FUNDAÇÃO GETULIO VARGAS
ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO

MARCO ALEXANDRE TERLIZZI

PRIVACY CONCERNS AND PROTECTION MOTIVATION THEORY IN THE CONTEXT OF MOBILE BANKING

SÃO PAULO – SP

2019

MARCO ALEXANDRE TERLIZZI

PRIVACY CONCERNS AND PROTECTION MOTIVATION THEORY IN THE CONTEXT OF MOBILE BANKING

Tese apresentada à Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas como requisito parcial à obtenção do título de Doutor em Administração

Campo de Conhecimento: Tecnologia da Informação

Orientador: Prof. Dr. Otávio Próspero Sanchez

SÃO PAULO – SP

2019

Terlizzi, Marco Alexandre.
Privacy concerns and protection motivation theory in the context of mobile banking / Marco Alexandre Terlizzi. – 2019.
96 f.

Orientador: Otávio Próspero Sanchez
Tese (doutorado CDAE) – Fundação Getulio Vargas, Escola de Administração de Empresas de São Paulo.

1. Proteção de dados. 2. Bancos – Inovações tecnológicas. 3. Internet – Aspectos sociais. 4. Direito a privacidade. I. Sanchez, Otávio Próspero. II. Tese (doutorado CDAE) – Escola de Administração de Empresas de São Paulo. III. Fundação Getulio Vargas. IV. Título.

CDU 613/614

Ficha Catalográfica elaborada por: Raphael Figueiredo Xavier CRB SP-009987/O
Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

MARCO ALEXANDRE TERLIZZI

PRIVACY CONCERNS AND PROTECTION MOTIVATION THEORY IN THE CONTEXT OF MOBILE BANKING

Tese apresentada à Escola de Administração de Empresas de São Paulo da Fundação Getulio Vargas como requisito parcial à obtenção do título de Doutor em Administração.

Campo de Conhecimento: Tecnologia da Informação

Data da Aprovação:

____/____/_____

Banca Examinadora:

Prof. Dr. Cesar Alexandre de Souza
Universidade de São Paulo - USP

Prof. Dr. João Luiz Becker
Escola de Administração de Empresas de São Paulo - EAESP/FGV

Profa. Dra. Susan Brown
University of Arizona

Prof. Dr. Otávio Próspero Sanchez (Orientador)
Escola de Administração de Empresas de São Paulo - EAESP/FGV

DEDICATÓRIA

A minha maravilhosa esposa Cynthia e as nossas filhas muito amadas Giovanna e Rafaela.

Aos meus pais Vicente e Fátima, meus maiores exemplos de vida, carinho e amor.

Aos meus queridos irmãos Antonio e Aurelio que sempre estiveram ao meu lado em toda a jornada da vida.

ACKNOWLEDGEMENTS

I want to thank this great institution, the FGV/EAESP, all the professors, students and employees that make this place an excellent and unique school. I am very grateful for all the support I received, and I am also very proud of being part of this institution.

I would like to express my gratitude to my advisor Dr. Otávio Próspero Sanchez for his valuable advice, notable expertise, academic spirit, patience, motivation and for inspiring me.

My sincere thanks to Dr. Susan Brown for allowing me as a visiting scholar at the MIS department at the University of Arizona. Also, I want to express my sincere gratitude to Dr. Laura Brandimarte for all the valuable contributions to my research.

I would like to say thanks to Dr. Cesar Alexandre de Souza, Dr. Alberto Luiz Albertin, and Dr. João Luiz Becker for their participation during the Qualification and/or Examining committee.

AGRADECIMENTOS

Quero agradecer a esta grande instituição, a FGV/EAESP, todos os professores, estudantes e funcionários que fazem deste lugar uma escola excelente e única. Sou muito grato por todo o apoio que recebi, e também tenho muito orgulho de fazer parte desta instituição.

Quero expressar minha gratidão ao meu orientador Dr. Otávio Próspero Sanchez por seus valiosos conselhos, conhecimento notável, espírito acadêmico, paciência, motivação e por me inspirar.

Meus sinceros agradecimentos a Dra. Susan Brown por me aceitar como pesquisador visitante no departamento de MIS da Universidade do Arizona. Quero também expressar minha sincera gratidão a Dra. Laura Brandimarte por todas as valiosas contribuições para minha pesquisa.

Gostaria de agradecer ao Dr. Cesar Alexandre de Souza, ao Dr. Alberto Luiz Albertin, e ao Dr. João Luiz Becker pela participação nas Bancas de Qualificação e/ou Defesa da Tese.

ABSTRACT

Nearly 100% of Americans aged 18 to 29 own a cell phone of some kind, and there has been a move toward using mobile devices for financial services; however, such a move also implies increased opportunities for fraud. Although technology has traditionally been blamed for showing some vulnerabilities, the literature recognizes that human behavior is still the most vulnerable link in an information security system, as it facilitates the discovery of personal identity, account numbers, and passwords, thus often leading to successful financial scams. Protection motivation theory (PMT) is naturally suited to information security contexts in which fear motivates users to protect their information assets; thus, we propose that it can also be meaningfully applied to a privacy context. We addressed four literature gaps: the lack of real-time technology for measuring fear; the omission of a full nomology of PMT as an antecedent of privacy concerns (PC); the omission of fear appeal manipulations in PC; and no reuse of the most up-to-date PC scale. The purpose of this thesis is to examine how PMT can be used in combination with PC in the context of mobile banking (m-banking) and its consequences for risk, trust, and intention to use. We tested our model in four different studies (grouped in three papers): two online surveys, one online experiment, and one lab experiment using emotion detection technology. We found that when an m-banking user is stimulated by a fear appeal message, the fear of losing information increases, consequently activating PC and inducing the user to use the platform more securely. We also contribute to the privacy literature by motivating and studying the relationship between fear and PC.

Keywords: *Privacy Concerns (PC); Protection Motivation Theory (PMT); Mobile Banking Information Privacy Concerns (MBIPC); Internet Privacy Concerns (IPC); CFIP; IUIPC; APCO; FaceReader*.

RESUMO

Quase 100% dos americanos entre 18 e 29 anos possuem algum tipo de telefone celular, e além disso, há uma tendência de crescimento no uso de serviços financeiros via dispositivos móveis. No entanto, tal tendência também resulta em maiores oportunidades de fraude. Embora a tecnologia seja geralmente responsabilizada pelas falhas de segurança, a literatura reconhece que o comportamento humano ainda é o elo mais vulnerável em um sistema de segurança da informação, pois facilita a descoberta de dados pessoais, números de conta e senhas, levando, muitas vezes, a fraudes financeiras bem-sucedidas. A teoria da motivação de proteção (PMT) é naturalmente adequada a contextos de segurança da informação nos quais o medo motiva os usuários a proteger suas informações; assim, propomos que a PMT também pode ser aplicada a um contexto de privacidade. Abordamos quatro lacunas da literatura: a falta de tecnologia em tempo real para medir o medo; a omissão de uma nomologia completa de PMT como antecedente das preocupações com a privacidade de dados (PC); a omissão de manipulações de apelo do medo em PC; e a não há reutilização da escala de PC mais atualizada da literatura. O objetivo deste estudo é examinar como a PMT pode ser utilizada em combinação com a PC no contexto do banco móvel (m-banking) e suas consequências no risco, confiança e intenção de uso. Testamos nosso modelo em quatro estudos diferentes (agrupados em três artigos): duas pesquisas on-line, um experimento on-line e um experimento em laboratório usando a tecnologia de detecção de emoções. Descobrimos que quando um usuário de m-banking é estimulado por uma mensagem de apelo ao medo, o medo de perder informações aumenta, consequentemente ativando PC e induzindo o usuário a usar a plataforma com mais segurança. Também contribuímos com a literatura sobre privacidade, motivando e estudando a relação entre o medo e PC.

Keywords: *Privacy Concerns (PC); Protection Motivation Theory (PMT); Mobile Banking Information Privacy Concerns (MBIPC); Internet Privacy Concerns (IPC); CFIP; IUIPC; APCO; FaceReader*.

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ACC	Improper access
AGFI	Adjusted goodness-of-fit
APCO	Antecedents → privacy concerns → outcomes
AVE	Average variance extracted
AWA	Awareness
CBSEM	Covariance based structural equation modelling
CFA	Confirmatory factor analysis
CFI	Comparative fit index
CFIP	Concerns for the information privacy scale
COL	Collection
CON	Control
CR	Composite reliability
ERR	Errors
FSI	Financial service industry
GFI	Goodness-of-fit
IPC	Internet privacy concerns
IS	Information systems
IT	Information technology
MBIPC	Mobile banking information privacy concerns
NFI	Normalized fit index
NNFI	Nonnormed fit index
PC	Privacy concerns
PMT	Protection motivation theory
RISK	Risk beliefs
RMSEA	Root mean square error of approximation
RMSR	Root mean square residual
SEC	Unauthorized secondary use
TRUS	Trusting beliefs

SUMMARY

1. INTRODUCTION

Mobile banking (m-banking), defined as the use of a mobile device to access a bank or credit union account, can be performed by accessing the service provider's webpage through the web browser on a mobile device, via text messaging, or by using an app downloaded to a mobile device (Fed, 2016). Mobile devices allow people to conveniently execute financial operations while reducing the costs to the financial service industry (FSI), which continues to invest in offering user-friendly applications (Forrester, 2017; Gartner, 2018). In 2017, the FSI spent US$ 364 billion worldwide on information technology (IT), or 13% of the world's total investments in IT (Deloitte, 2018, p. 5).

These investments are crucial for supporting rapid growth in the adoption of smartphones for financial services. Presently, nearly 100% of Americans aged 18 to 29 own a cell phone of some kind (Pew, 2018), and together with this massive adoption of mobile devices, there has been a move toward using mobile devices for financial services. Since 2011, the US Federal Reserve System (Fed, 2016) has been conducting an annual study to examine trends in the adoption and use of m-banking and how the evolution of mobile financial services affects consumers' interaction with financial institutions. The last published study identified that 53% of smartphone owners with a bank account had used m-banking in the 12 months prior to the survey.

The growth in the use of m-banking attests to the significant convenience of such a service; however, it also enables increased opportunities for fraud. Information systems (IS)-based financial fraud has become a major problem in recent years. In 2017, 16.7 million US consumers were victims of identity fraud, with the amount stolen reaching $16.8 billion. In the same vein, account takeover, or the use of another person's account information (e.g., a credit card number) to obtain products and services using that person's existing accounts, tripled over the past year, reaching $5.1 billion, and it continues to be one of the most challenging fraud types for consumers, with victims paying an average of $290 in out-of-pocket costs and spending 16 hours, on average, to resolve (Javelin, 2018).

Consumers usually attribute the responsibility for preventing fraud and data breaches to financial institutions (Javelin, 2018). Although technology has traditionally been blamed for showing some vulnerabilities, the literature recognizes that human behavior is still the most vulnerable link, as it facilitates the discovery of personal identity, account numbers, and passwords, thus often leading to successful financial scams (Abawajy, 2014; Malcolm, Cate, Kathryn, Agata, & Marcus, 2012; Terlizzi, Meirelles, & Cunha, 2017). Additionally, it is known that individuals are in a better position to deter technology-based fraud when they are concerned about revealing their personal information (Earp, Anton, Aiman-Smith, & Stufflebeam, 2005). Although not disclosing personal information is a critical behavior in defending one's financial assets from being misappropriated, this protective practice also prevents individuals from using financial systems in general and, in particular, from adopting m-banking (Fed, 2016).

