativity," *Information & Management*, pp. 1-11.

Gong, X., Zhang, K. Z. K., Chen, C. Y., Cheung, C. M. K., and Lee, M. K. O. 2020. "Transition from Web to Mobile Payment Services: The Triple Effects of Status Quo Inertia," *International Journal of Information Management* (50), pp. 310-324.

Herath, T., Chen, R., Wang, J. G., Banjara, K., Wilbur, J., and Rao, H. R. 2014. "Security Services as Coping Mechanisms: An Investigation into User Intention to Adopt an Email Authentication Service," *Information Systems Journal* (24:1), pp. 61-84.

Hong, S. J., and Tam, K. Y. 2006. "Understanding the Adoption of Multipurpose Information Appliances: The Case of Mobile Data Services," *Information Systems Research* (17:2), pp. 162-179.

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

iiMedia Report. 2019. "Social Value of the Adoption of China Face-Scanning Payment Technology Research Report." Retrieved from https://report.iimedia.cn/repo8-0/38932.html?acPlatCode=xq&acFrom=bg38932

Johnston, A. C., and Warkentin, M. 2010. "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly* (34:3), pp. 549-566.

Li, H., Wu, J., Gao, Y., and Shi, Y. 2016. "Examining Individuals' Adoption of Healthcare Wearable Devices: An Empirical Study from Privacy Calculus Perspective," *International Journal of Medical Informatics* (88), pp. 8-17.

Lin, S.-H. 2000. "An Introduction to Face Recognition Technology," *Informing Science* (3:1), pp. 1-8.

Miltgen, C. L., Popovič, A., and Oliveira, T. 2013. "Determinants of End-User Acceptance of Biometrics: Integrating the "Big 3" of Technology Acceptance with Privacy Context," *Decision Support Systems* (56), pp. 103-114.

Oh, J., Lee, U., and Lee, K. 2019. "Usability Evaluation Model for Biometric System Considering Privacy Concern Based on Mcdm Model," *Security and Communication Networks* (2019), pp. 1-15.

Ozturk, A. B., Bilgihan, A., Salehi-Esfahani, S., and Hua, N. 2017. "Understanding the Mobile Payment Technology Acceptance Based on Valence Theory a Case of Restaurant Transactions," *International Journal of Contemporary Hospitality Management* (29:8), pp. 2027-2049.

Pons, A. P., and Polak, P. 2008. "Understanding User Perspectives on Biometric Technology," *Communications of the ACM* (51:9), pp. 115-118.

Prabhakar, S., Pankanti, S., and Jain, A. K. 2003. "Biometric Recognition: Security and Privacy Concerns," *IEEE security & privacy* (1:2), pp. 33-42.

Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change," *Journal of Psychology* (91:1), pp. 93-114.

Silic, M., Barlow, J., and Back, A. 2018. "Evaluating the Role of Trust in Adoption: A Conceptual Replication in the Context of Open Source Systems," *AIS Transactions on Replication Research* (4:1), pp. 1-17.

Sun, H. S. 2012. "Understanding User Revisions When Using Information System Features: Adaptive System Use and Triggers," *MIS Quarterly* (36:2), pp. 453-478.

Teubner, T., and Flath, C. M. 2019. "Privacy in the Sharing Economy," *Journal of the Association for Information Systems* (20:3), pp. 213-242.

Vazquez-Fernandez, E., and Gonzalez-Jimenez, D. 2016. "Face Recognition for Authentication on Mobile Devices," *Image and Vision Computing* (55), pp. 31-33.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425-478.

Venkatesh, V., Thong, J. Y. L., and Xu, X. 2012. "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," *MIS Quarterly* (36:1), pp. 157-178.

Xu, H., Teo, H. H., Tan, B. C. Y., and Agarwal, R. 2009. "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services," *Journal of Management Information Systems* (26:3), pp. 135-173.

Zhang, W. K., and Kang, M. J. 2019. "Factors Affecting the Use of Facial-Recognition Payment: An Example of Chinese Consumers," *IEEE Access* (7), pp. 154360-154374.

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B. J., and Zhu, Q. 2018. "Health Information Privacy Concerns, Antecedents, and Information Disclosure Intention in Online Health Communities," *Information & Management* (55:4), pp. 482-493.