Although they might decrease technology adoption, privacy concerns (PC), or concerns about how personal and financial information is handled by different platforms or technologies,

can drive positive attitudes toward reducing vulnerabilities. Examples include avoiding the exposure of passwords, avoiding the use of public Wi-Fi networks, enrolling to receive messages about unauthorized account changes, and adopting antivirus software. The factors affecting and affected by PC are complex and require a thorough investigation (Dinev, McConnell, & Smith, 2015; Xu, Dinev, Smith, & Hart, 2011). Given the growth in the number of users of m-banking and the economic importance of the sector, this context is of particular interest. The purpose of this thesis is to examine how PMT can be used in combination with PC in the context of m-banking and its consequences for risk, trust, and intention to use.

PMT is naturally suited to information security contexts in which fear motivates users to protect their information assets (Boss, Galletta, Lowry, Moody, & Polak, 2015); however, we propose that it can also be meaningfully applied to a privacy context. On the one hand, the two contexts of privacy and security are closely related. Specifically, when considering information privacy as control over access to information, security represents a means of achieving privacy (Miyazaki & Fernandez, 2001). However, security can also be viewed as a means of invading privacy, as is the case in arguments about the tradeoff of privacy vs. security, according to which if people want to feel secure, then they must accept being monitored, which necessarily implies a privacy intrusion.[1] Arguably, privacy and security are neither the same nor two opposite concepts: they are related but different. Information privacy is more than control over access to information – it is a more nuanced concept in which all-or-nothing security solutions are not useful. In many circumstances, for instance, people would be fine sharing their information with someone for a specific purpose, but they would not want that information to be used for other purposes (Belanger & Xu, 2015; Martin & Shilton, 2016; Nissenbaum, 2004). Consider financial information: people are comfortable with their bank accessing this information so that it can provide them with financial services; however, they may not be comfortable with that information being used for marketing purposes, such as promoting third-party services. Thus, people may not be concerned about the security measures that the bank applies in regard to protecting the confidentiality, integrity, and availability (the three pillars of information security) of their information, but they may have PC associated with how that information is used. The similarities and distinctions between privacy and security make a theoretical framework previously applied to security, such as PMT, potentially but not trivially useful for privacy as well. It is crucial to understand not only the nature of PC but also the reason why people make certain privacy-related decisions for models to be useful for prediction (Bélanger & Crossler, 2011). This security context involves emotional reactions from individuals and thus a study on the subject is needed.

We tested our model in four different studies (grouped in three papers): two online surveys, one online experiment, and one lab experiment using emotion detection technology. We addressed four gaps found in the IS literature: (1) the lack of a real-time and noninvasive technique for measuring fear; (2) the omission of a full nomology of PMT as an antecedent of PC; (3) the omission of fear appeal manipulations in the privacy context; and (4) no reuse of the most up-to-date PC scale as initially conceptualized by Hong and Thong (2013).

[1] For instance, see: https://www.wired.com/2008/01/securitymatters-0124/.

We found that the majority of PMT constructs and the emotion of fear, never studied before in the context of privacy, influence PC. The implication is that when an m-banking user is stimulated by a fear appeal message, the fear of losing information increases, consequently activating PC and inducing the user to use this platform more securely.

1.1 Research Objectives

As a general objective, this study intends to propose a model to contribute to Information Privacy Concerns literature, specifically regarding the use of financial information.

To meet that general objective, this study has three specific aims:

a) Perform a literature review about Information Privacy Concerns considering the scales, the antecedents, the outcomes, and the theories/practices that support the constructs.

b) Identify, test and validate a scale for the core construct of the model, denominated as MBIPC;

c) Conduct surveys and experiments to empirically test the nomological network of the construct, by manipulating some factors that encourage or inhibit individuals to securely use m-banking technology.

1.2 Justification and Relevance

Regarding the challenging scenario that individuals and organizations are facing, with a massive and growing volume of data breaches and privacy invasions, the relevance of this study is founded on three major pillars: theoretical, individual and organizational.

From the theoretical point of view, the relevance of the present study lies in the proposal of a model for MBIPC and a test for its effectiveness. Although the information system literature has already proposed other models, we shed light on a new construct that may help in future studies about Information Privacy, since we still don't have a specific scale to measure privacy concerns about m-banking technology.

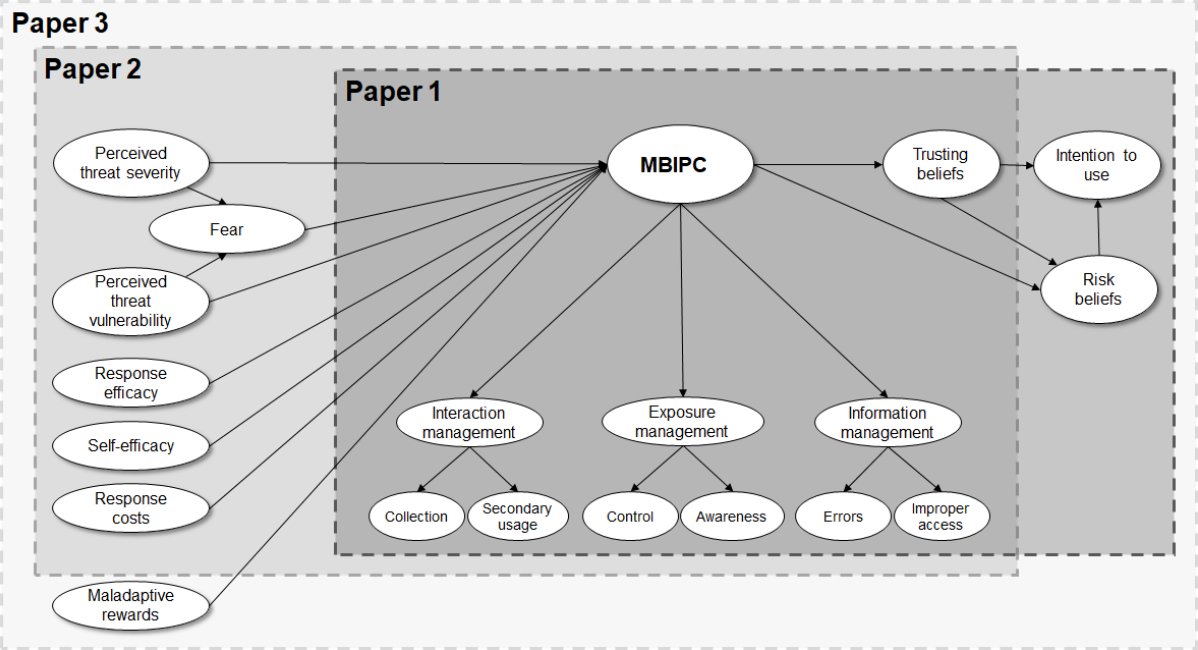
From the individual perspective, the relevance is justified by the personal security aspect, since the disclosure of sensitive information, like financial information, could harm the individual financially, physically or socially. Additionally, individual behavior is the most vulnerable link in an information security system that can be exploited by scammers using social engineering (exploitation of humans to gain unauthorized access to sensitive information using social interaction and a computer-related entity).

Finally, considering that Information Privacy is also a discipline focused on practice and that organizations have a great interest in protecting their consumers' sensitive data, this study contributes to a practice perspective. Being so, based on the MBIPC construct here proposed, we expect that FSI will be able to identify some key elements to improve their policies and processes to enhance the protection of customers' sensitive data.

1.3 Dissertation Structure

The core of this dissertation is a set of three papers that address the nomological network for MBIPC. In order to better describe each part of the nomological network, the proposed model was sliced into three sections and presented in each paper (Figure 1).

Figure 1 – Proposed model.



The first paper focused on the MBIPC scale, that is a conceptual replication of the work of Hong and Thong (2013), who developed the Internet Privacy Concerns (IPC) scale to measure individuals' concerns regarding how personal information is handled by websites. We adapted the wording of the original survey items to the context of mobile banking and followed the same procedures to assess the scale. We tested our research model in an online survey with 378 Americans from Amazon Mechanical Turk. In contrast with the original study, however, we detected a high correlation between the Control and Awareness dimensions, suggesting the design of an additional second-order dimension that we labeled as "exposure management" (individuals' consciousness about existing controls that mitigate the risks of personal data loss).

The second paper partially assessed our proposed model. It examined the influence of PMT (partial nomology) on MBIPC and the consequences of this influence on trust. We tested our research model in an online survey with 351 American m-banking users from Amazon Mechanical Turk. We addressed two literature gaps: the omission of fear in PMT as an antecedent of PC; and no reuse of the most up-to-date PC scale (IPC) as initially conceptualized – IPC have been cited in 54 papers at Web of Science, but none of them used the original and third-order factor scale. We found that the fear of losing information from m-banking activates PC and induces the user to trust less this platform.

The third paper assessed the full proposed model. It examined the influence of PMT (full nomology) on MBIPC and the consequences of this influence in trust, risk, and intention to use. We tested our model in two different studies, one lab experiment using emotion detection technology and one online experiment. We addressed four literature gaps: the lack of real-time

technology for measuring fear; the omission of a full nomology of PMT as an antecedent of PC; the omission of fear appeal manipulations in PC; and no reuse of the most up-to-date PC scale (IPC). We found that when an m-banking user is stimulated by a fear appeal message, the fear of losing information increases, consequently activating PC and inducing the user to use the platform more securely. We also contributed to the privacy literature by motivating and studying the relationship between fear and PC.

Lastly, the final chapter presents a general conclusion of the study.

2. PAPER 1: Internet Privacy Concerns – Scale Adaptation and Validation for the Mobile Banking Context

2.1 Introduction

> *Information privacy can be defined as the ability of the individual to control personally (vis-a-vis other individuals, groups, organizations, etc.) information about one's self (Stone, Gueutal, Gardner, & McClure, 1983, p. 460).*

We live in an era where people have to handle so much information that they are likely to lose control of the data they are sharing and be unaware of the consequences. People do not exactly know whether and to what degree they should be concerned about privacy (Acquisti, Brandimarte, & Loewenstein, 2015). This is not a new issue, as the secure storage of a significant amount of personal data in computers and its proper use is a public concern that has been discussed for a long time (Ware, 1973). However, this issue continues to be highlighted as an essential research topic in many disciplines, including economics, law, marketing, psychology, and especially in information systems (Bélanger & Crossler, 2011).

In the last three decades, many studies have been perfecting an instrument to measure information privacy concerns; however, privacy attitudes are often measured in an ad hoc manner using questionnaires instead of reusing measurement instruments (Preibusch, 2013). In their original study, based on Multidimensional Developmental Theory (Laufer & Wolfe, 1977), Hong and Thong (2013) developed a scale to measure individuals' concerns regarding how personal information is handled by websites. They named their instrument Internet Privacy Concerns (IPC). Hong and Thong (2013) identified that, although there was evolving literature on privacy concerns, there was little agreement about its conceptualization regarding its dimensions, factor structure, and the wording of the items used in prior instruments. Thus, after four online surveys involving almost 4,000 Internet users, the authors resolved these discrepancies and demonstrated that the third-order conceptualization of IPC had nomological validity.

Table 1 – Some information privacy concerns scales (chronological order).

Scale	Definition	Based on	Factor Structure	Dimensions	Author(s)
Concerns for Information Privacy	Individual's concerns about organizational information privacy practices.	Prior studies	Reflective 4 first-order	Collection, Errors, Improper Access, and Secondary Usage	(Smith, Milberg, & Burke, 1996)
Concerns for Information Privacy	Consumers' concern for information privacy.	CFIP scale	Reflective 1 second-order with 4 first-order	Collection, Errors, Improper Access, and Secondary Usage	(Stewart & Segars, 2002)
Internet Users' Information Privacy Concerns	The degree to which an Internet user is concerned about online marketers' collection of personal information, the user's control over the collected information, and the user's awareness of how the collected information is used.	Social Contract Theory	Reflective 1 second-order with 3 first-order	Awareness, Collection, and Control	(Malhotra, Sung, & Agarwal, 2004)

Scale	Definition	Based on	Factor Structure	Dimensions	Author(s)
User Privacy Values	The degree to which consumers value information privacy.	The Code of Fair Information Practices	Reflective 6 first-order	Access/Participation, Collection, Information Storage, Notice/Awareness, Personalization, and Transfer	(Earp et al., 2005)
Mobile Users' Concerns for Information Privacy	The interplay between mobiles users and service providers where privacy is concerned.	Communication Privacy Management Theory	Reflective 1 second-order with 3 first-order	Perceived Intrusion, Perceived Surveillance, and Secondary Usage	(Xu, Teo, Tan, & Agarwal, 2012)
Concerns over Collective Privacy on Social Networking Sites	Individual's concerns over collective privacy on social network sites.	Communication Privacy Management Theory	Reflective 1 second-order with 3 first-order	Collective Privacy Access, Collective Privacy Control, and Collective Privacy Diffusion	(Jia & Xu, 2015)
Notes: Col = Collection, Sec = Secondary Usage, Err = Errors, Acc = Improper Access, Con = Control, and Awa = Awareness.					

By analyzing past research (Table 1), we observe indeed some contrasts on the scales that were developed to measure information privacy concerns. The scales were based on different theories and practices, presented a variety of definitions, and were defined using different structures and dimensions. Considering these contrasts, we believe that a replication study is necessary to assess whether the IPC scale is stable over time and applicable to different contexts. We choose IPC because this is the most up-to-date and robust information privacy scale proposed in the Information Systems (IS) field.

The context of m-banking in the U.S. is an ideal scenario to study privacy concerns for some reasons. First, financial information is a highly sensitive type of data (Culnan, 1993; Woodman et al., 1982). Second, the use of m-banking has been growing steadily (McKinsey, 2017). In 2015, 43% of all mobile phone owners in the U.S. with a bank account had used m-banking, up from 39% in 2014 and 33% in 2013 (Fed, 2016). Furthermore, recent headlines have highlighted major data breaches in this industry, including JPMorgan Chase (Ross, 2015), UniCredit Bank (Sirletti & Robinson, 2016) and Equifax (Economist, 2017), raising questions about the capacity of banks, credit bureaus and their partners to protect the privacy of citizens' financial information. Finally, information privacy concerns still constitute one of the leading barriers reported by nonusers for not adopting m-banking (Fed, 2016).

In recent years, some researchers have conducted specific replication studies to validate the applicability of the scales about information privacy concerns in new contexts. For example, Osatuyi (2015) replicated the concerns for the information privacy scale (CFIP) (Smith et al., 1996; Stewart & Segars, 2002) in the context of social media, and Kenny and Connolly (2017) partially replicated IPC using a second-order factor approach in the context of mobile health applications. Our work extends this line of research by assessing and expanding IPC in the context of mobile banking (m-banking)[2] and checking for nomological validity of its third-order

[2] The U.S. Federal Reserve (Fed, 2016, p. 7) defines mobile banking as using "a mobile phone to access your bank or credit union account. This can be done either by accessing your bank or credit union's web page through the web browser on your mobile phone, via text messaging, or by using an app downloaded to your mobile phone."

conceptualization. The reuse of a scale has three advantages: (1) it advances state of the art to build on prior work, (2) it makes high-quality measures available for the current research, and (3) it saves time for the researcher that can be better spent on the original contribution (Preibusch, 2013).

Figure 2 – Results of the original study.

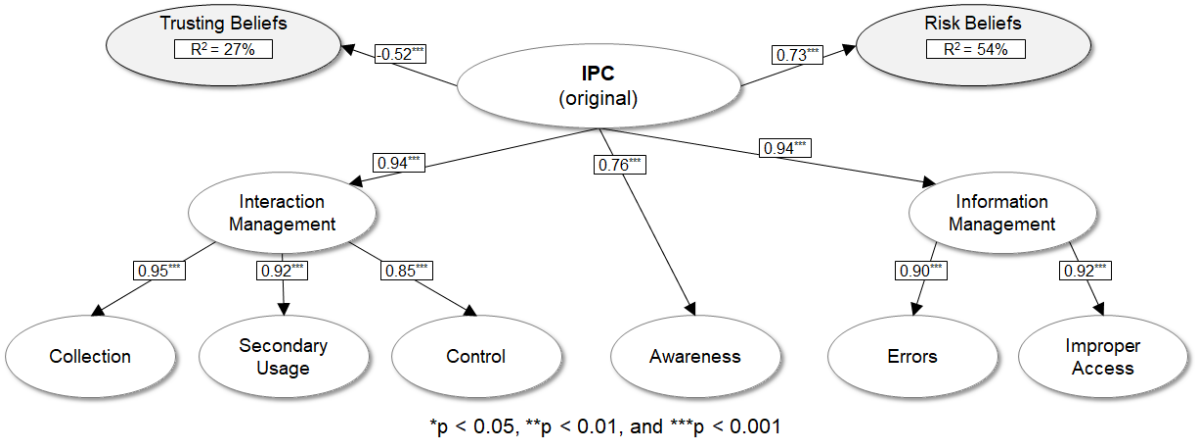


Figure 2 shows the research model, paths, and results from the original study that are part of this replication. The final scale of IPC proposed a third-order factor with two new second-order factors: (1) interaction management – the ability of an individual to manage the collection and subsequent use of his or her personal information by websites, and (2) information management – an individual's perception of how websites handle personal data. The results provided evidence that online users with high information privacy concerns have lower trust in how sites handle personal information and perceive higher risk in providing personal information to websites.

2.2 Method

This study is a conceptual replication (Dennis & Valacich, 2014), of the work of Hong and Thong (2013) in which we adapt the wording of the survey items that were designed to measure the IPC scale to the context of m-banking and name the revised scale as Mobile Banking Information Privacy Concerns (MBIPC). We address two of the three future directions proposed by Hong and Thong (2013): (1) we reevaluate the lower-order dimensions of privacy concerns on a periodic basis, and (2) we test the conceptualization of the scale in other countries.

Prior literature adapted the context of the information privacy scale by changing some keywords in the survey items. For example, (1) Hong and Thong (2013) changed the term "companies" that was used in the CFIP scale (Smith et al., 1996) to "commercial websites;" (2) Osatuyi (2015), in a replication paper, changed it to "social media sites;" and (3) Kenny and Connolly (2017) used "health care entities" instead. We follow the same rationale and change the term "commercial websites" used in the IPC scale (Hong & Thong, 2013) to "mobile banking apps and websites" (see Appendix A), and obtain additional feedback from five doctoral students on the clarity of the questions and options before deploying the final version.

Hong and Thong (2013) studied several conceptualizations of IPC with four online surveys that were conducted in Hong Kong. Study 1 compares the integrated conceptualization of IPC to two existing conceptualizations in the literature. Study 2 replicates the study on a different sample and confirms the results of study 1. The final instrument was validated in study 3 (n = 992) and cross-validated in study 4 (n = 887). Consistent with the original study, we execute the same procedures and validate the final instrument used in studies 3 and 4, as well as its nomological network (the relationships between MBIPC, trusting beliefs and risk beliefs).

In order to study the stability of the scale and its applicability in a different culture, we recruit online participants from Amazon Mechanical Turk restricting participation to U.S. residents, with the intention of generalizing the results to the U.S. population (Steelman, Hammer, & Limayem, 2014). We compensate participants $0.6 for completing the study.

The recruitment of participants from the MTurk platform is motivated by the fact that MTurk workers are experienced Internet users, and are thus likely to have experience in online activities. This is the population we need to target in order to study a context such as mobile banking, which requires at least some familiarity with online activities. Furthermore, MTurk has been shown to be a reliable source for high-quality and representative data for various fields and research purposes (Paolacci, Chandler, & Ipeirotis, 2010).

A priori sample size calculations[3] were performed using Westland (2010) formulas to ensure that the study sample size was adequate to detect the same effect size of the original study. Under the conditions of the original study (effect size: 0.52, desired statistical power level: 0.8, probability level: 0.05, number of latent variables: 11, and number of observed variables: 26), a minimum sample size of 316 is required. Thus, we recruit 400 participants (Soper, 2018; Westland, 2010).

We remove 22 participants who answered the attention check question incorrectly; this leaves us with 378 responses for analysis. Table 2 provides the demographics of the remaining participants in our study and compares the subject pool to the one recruited by Hong and Thong (2013).

Table 2 – Demographics of samples.

Variables	**Original**		**Replication** Mobile Banking
	Study 3 Commercial Websites	**Study 4** Government Websites	
Sample Size	992	887	378
Country	China (Hong Kong)	China (Hong Kong)	United States
Mean Age	25.13	25.11	Mean 35.3 / Median 37
Sex (Female/Male)	53% / 44%	58% / 40%	57.7% / 42.3%

Our sample size is smaller than Hong and Thong's (2013) study 4, but, as shown above, it is large enough to detect the same effect as the original study. The mean age of the subjects in the replication study is ten years older than in the original research; however, the median age is close to the median age of the U.S. population, which is 37.9, according to the most recent U.S.

[3] https://www.danielsoper.com/statcalc/calculator.aspx?id=89.

Census estimates (Census, 2017). Finally, our replication is composed of a similar percentage of females/males as in the original study 4.

2.3 Results

We use IBM® SPSS® Amos 23 to conduct confirmatory factor analysis (CFA). In the next subsections, we compare our results and contrast them with the original study.

2.3.1 Measurement Model Assessment

We examine our descriptive statistics for the six key dimensions of the original study (Table 3). In the replication study, the means of the collection, secondary usage, errors and improper access constructs are comparable to the ones in the original study. The means of the control and awareness constructs are not as similar; however, they are close to the means of study 3. As in the original study, we calculate the difference between the mean of each dimension and the collection dimension; however, we cannot perform an independent samples t-test comparing the means between the original and the replication study because standard deviations were not reported in the original paper.

Table 3 – Descriptive statistics for the six key dimensions.

Dimension	**Original**				**Replication** Mobile Banking		
	Study 3 Commercial Websites		**Study 4** Government Websites				
	Mean	**Difference**	**Mean**	**Difference**	**Mean**	**Difference**	**Std.Dev.**
Collection	5.45	N/A	4.27	N/A	4.08	N/A	1.59
Secondary Usage	5.75	0.30	4.28	0.01	4.10	0.02	1.68
Errors	5.17	-0.28	4.33	0.06	4.03	-0.05	1.61
Improper Access	5.52	0.07	4.61	0.34	4.58	0.50	1.72
Control	5.30	-0.15	4.12	-0.15	5.25	1.17	1.37
Awareness	5.62	0.17	4.87	0.60	5.19	1.11	1.37

Notes: Difference is calculated by subtracting the mean of each dimension from the mean of the collection dimension (Difference = Mean $_{\text{Dimension}}$ – Mean $_{\text{Collection}}$); Std.Dev. = standard deviation.

Following the procedures of the original study, we implement CFA to examine the factor structures. Considering that study 4 cross-validate study 3, the original study did not publish all measures for study 4, so we compare our measures and fit indices with those of study 3.

Table 4 – Reliability and convergent validity of first-order factors.

Dimensions	**Original – Study 3** Commercial Websites				**Replication** Mobile Banking			
	Mean	**SD**	**Factor Loadings**	**Squared Multiple Correlation**	**Mean**	**SD**	**Factor Loadings**	**Squared Multiple Correlation**
Collection	**C.A. = 0.81; C.R. = 0.81**				**C.A. = 0.91; C.R. = 0.91**			
COL1	5.41	1.02	0.72	0.52	3.74	1.69	0.87	0.76
COL2	5.73	0.95	0.77	0.59	4.42	1.77	0.83	0.68
COL3	5.60	1.03	0.82	0.67	4.09	1.73	0.92	0.86
Secondary Usage	**C.A. = 0.93; C.R. = 0.93**				**C.A. = 0.94; C.R. = 0.94**			
SEC1	5.77	0.98	0.85	0.72	4.08	1.75	0.91	0.83
SEC2	5.71	1.11	0.93	0.86	4.05	1.81	0.91	0.82
SEC3	5.77	1.08	0.94	0.88	4.19	1.79	0.93	0.87

Dimensions	Original – Study 3 Commercial Websites				Replication Mobile Banking			
	Mean	**SD**	**Factor Loadings**	**Squared Multiple Correlation**	**Mean**	**SD**	**Factor Loadings**	**Squared Multiple Correlation**
Errors	**C.A. = 0.91; C.R. = 0.91**				**C.A. = 0.92; C.R. = 0.92**			
ERR1	5.25	1.06	0.86	0.74	4.11	1.69	0.91	0.83
ERR2	5.10	1.07	0.90	0.80	4.02	1.77	0.90	0.82
ERR3	5.16	1.10	0.88	0.78	3.98	1.73	0.87	0.76
Improper Access	**C.A. = 0.94; C.R. = 0.95**				**C.A. = 0.95; C.R. = 0.95**			
ACC1	5.52	1.04	0.91	0.83	4.65	1.76	0.91	0.82
ACC2	5.52	1.05	0.93	0.87	4.55	1.81	0.94	0.88
ACC3	5.54	1.04	0.92	0.85	4.53	1.85	0.94	0.88
Control	**C.A. = 0.95; C.R. = 0.95**				**C.A. = 0.92; C.R. = 0.92**			
CON1	5.38	1.10	0.92	0.84	5.16	1.44	0.90	0.81
CON2	5.33	1.09	0.95	0.89	5.34	1.47	0.93	0.86
CON3	5.21	1.12	0.91	0.84	5.25	1.51	0.86	0.74
Awareness	**C.A. = 0.92; C.R. = 0.92**				**C.A. = 0.91; C.R. = 0.91**			
AWA1	5.53	1.03	0.87	0.76	4.98	1.55	0.81	0.66
AWA2	5.69	1.01	0.92	0.85	5.25	1.46	0.94	0.89
AWA3	5.64	1.02	0.89	0.79	5.34	1.46	0.88	0.78

Notes: The factor loadings are from the confirmatory factor analysis. C.A. = Cronbach's alpha, and C.R. = Composite reliability

Table 4 presents the tests of reliability and convergent validity of the six first-order factors. Cronbach's alphas and composite reliabilities for all of the factors are above 0.80, indicating good reliability for the first-order factors. All factor loadings are higher than 0.80, and the squared multiple correlations between the individual items and their *a priori* factors are high (> 0.65, with the majority being over 0.80), demonstrating high convergent validity.

Table 5 presents tests of the discriminant validity of the six first-order factors. Correlations between factors are lower than the square root of the average variance extracted from the individual factors, thereby demonstrating discriminant validity. Thus, consistent with the original paper, our factors have adequate reliability, convergent validity, and discriminant validity.

Table 5 – Discriminant validity of first-order factors.

Dimensions	Original Study 3	Replication		Correlations (original study in the upper right half of the matrix, and replication study in the lower left half of the matrix)					
	AVE	**AVE**	$\sqrt{AVE}$	**COL**	**SEC**	**ERR**	**ACC**	**CON**	**AWA**
Collection	0.60	0.76	0.872	--	0.67	0.57	0.61	0.63	0.59
Secondary Usage	0.82	0.84	0.916	0.823	--	0.54	0.71	0.60	0.57
Errors	0.77	0.80	0.896	0.647	0.709	--	0.63	0.71	0.56
Improper Access	0.85	0.86	0.929	0.681	0.731	0.788	--	0.62	0.68
Control	0.86	0.80	0.895	0.573	0.582	0.500	0.530	--	0.54
Awareness	0.80	0.78	0.880	0.467	0.516	0.538	0.544	0.753	--
Marker Variable	NA	NA	NA	0.122	0.089	-0.045	0.107	0.090	-0.106

Notes: AVE = Average variance extracted

Based on the uncovering of the six key dimensions in the existing privacy literature, the original study proposed some alternative models of IPC to assess if a third-order factor structure was desirable. Models 3 (six correlated first-order factors) and 4 (second-order factor of IPC on the six first-order factors) are the baseline models, and models 5 to 12 are higher-order

models grounded on the theoretical frameworks identified by multidimensional developmental theory (Laufer & Wolfe, 1977).

In the next step, following the procedures of the original study, we generate and compare goodness-of-fit indices for the two baseline models (models 3 and 4) and the eight alternative models (models 5 to 12). Table 6 presents the comparison of the CFA fit indices between the original study and the replication study. Consistent with the original research, all models show a good fit, with all indices falling within recommended ranges. However, in contrast with the original research where model 12 (one third-order factor) had the best performance, in our research, considering CFI, RMSR, and RMSEA, model 9 (two second-order factors) has the best performance. Thus, we decided to test the structural properties of model 9 in the post hoc analysis section.

Table 6 – Part 1 – Comparative of CFA fit indices between original (study 3) and replication studies.

Fit Indices	**Baseline Models**				**Theoretical Framework 1a**				**Theoretical Framework 1b**			
	Model 3 (6 correlated first-order factors)		**Model 4** (Model 3 with a second-order factor)		**Model 5** (1 second-order factor and 2 first-order factors)		**Model 6** (Model 5 with a third-order factor)		**Model 7** (1 second-order factor and 1 first-order factor)		**Model 8** (Model 7 with a third-order factor)	
	O	**R**	**O**	**R**	**O**	**R**	**O**	**R**	**O**	**R**	**O**	**R**
X^2	378.6	276.6	576.3	459.2	668.5	343.4	551.6	343.3	692.8	459.2	576.3	460.4
Df	120	120	129	129	129	129	128	128	130	130	128	128
X^2 / df	3.16	2.30	4.47	3.56	5.18	2.66	4.31	2.69	5.33	3.53	4.50	3.60
GFI	0.96	0.93	0.94	0.89	0.93	0.91	0.94	0.91	0.93	0.89	0.94	0.89
AGFI	0.94	0.90	0.92	0.85	0.91	0.88	0.92	0.88	0.91	0.85	0.92	0.85
NFI	0.99	0.96	0.99	0.94	0.99	0.95	0.99	0.95	0.99	0.94	0.99	0.094
CFI	0.99	0.98	0.99	0.95	0.99	0.97	0.99	0.97	0.99	0.95	0.99	0.95
RMSR	0.031	0.025	0.050	0.070	0.270	0.039	0.048	0.039	0.260	0.070	0.050	0.070
RMSEA	0.046	0.059	0.059	0.082	0.062	0.066	0.057	0.067	0.064	0.082	0.060	0.083
Notes: O = Original and R = Replication												

Table 6 – Part 2 – Comparative of CFA fit indices between original (study 3) and replication studies.

Fit Indices	**Theoretical Framework 2a**				**Theoretical Framework 2b**				**Indicative of a good fitting model** (Hair, Black, Babin, & Anderson, 2013, p. 584; MacKenzie, Podsakoff, & Podsakoff, 2011, p. 313)
	Model 9 (2 second-order factors and 2 first-order factors)		**Model 10** (Model 9 with a third-order factor)		**Model 11** (2 second-order factors and 1 first-order factor)		**Model 12** (Model 11 with a third-order factor)		
	O	**R**	**O**	**R**	**O**	**R**	**O**	**R**	
X^2	538.8	280.0	490.8	390.8	547.9	421.8	420.2	414.1	NA
Df	127	127	127	127	129	129	127	127	NA
X^2 / df	4.24	2.20	3.86	3.08	4.25	3.27	3.31	3.26	≤ 5
GFI	0.94	0.92	0.95	0.90	0.94	0.89	0.95	0.90	≥ 0.90
AGFI	0.93	0.90	0.93	0.86	0.93	0.86	0.94	0.86	≥ 0.80
NFI	0.99	0.96	0.99	0.95	0.99	0.94	0.99	0.94	≥ 0.90
CFI	0.99	0.98	0.99	0.96	0.99	0.96	0.99	0.96	≥ 0.95
RMSR	0.330	0.026	0.043	0.060	0.330	0.066	0.035	0.068	≤ 0.08
RMSEA	0.055	0.057	0.054	0.074	0.055	0.078	0.049	0.077	≤ 0.06
Notes: O = Original and R = Replication. We consider MacKenzie et al. (2011) a more stringent and updated reference for IS research.									

2.3.2 Structural Model

Following the procedures of the original study, to confirm the nomological validity (Bearden & Netemeyer, 1999; Chin, 1998) of model 12 (final model), we examine the relationship between MBIPC and two theoretically related constructs: trusting beliefs and risk beliefs of m-banking. Privacy concerns are theorized to have a negative relationship with trusting beliefs and a positive relationship with risk beliefs.

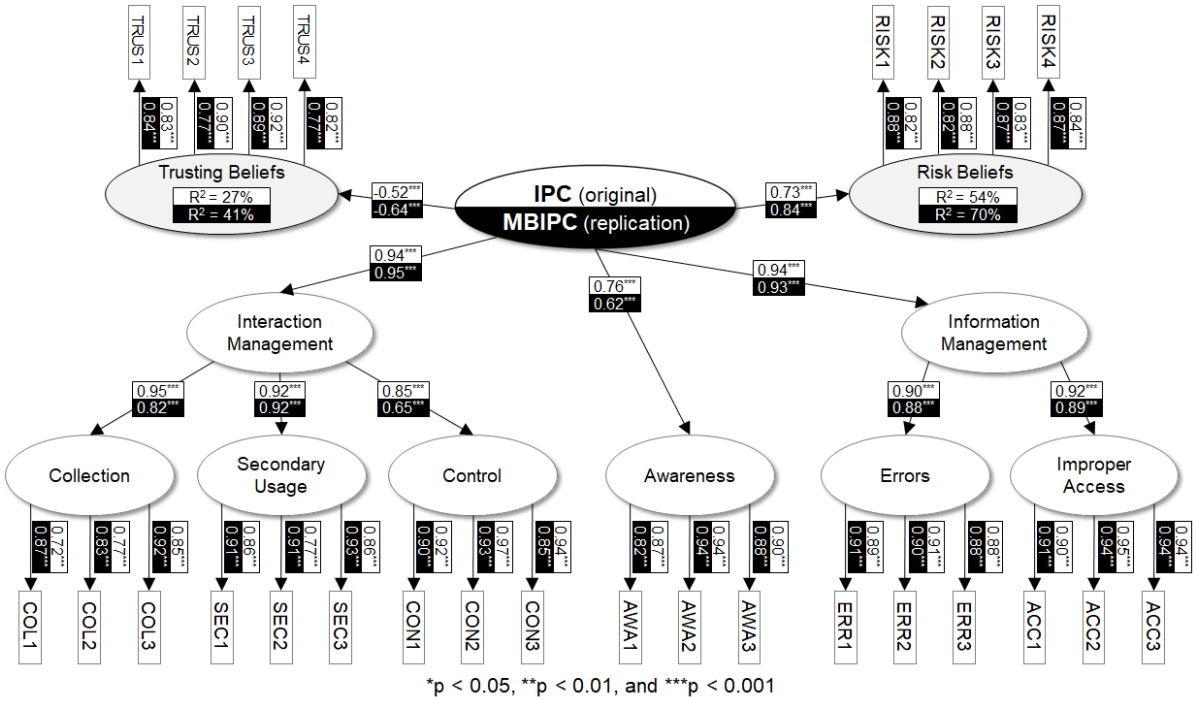
Table 7 – Goodness-of-fit statistics of the original study and replication study.

Fit Indices	Original Study	Replication Study
X^2	1147.17	742.81
Df	289	289
X^2 / df	3.97	2.57
GFI	0.90	0.87
AGFI	0.88	0.85
NFI	0.99	0.92
CFI	0.99	0.95
RMRS	0.008	0.062
RMSEA	0.06	0.06
Nonnormed fit index (NNFI)	0.99	0.95

The structural model's fit indices (Figure 3) are within the recommended ranges, indicating a good fit with the data (Table 7). The only exception is that GFI is below the recommended value of 0.9; however, this can be due to the lower sample size of the replication study. Since the other fit indices, more immune to sample size changes, are within limits, we do not deem this aspect especially concerning. Figure 3 compares the results of the path coefficients, significance and fit indices from the original study with the results of the replication study. The third-order factor explained 41% of the variance in trusting beliefs and 70% of the variance in risk beliefs, which are superior to the original article's, 27% and 54% respectively. Hence, consistent with the original article, we conclude that the third-order factor structure of IPC has good nomological validity.

We conduct the marker variable test (Lindell & Whitney, 2001; Malhotra, Kim, & Patil, 2006) using response costs (Boss et al., 2015) as a marker variable. Correlations between the marker and the dependent variables are small (Table 5), giving a good signal that the marker works. The fact that the signal swings from positive to negative is also good (Lindell & Whitney, 2001, p. 118). We choose $r_{sec\text{-}s}$ (0.089) as the estimator of r_s in equation 4 (Lindell & Whitney, 2001) (the second-least correlation is chosen for a more conservative approach). The results suggest that common method variance does not present a major threat to our analysis.

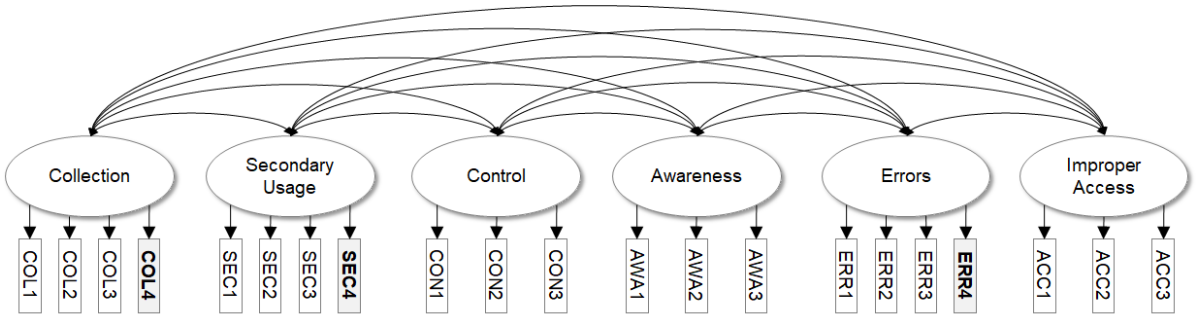
Figure 3 – Results of the original study and replication study.



2.3.3 Post hoc Analysis

As a post hoc analysis to further examine the possible improvements to the original scale, we conduct two additional tests. First, in the original paper, in order to reduce the length of the questionnaire, Hong and Thong (2013) selected the three items from previous literature with the highest loading on each dimension. We test the baseline model 3 (Figure 4) including the extra items that were not used from previous literature (COL4, SEC4, and ERR4) and the model performs worse (see additional indicators on Appendix A), thus supporting Hong and Thong (2013) decision to select only the three items with the highest loadings.

Figure 4 – Alternative model 3B with the items from the prior literature not included in the original paper.



Second, in model 12, we identify a high modification index (113.686) between the residuals of the first-order factors of Control and Awareness, indicating that these two factors are correlated and suggesting the need for an additional second-order factor. Therefore, we create an alternative model 12B (Figure 5) that has a better performance in the measurement model,

very close to our results for model 9. We label this new dimension as "exposure management." We speculate more about this data-driven result in the discussion section.

Figure 5 – Alternative model 12B with a new dimension "exposure management."

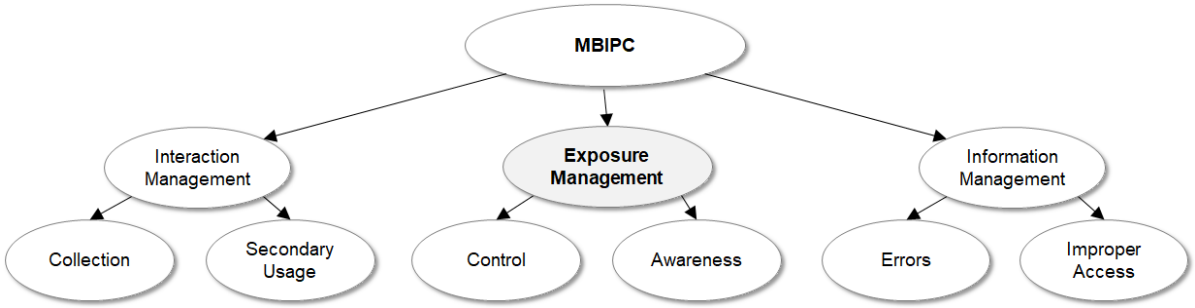


Table 8 – Goodness-of-fit statistics of model 12 and additional model – measurement model.

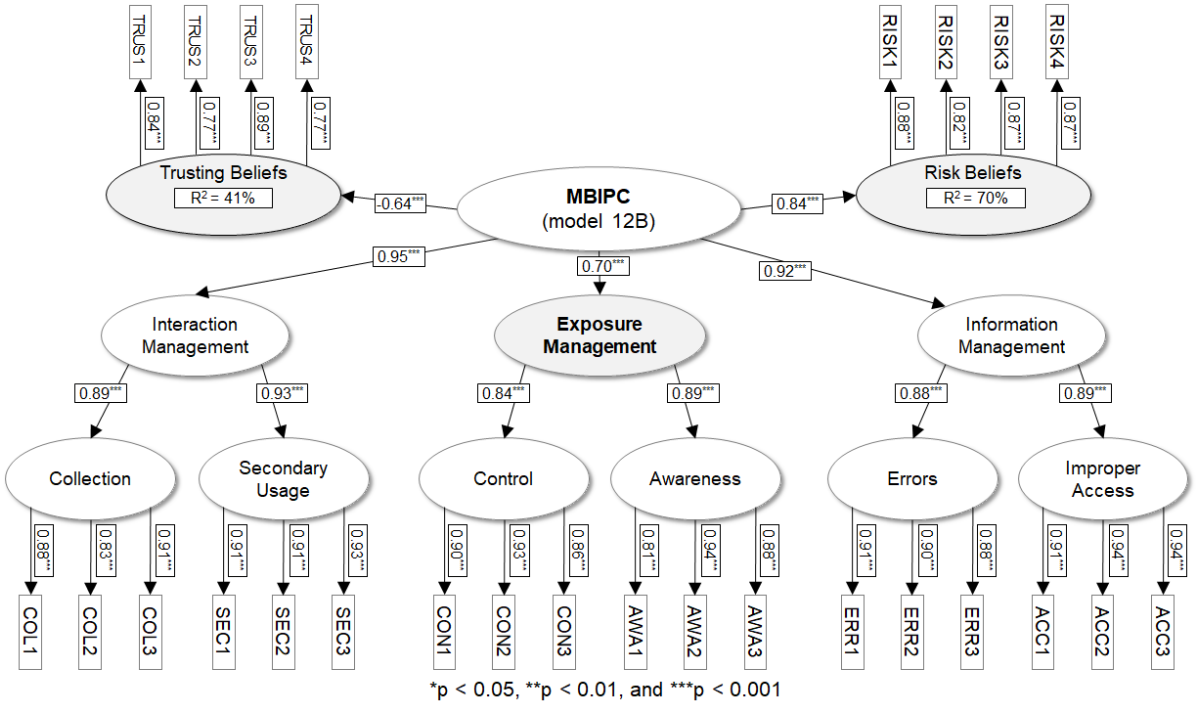
Fit Indices	Original Study	Replication Study		
	Model 12	**Model 12**	**Model 12B** (alternative model)	**Model 9 (best performance)**
X^2	420.18	414.08	293.05	280.02
Df	127	127	126	127
X^2 / df	3.31	3.26	2.33	2.20
GFI	0.95	0.90	0.92	0.92
AGFI	0.94	0.86	0.89	0.90
NFI	0.99	0.94	0.96	0.96
CFI	0.99	0.96	0.98	0.98
RMSR	0.035	0.068	0.030	0.026
RMSEA	0.049	0.077	0.059	0.057

Next, we test models 9 and 12B in the structural model and compare them to model 12 (final model with the best performance in the original study). Model 12B (Table 9 and Figure 6) presents the best performance, surpassing model 9 (Table 9) and corroborating our proposal to create a new second-order factor.

Table 9 – Goodness-of-fit statistics of model 12 and additional model – structural model.

Fit Indices	Original Study	Replication Study		
	Model 12	**Model 12**	**Model 12B best performance**	**Model 9**
X^2	1147.17	742.81	616.45	739.93
Df	289	289	288	289
X^2 / df	3.97	2.57	2.14	2.56
GFI	0.90	0.87	0.89	0.87
AGFI	0.88	0.85	0.87	0.85
NFI	0.99	0.92	0.94	0.93
CFI	0.99	0.95	0.97	0.95
RMSR	0.0083	0.0617	0.0409	0.0605
RMSEA	0.063	0.065	0.055	0.064

Figure 6 – Results of alternative model 12B.



2.4 Discussion

It has been 40 years since Laufer and Wolfe (1977, p. 22) observed that ”if we are to understand privacy as a future as well as a contemporary social issue, we must understand privacy as a concept.” However, understanding privacy as a concept has proven to be a nontrivial task. Defining and measuring privacy is complicated because the relationships depend more on perceptions than on objective assessments. In the IS field, information privacy concerns is the concept that best situates current information privacy issues, and its measurements have been evolving over the years along with new Technologies (Hong & Thong, 2013; Jia & Xu, 2015; Malhotra et al., 2004; Smith et al., 1996; Stewart & Segars, 2002).

In this scenario, replication studies are valuable because they enable IS researchers to validate existing instruments and understand the phenomenon in a new context (Niederman & March, 2015). Therefore, this study fulfills the primary goal of a replication study by assessing the IPC scale developed by Hong and Thong (2013) in the context of m-banking. Additionally, this paper continues the work of Kenny and Connolly (2017), not only using the IPC scale in a different context but also replicating and comparing step-by-step both the measurement and structure of the original study (third-order factor conceptualization). The results of our replication study also confirm the stability of IPC, thereby helping the field to be more confident about the stability and applicability of the scale over the years and in different scenarios.

The original research developed a robust scale summarizing previous literature on information privacy concerns from different fields and tested it in the context of commercial and government websites in Hong Kong. The authors proposed three directions for future research – we address two of them in this study.

First, "reevaluate the lower-order dimensions of privacy concerns on a periodic basis, especially after significant social and technological changes." In our study, we collect the data in March 2018, 5 years after the publication of the original paper. In this period, we witnessed the evolution of m-banking and the broad adoption of this new technology. The use of m-banking surpassed traditional channels, such as telephones, ATMs, and Internet banking. Additionally, a significant number of features that are provided by this technology increased the user's perception of control of his/her financial information (Forrester, 2017).

The second suggested direction for future research was to "test the conceptualization of the scale in other countries (not an Asian country)." In our study, we recruit only U.S. residents 18 years old or older. All states in the U.S. have enacted security breach notification laws requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information (NCSL, 2018). Because of that, it is safe to assume that Americans are quite aware of privacy issues. Furthermore, in recent years, we observed a significant number of data breaches affecting different types and sizes of organizations, including Yahoo, eBay, Target, Uber, U.S. Office of Personnel Management, Sony, Home Depot, Adobe, FedEx, Deloitte, etc. In the financial industry, which is the object of our study, in July 2017, a data breach on Equifax, one of the largest credit bureaus in the U.S., exposed the personal and financial information of more than 140 million American consumers, which was more than 55% of the adult population of the United States at that time (Census, 2017). These large-scale data breaches can be quite costly for a company's customer perceptions in the marketplace (Goode, Hoehle, Venkatesh, & Brown, 2017).

In contrast with the original research where model 12 (one third-order factor) had the best performance, in our research, model 9 (two second-order factors) has the best performance in the measurement model, recognizing the unique roles of control and awareness. Furthermore, in our post hoc analysis, based on model 12, we detect a high correlation between the dimensions of control and awareness and propose an alternative model (12B). We test the structural properties of model 12B, which presents the best performance, surpassing models 9 and 12. We speculate that this correlation is different from the original study because we collect our data sample in another country and almost a decade later. As previously discussed, American citizens are more aware of privacy issues today than ever before due to the existing security breach notification laws. Further, Americans may have an increased perception of the control of their financial data because of the significant number of features offered by m-banking. Thus, we propose a new second-order dimension, named "exposure management," that represents individuals' consciousness about existing controls that mitigate the risks of personal data loss. This new second-order dimension can represent an advance for the information privacy scale in the IS field. We thus call for future studies to consider assessing this alternate proposed conceptualization.

Even though model 9's statistics are marginally better, we believe that our revised model 12B is a better representation of the phenomenon. Individuals are aware that a data breach can lead to identity theft, and they want to be aware of controls to protect their information from being misused, for instance by creating a report on the government online platform identitytheft.gov (FTC, 2017). However, more research is necessary to validate our findings and speculations.

Future studies should also address the third direction proposed by Hong and Thong (2013, p. 294):

> *The integrated conceptualization of IPC can be used in a nomological network to investigate the antecedents and consequences of IPC in a particular research context. For example, it would be interesting to examine the impact of IPC on consumers' online behavior through longitudinal studies.*

2.5 Limitations

Different from the original study that recruited participants by posting a banner on a website, we recruit participants from MTurk (MTurkers).

While the MTurk population may not be entirely representative of the U.S. population, which is the population of interest for our replication, much work has shown that MTurk is a reliable source for high-quality and representative data for various fields and research purposes (Buhrmester, Kwang, & Gosling, 2011; Crump, McDonnell, & Gureckis, 2013; Fort, Adda, & Cohen, 2011; Goodman, Cryder, & Cheema, 2013; Litman, Robinson, & Rosenzweig, 2015; Paolacci & Chandler, 2014; Peer, Vosgerau, & Acquisti, 2014; Rand, 2012; Simcox & Fiez, 2014; Sprouse, 2011). Furthermore, the subjects in our sample are clearly in the population of interest, as all participants are Internet users and reported using m-banking. However, MTurkers are, in many ways, a group of users with unique characteristics, which may limit the generalizability of the findings. Thus, statements about causal relationships that are presented in this model should be tested in different populations in future research.

2.6 Conclusion

Considering the challenging scenario that individuals and organizations are facing, with a massive and growing volume of data breaches and privacy invasions, we understand that it is of vital importance for the academic community to continue replicating and perfecting a scale to measure information privacy concerns over the years. This replication study supports the findings of the original research. It demonstrates that the initially developed scale is stable over time and applicable to different contexts, both technical and cultural. Therefore, we shed light on an adapted instrument that may help in future studies about m-banking and financial information privacy. These future studies can confirm the use of the new proposed dimension of exposure management as a second-order factor. Information privacy concerns may vary geographically but exist across time and culture (Bellman, Johnson, Kobrin, & Lohse, 2004). The disclosure of sensitive information, including financial information, can harm the individual financially, physically, psychologically, or socially, but we remain optimistic that users will continue to adopt m-banking securely.

2.7 Appendix A: Items of MBIPC

We changed the context of the original study from "commercial/government website" to "mobile banking app or website." All items were based on seven-point Likert scales with anchors ranging from 1 (strongly disagree) to 7 (strongly agree).

Collection (COL): The degree to which a person is concerned about the amount of individual-specific data possessed by mobile banking. Based on Hong and Thong (2013) and previously designed by Smith et al. (1996).

COL1: It usually bothers me when **a mobile banking app or website** asks me for personal information.
COL2: When **a mobile banking app or website** asks me for personal information, I sometimes think twice before providing it.
COL3: I am concerned that **a mobile banking app or website** collects too much personal information about me.
COL4[4]**:** It bothers me to give personal information to **many mobile banking apps or websites**.

Unauthorized Secondary Use (SEC): The degree to which a person is concerned that personal information is collected by mobile banking for one purpose but is used for another, secondary purpose without authorization from the individual. Based on Hong and Thong (2013) and previously designed by Smith et al. (1996).

SEC1: I am concerned that when I give personal information to **a mobile banking app or website** for some reason, **that mobile banking app or website** would use the information for other reasons.
SEC2: I am concerned that **a mobile banking app or website** would sell my personal information in their computer databases to other companies.
SEC3: I am concerned that **a mobile banking app or website** would share my personal information with other companies without my authorization.
SEC4[4]**:** **A mobile banking app or website** should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.

Errors (ERR): The degree to which a person is concerned that protections against deliberate and accidental errors in personal data collected by mobile banking are inadequate. Based on Hong and Thong (2013) and previously designed by Smith et al. (1996).

ERR1: I am concerned that **mobile banking apps or websites** do not take enough steps to make sure that my personal information in their files is accurate.
ERR2: I am concerned that **mobile banking apps or websites** do not have adequate procedures to correct errors in my personal information.
ERR3: I am concerned that **mobile banking apps or websites** do not devote enough time and effort to verifying the accuracy of my personal information in their databases.
ERR4[4]**:** All the personal information in computer databases should be double-checked for accuracy – no matter how much this cost.

Improper Access (ACC): The degree to which a person is concerned that personal information held by mobile banking is readily available to people not properly authorized to view or work with the data. Based on Hong and Thong (2013) and previously designed by Smith et al. (1996).

ACC1: I am concerned that **mobile banking databases** that contain my personal information are not protected from unauthorized access.
ACC2: I am concerned that **mobile banking apps or websites** do not devote enough time and effort to preventing unauthorized access to my personal information.
ACC3: I am concerned that **mobile banking apps or websites** do not take enough steps to make sure that unauthorized people cannot access my personal information stored on their computers.

[4] This is the item with lowest loading from the previous literature; it was not included in the original paper to reduce the length of the questionnaire (Hong & Thong, 2013, p. 286).

Control (CON): The degree to which a person is concerned that he/she does not have adequate control over his/her personal information held by a mobile banking. Based on Hong and Thong (2013) and previously designed by Malhotra et al. (2004).

CON1: It usually bothers me when I do not have control of personal information that I provide to **a mobile banking app or website**.

CON2: It usually bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by **a mobile banking app or website**.

CON3: I am concerned when control is lost or unwillingly reduced as a result of a **financial transaction with a mobile banking app or website**.

Awareness (AWA) – The degree to which a person is concerned about his/her awareness of information privacy practices by mobile banking. Based on Hong and Thong (2013) and previously designed by Malhotra et al. (2004).

AWA1: I am concerned when a clear and conspicuous disclosure is not included in the online privacy policies of **mobile banking apps or websites**.

AWA2: It usually bothers me when I am not aware or knowledgeable about how my personal information will be used by **mobile banking apps or websites**.

AWA3: It usually bothers me when **mobile banking apps or websites** seeking my information online do not disclose the ways that the data are collected, processed, and used.

Trusting Beliefs (TRUS) – The degree to which people believe that mobile banking is dependable in protecting individuals' personal information. Based on Hong and Thong (2013) and previously used by Malhotra et al. (2004).

TRUS1: **Mobile banking apps and websites**, in general, would be trustworthy in handling my personal information.

TRUS2: **Mobile banking apps and websites** would keep my best interests in mind when dealing with my personal information.

TRUS3: **Mobile banking apps and websites** would fulfill their promises related to my personal information.

TRUS4: **Mobile banking apps and websites** are in general predictable and consistent regarding the usage of my personal information.

Risk Beliefs (RISK) – The expectation that a high potential for loss is associated with the release of personal information to mobile banking. Based on Hong and Thong (2013) and previously used by Malhotra et al. (2004).

RISK1: In general, it would be risky to give my personal information to **mobile banking apps or websites**.

RISK2: There would be a high potential for loss associated with giving my personal information to **mobile banking apps or websites**.

RISK3: There would be too much uncertainty associated with giving my personal information to **mobile banking apps or websites**.

RISK4: Providing **mobile banking apps or websites** with my personal information would involve many unexpected problems.

3. PAPER 2: Privacy Concerns and Protection Motivation Theory in the Context of Mobile Banking: An Online Survey

3.1 Introduction

> *Information privacy can be defined as the ability of the individual to control personally (vis-a-vis other individuals, groups, organizations, etc.) information about one's self (Stone et al., 1983).*

We live in the age of information, where we have to handle with so much information and so many online platforms that we lose control of what kind of personal data we are sharing, where we are sharing, and why we are sharing. It means that we do not exactly know whether and to what degree we should be concerned about privacy (Acquisti et al., 2015). But this is not a new issue, information privacy is a public concern that has been discussed for a long time (Ware, 1973) and continue to be highlighted as an essential research topic in many disciplines, like economics, law, marketing, and information systems (IS) (Bélanger & Crossler, 2011; Smith, Dinev, & Xu, 2011).

Especially in the IS field, empirical studies usually use the construct "information privacy concerns" (PC) and the "antecedents → privacy concerns → outcomes" (APCO) macro model to explore the relationships between PC and other constructs (Smith et al., 2011; Xu et al., 2011). This model that was initially developed in 2011 was subsequently enhanced by including more recent findings from the behavioral economics literature applied to IS contexts, concluding that little attention has been paid to the antecedents of PC and declaring new propositions for future studies. Our study is inspired by one of these propositions that argue message framing as acting as a peripheral cue which can impact the APCO model constructs (Dinev et al., 2015, p. 647). It means that the message framing might include a fear appeal message and can be investigated by using the protection motivation theory (PMT) as a foundation to explain how privacy threats, with adequate amounts of efficacy, can motivate individuals toward protection from a threat, engaging in beneficial security practices and avoiding harmful ones (Moody, Siponen, & Pahnila, 2018).

Therefore, the purpose of this study is to examine the influence of PMT on PC, including emotional effects of privacy threats, and the consequences of their combined influence on trust, specifically in the context of m-banking. We placed particular emphasis on m-banking users' perceptions regarding the fear of financial data loss. We believe that the context of m-banking[5], in the U.S. is an ideal scenario to study privacy concerns for some reasons:

First, with the massive use of electronic forms of payment, people's financial data provide a complete picture of who they are, exposing a person's lifestyle, hobbies, work, health, and much more. So, it is a consensus among researchers and practitioners that financial information is a highly sensitive data (Culnan, 1993; Woodman et al., 1982) that, if leaked, can be disastrous for individuals and organizations (Goode et al., 2017).

Second, nearly 100% of Americans aged 18 to 29 own a cell phone of some kind (Pew, 2018) and, despite the fact that the use of m-banking has been growing steadily, information

[5] The U.S. Federal Reserve (Fed, 2016, p. 7) defines mobile banking as using "a mobile phone to access your bank or credit union account. This can be done either by accessing your bank or credit union's web page through the web browser on your mobile phone, via text messaging, or by using an app downloaded to your mobile phone."

privacy concerns still constitute one of the leading barriers reported by nonusers for not adopting m-banking. In 2015, 43% of all mobile phone owners in the U.S. with a bank account had used m-banking, up from 39% in 2014 and 33% in 2013 (Fed, 2016; McKinsey, 2017).

Third, the financial service industry, which is the primary industry responsible for protecting citizens' financial data, is one of the largest worldwide investors in technology, with US$ 364 billion in 2016 (Deloitte, 2018) and investments in cybersecurity, privacy and m-banking applications ranked as a top priority (Gartner, 2018). However, recent headlines have highlighted major data breaches in this industry, including JPMorgan Chase (Ross, 2015), UniCredit Bank (Sirletti & Robinson, 2016) and Equifax (Economist, 2017), raising questions about the capacity of banks, credit bureaus and their partners to protect the privacy of citizens' financial information.

We tested our research model in an online survey with 351 American m-banking users from Amazon Mechanical Turk. By doing so, we also addressed two broad gaps in the IS literature: (1) the omission of fear in PMT as an antecedent of PC; and (2) no reuse of the most up-to-date PC scale as initially conceptualized (Hong & Thong, 2013). As an overall result, we found that the fear of losing information from m-banking activates PC and induces the user to trust less in this platform.

This work is structured as follows. Initially, the theoretical background is outlined, including a review of the relevant literature on PMT and PC as well as the study hypotheses. Then, the methodology employed to test the research model is proposed. Finally, the study findings and their implications are discussed. This paper concludes by outlining the limitations and potential directions for future studies in this area.

3.2 Literature Review

In the following sections, we describe the foundations of PC and PMT and the gaps identified in the literature.

3.2.1 Information Privacy Concerns

Privacy was conceptualized in the late 18th century at the individual level as "the right to be left alone" (Warren & Brandeis, 1890). This concept has had an influence on numerous court cases within the US concerning protecting the privacy of individuals (Smith et al., 2011). Later, the concept was explicitly defined for information privacy as the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others (Westin, 1967).

With the introduction of computers, the privacy and security of a significant amount of information stored on electronic devices became a public concern (Ware, 1973). In this way, the concept of information privacy has been highlighted as an essential research topic in many disciplines, including economics, law, marketing, psychology, and, in particular, in the IS field (Smith et al., 2011; Xu et al., 2011). The "antecedents → privacy concerns → outcomes" (APCO) macro model summarized a significant part of the empirical research on PC in IS field and concluded that little attention had been paid to the antecedents of PC (Smith et al., 2011).

However, understanding information privacy as a concept has been proven to be a not trivial task. Defining and measuring information privacy is complicated because the relationships depend more on perceptions than on rational assessments. It is often argued that a universally accepted conceptualization of information privacy cannot be attained due to the varying perspectives from which it is examined. Thus, almost all empirical information privacy research in the social sciences relies on the measurement of a privacy-related proxy of some sort (Xu et al., 2011). Specifically, in the IS field, the proxy that has been proposed to measure information privacy is referred to as information privacy concerns.

3.2.2 Protection Motivation Theory

PMT was initially derived from the expectancy-value theory, which is a social cognition behavioral theory. Since its introduction in 1975, PMT has been widely adopted as a framework for predicting intervention in health-related behavior, and it has been enhanced and extended over time. Rogers (1983) updated PMT to be a more general theory to explain behaviors that avert the consequences of threats; additionally, in 2000, two relevant meta-analyses derived similar overall PMT models (Floyd, Prentice-Dunn, & Rogers, 2000; S. Milne, Sheeran, & Orbell, 2000).

PMT identifies two processes balanced to explain the protection motivation, the threat appraisal process, and the coping appraisal processes. When a potential security threat is discovered, individuals go through a process of first recognizing they are threatened by malicious technology, then coping with the malicious threat and deciding whether they are satisfied with the mitigation or removal of the threat based on their coping process. The threat appraisal process involves the user deciding whether he perceives that he is vulnerable to a given threat (perceived vulnerability) and the severity of the threat (perceived severity). The more serious the threat to an individual is and the more vulnerable s/he is, the more fear will be stimulated (S. Milne et al., 2000). The coping appraisal process involves the user deciding whether a protective action is effective at providing protection from the threat (response efficacy), whether he is capable of performing the protective action (self-efficacy) and if it is worth the perceived cost of doing so (perceived cost) (Floyd et al., 2000).

On the one hand, PMT has been used to propose new information security models (Moody et al., 2018) and explain individual's motivation for applying information security protective behaviors, such as creating backups to protect computing resources, using antivirus and antispyware software, following security policies, and adopting safe behaviors on online platforms (Boehmer et al., 2015; Boss et al., 2015; Y. Chen & Zahedi, 2016; Johnston & Warkentin, 2010; Johnston et al., 2015; Liang & Xue, 2010). On the other hand, PMT has not been fully and accurately used to predict PC (Alashoor et al., 2017; Mohamed & Ahmad, 2012; Seounmi Youn, 2009).

To support our hypothesis development, in Table 10, we first present an overview of the findings of the previous IS literature, demonstrating the relationships and effect direction between PMT constructs and their outcomes.

This overview was particularly important to show the effects of PMT on protective behaviors and intentions are still not very well established or consistent on literature. Except

for fear (only in a positive direction when included), all other constructs have mixed results either with opposite directions and unsupported hypotheses.

Table 10 – Relationship between PMT and outcomes in the IS literature.

PMT and effect direction						Outcomes	Author(s)
Threat			Coping				
PS	PV	Fe	RE	SE	RC		
	+			(-)		PC over social network sites (model 1)	(Alashoor, Han, & Joseph, 2017)
n/s	+		+	+	(-)	Adoption of QR codes as an authentication service	(Yang, Zhang, & Lanting, 2017)
+	+		+	+		Online protective actions	(Y. Chen & Zahedi, 2016)
(-)	+		n/s	+	+	Online unsafety behavior	(Chou & Chou, 2016)
n/s	n/s		+	+	n/s	The protective behavior of securing desktops	(Hanus & Wu, 2016)
(-)	n/s		+	(-)	(-)	Online safety behaviors	(Tsai et al., 2016)
n/s	n/s		+	+		Adoption of security behaviors	(Boehmer, LaRose, Rifon, Alhabash, & Cotten, 2015)
+	+	+	+	+	(-)	Protective behavior (backups in a high fear appeal)	(Boss et al., 2015)
+	n/s		+	+		Compliance with information security policies	(Johnston, Warkentin, & Siponen, 2015)
+	(-)		+	+	(-)	Unified security practices	(Crossler & Bélanger, 2014)
(-)	+		+	+	n/s	Intention to comply with security policies	(Ifinedo, 2012)
+	+		n/s	+		PC with social networking sites	(Mohamed & Ahmad, 2012)
			+	+		Intention to practice safe computing at home	(Anderson & Agarwal, 2010)
(-)	n/s		+	+		Installation of antispyware software	(Johnston & Warkentin, 2010)
+	+		+	+	(-)	Intentions and behaviors to use antispyware	(Liang & Xue, 2010)
+	+		+	+	(-)	Intention to adopt antimalware	(Y. Lee & Larsen, 2009)
	+			n/s		Privacy concerns and protective privacy behavior	(Seounmi Youn, 2009)
n/s	n/s	+	+		(-)	Intention to use strong Passwords	(L. Zhang & McDowell, 2009)
(-)	(-)		(-)	(-)	(-)	Omission of online safety measures	(Workman, Bommer, & Straub, 2008)
	+					Internet PC	(Dinev & Hart, 2004)
+ (-) n/s	+ (-) n/s	+	+ (-) n/s	+ (-) n/s	+ (-) n/s	Summary	

Notes: PS = perceived threat severity; PV = perceived threat vulnerability; Fe = fear; RE = response efficacy; SE = self-efficacy; RC = response costs; n/s = not significant.

3.2.3 Gaps in the PMT and PC Literature

Our literature review identified two relevant gaps.

First, the omission of fear in PMT as an antecedent of PC. In the IS security literature, some researchers have embraced PMT by using parts of it (Anderson & Agarwal, 2010; Y. Chen & Zahedi, 2016; Crossler & Bélanger, 2014; Johnston & Warkentin, 2010), and only two studies adopted fear (Boss et al., 2015; L. Zhang & McDowell, 2009). In the IS privacy literature, we could not find any study that used fear in PMT, which would further our understanding of privacy behaviors (Alashoor et al., 2017).

Second, to our knowledge, there has been no reuse of the most up-to-date PC scale as initially conceptualized. To date, the IPC scale (Hong & Thong, 2013) is the most complete and up-to-date scale in the IS field for measuring PC. IPC, a third-order latent construct, summarized the previous literature on PC from different fields. IPC was tested in the context of websites in Hong Kong in a sequence of four studies with nearly 4,000 participants. Moreover, IPC was partially replicated in the context of mobile health applications using a

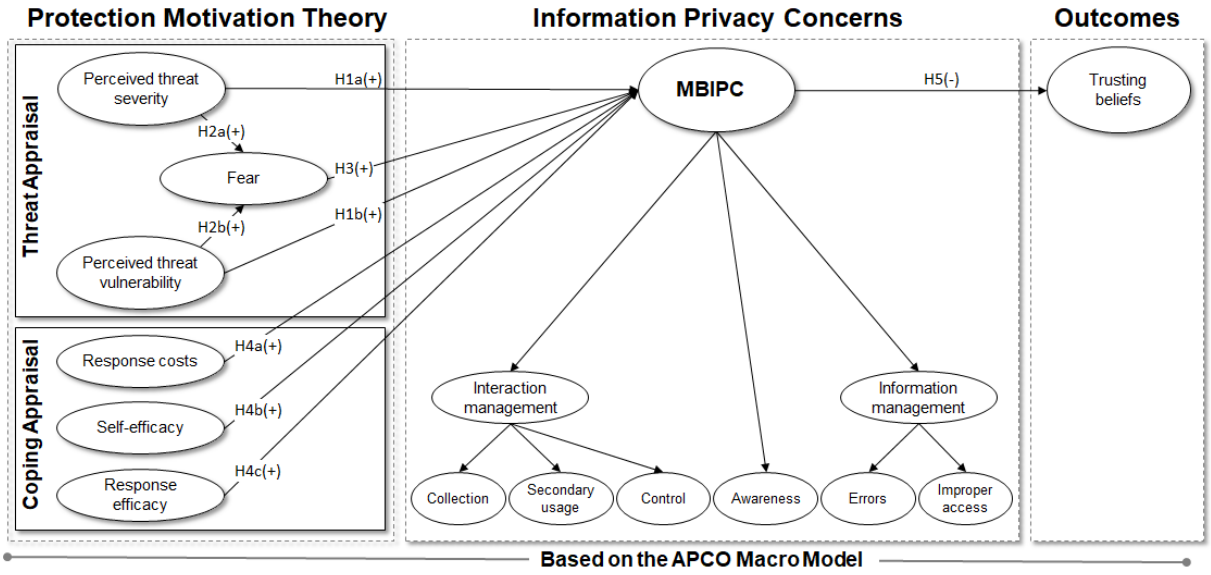
second-order factor approach (Kenny & Connolly, 2017). Although IPC has been cited in 54 papers (Web of Science), none of them used the original and third-order factor scale.

3.3 Research Model

Aligned with the existing literature, we argue that PMT can be theorized as an antecedent of PC. To attend to the purpose of the research and to address the gaps identified, we developed our research model, presented in Figure 7. We first leveraged PMT (antecedents) to model the relationships between the process by which individuals evaluate the threats of data loss from m-banking and PC. Then, still using PMT, we studied how individuals evaluate coping strategies to avoid data loss and their relationships with PC. Finally, we studied the impact of PC on trust to use m-banking (outcomes). The result is a model that allows us to examine the tension between m-banking users' trust in this technology and their concerns about the privacy of their financial information, considering the degree of grave threats and possible coping strategies.

Considering the results shown in Table 10 (some mixed results in opposite directions and some unsupported hypotheses), we based our hypotheses on the foundation of PMT, and below, we explain the concepts of the constructs and the relationships in our model.

Figure 7 – Research model.



3.3.1 Threat Appraisal

A threat appraisal consists of perceived threat severity, perceived threat vulnerability, and fear. Perceived threat severity refers to how dangerous the individual believes that the threat would be to him/herself (S. Milne et al., 2000); from the IS perspective, it is the extent to which an individual perceives that the negative consequences caused by an IT threat are severe (Liang & Xue, 2009). Perceived threat vulnerability refers to how personally susceptible an individual feels to the threat (S. Milne et al., 2000); in the IS context, it is the individual's subjective probability that the IT threat will negatively affect him/her (Liang & Xue, 2009). Reasonably, the more severe the negative consequence of the threat is perceived to be, the more likely that one will be concerned about it. Therefore, we posit the following:

H1a: The perceived threat severity of losing personal information from m-banking will positively influence MBIPC.

H1b: The perceived threat vulnerability of losing personal information from m-banking will positively influence MBIPC.

Combined with severity and vulnerability, fear has a unique role in PMT, as shown in Figure 7. Fear is a negative emotion representing a response that arises from recognizing danger. This response may include any combination of apprehension, fright, arousal, concern, worry, discomfort, or a generally negative mood, and it manifests itself emotionally, cognitively, and physically (Boss et al., 2015). The more vulnerable an individual feels to a threat and the more severe s/he believes it to be real, the more fear will be stimulated (S. Milne et al., 2000). Therefore, threat severity and threat vulnerability predict fear (Floyd et al., 2000). Thus, we hypothesize the following:

H2a: The perceived threat severity of losing personal information from m-banking will positively influence fear of losing personal information.

H2b: The perceived threat vulnerability of losing personal information from m-banking will positively influence fear of losing personal information.

Moreover, the higher the perceived threat and fear, the more likely the individual will be motivated to protect him/herself (S. Milne et al., 2000). Most of the previous IS literature has found that perceived threat severity and perceived threat vulnerability positively increase some data protective behaviors (Table 10). If fear can be realistically measured, then its relationship with PC can also be explored. Therefore, we posit the following:

H3: The fear of losing personal information from m-banking will positively influence MBIPC.

3.3.2 Coping Appraisal

Coping appraisal is the process of considering one's response efficacy, self-efficacy, and the costs of performing the adaptive behavior. The threat and the associated fear can motivate an adaptive behavior if a person feels capable of coping with the threat to mitigate the risk (Floyd et al., 2000). Response efficacy represents the belief that the coping response will work and that taking the protective action will be useful in protecting oneself or others (Floyd et al., 2000). Self-efficacy refers to the perceived ability of a person to carry out the adaptive coping response (Floyd et al., 2000). Finally, response costs are any costs (e.g., monetary, personal, time, effort) associated with taking the adaptive coping response (Floyd et al., 2000).

The previous IS literature has presented some mixed results (Table 10). We argue that individuals who believe in the effectiveness of protective measures (response efficacy) and perceive that they can handle the threatening situation (self-efficacy) are fully aware of the severity and vulnerability of the threat and will thus likely show higher PC. We are not aware of existing literature that studies the effect of response cost on privacy concerns, but on the same vein, we argue that if individuals deem the solution to protect their information to be beyond their resources, like effort, time or money (in our context, it means to take the necessary effort to password protect their mobile devices), then they will be more concerned with the possibility of losing personal and financial data from their mobile devices. We rely on these arguments and hypothesize the following:

H4a: The response costs of protecting personal information while using m-banking will positively influence MBIPC.

H4b: Self-efficacy with regard to protecting personal information while using m-banking will positively influence MBIPC.

H4c: Response efficacy with regard to protecting personal information while using m-banking will positively influence MBIPC.

3.3.3 MBIPC and Trusting Beliefs

In our context, trust represents the degree to which people believe that m-banking is reliable in protecting individuals' personal information (based on Hong and Thong (2013)). Prior studies in information privacy have empirically demonstrated that trust has a negative relationship with PC (Hong & Thong, 2013; Malhotra et al., 2004). Two other examples: (1) individuals with high rates of PC do not trust commercial websites (Metzger, 2004); and (2) as individuals' PC increase, users report registering for websites less frequently and providing incomplete information because they trust less in the website (Sheehan & Hoy, 1999). We replicate these relationships and hypothesize the following:

H5: MBIPC will negatively influence m-banking users' trusting beliefs in the platform.

3.4 Methodology

The model was tested with Amazon Mechanical Turk users (MTurkers), restricting location to U.S. only. We compensated the participants with $1 for completion of the study. MTurkers subjects are appropriate for this context, allowing us to generalize the results to the U.S. population (Steelman et al., 2014). The sample consisted of 351 usable responses (after filtering out 49 participants who either missed attention-checking questions or were not m-banking users). The sample shows 58% male, 87% Employed, and 50% reported a bachelor's degree or higher as their degree of education. They are adults (Mage = 35.3, SD = 9.5) residing in the U.S.

All measures were adapted from prior research. Measures for mobile banking information privacy concerns were operationalized as individual's perception of his or her concern for how personal information is handled by m-banking and was adapted from Hong and Thong (2013). This scale contains a third-order factor with two second-order factors: (1) interaction management – the ability of an individual to manage the collection and subsequent use of his or her personal information by m-banking technologies; and (2) information management – individual's perception of how m-banking technology handles personal data. Measures for protection motivation theory were adapted from Boss et al. (2015), and trusting beliefs from Hong and Thong (2013). The measurement items are declared in Appendix A. In addition to the constructs found within our theoretical model, we also included measures of various demographic variables, such as gender, age, and level of education. For our study, we adapted the wording of the IPC scale (Hong & Thong, 2013) to the context of m-banking. We retained the 18 original items and named the new construct mobile banking information privacy concerns (MBIPC). MBIPC refer to an individual's concerns about how personal and financial information is handled in m-banking.

3.5 Analysis and Results

In this section, we detail the procedures of pre-analysis and data validation undergone to establish construct validity and reliability of the measurement items. After establishing these necessary pre-conditions, we evaluate the proposed model using covariance-based structural equation modeling (CBSEM).

3.5.1 Establishing Construct Validity

Since most constructs and many relationships of the hypothesized in the model were derived from the prior literature, we chose to use confirmatory factor analysis (CFA) to validate the measurement model. CFA is appropriate in situations where theory suggests known relationships among the indicators and their intended factors (Hair et al., 2013). The measurement model exhibited an acceptable fit to the data (χ^2_{782} = 1519.16, $p < 0.001$, χ^2/df = 1.94, CFI = 0.96, RMSEA = 0.052, SRMR = 0.029). "*A cutoff value close to 0.95 for CFI, 0.08 for SRMR, and 0.06 for RMSEA is indicative of a good fitting model*" (MacKenzie et al., 2011, p. 313). Satisfied that the model was acceptable for the preliminary stage, we could then calculate the correlations, reliabilities, and average variance extracted (AVE) values to further aid in establishing factorial validity. These metrics are summarized in Table 11. To demonstrate factorial validity, the AVE for a construct should be > 0.5 (convergent validity). Additionally, discriminant validity is demonstrated when the square root of a construct's AVE is higher than the correlation between that construct and all other constructs in the model. As shown in Table 11, the constructs in the model meet all of these criteria. To establish reliability, the composite reliability (CR) value should be ≥ 0.7 (Fornell & Larcker, 1981). The computed reliability values shown in Table 11 indicate satisfactory reliabilities.

Table 11 – Overall reliabilities, AVE, means, standard deviations, and correlations.

Construct	CR	AVE	Mean	SD	1	2	3	4	5	6	7	8	9	10	11	12	13
1. Severity	.91	.84	3.75	1.59	**.92**												
2. Vulnerability	.93	.86	3.56	1.55	.87	**.93**											
3. Fear	.96	.85	4.00	1.66	.66	.66	**.92**										
4. Response efficacy	.89	.80	6.09	1.14	.01	-.02	.07	**.89**									
5. Self-efficacy	.97	.80	5.65	1.67	.23	.22	.24	.23	**.89**								
6. Response costs	.88	.71	3.47	1.92	.31	.34	.23	-.14	.08	**.84**							
7. Collection	.91	.77	3.96	1.74	.74	.79	.61	.01	.24	.36	**.88**						
8. Secondary usage	.94	.85	4.03	1.79	.76	.77	.61	.05	.29	.33	.85	**.92**					
9. Control	.93	.81	5.15	1.52	.52	.47	.53	.24	.57	.18	.59	.61	**.90**				
10. Awareness	.92	.80	5.10	1.56	.52	.54	.54	.23	.55	.15	.50	.56	.78	**.89**			
11. Errors	.93	.81	4.00	1.75	.75	.77	.61	-.02	.31	.39	.70	.75	.55	.60	**.90**		
12. Improper access	.95	.87	4.47	1.81	.68	.71	.62	.05	.28	.35	.68	.76	.56	.58	.81	**.93**	
13. Trusting beliefs	.93	.78	4.75	1.47	-.62	-.59	-.45	.12	-.14	-.29	-.59	-.58	-.36	-.32	-.60	-.56	**.88**

Notes: N = 351; CR = composite reliability; AVE = average variance extracted; SD = standard deviation; bold values along the diagonal are the square root of the AVE.

3.5.2 Evaluating Common-Method Bias

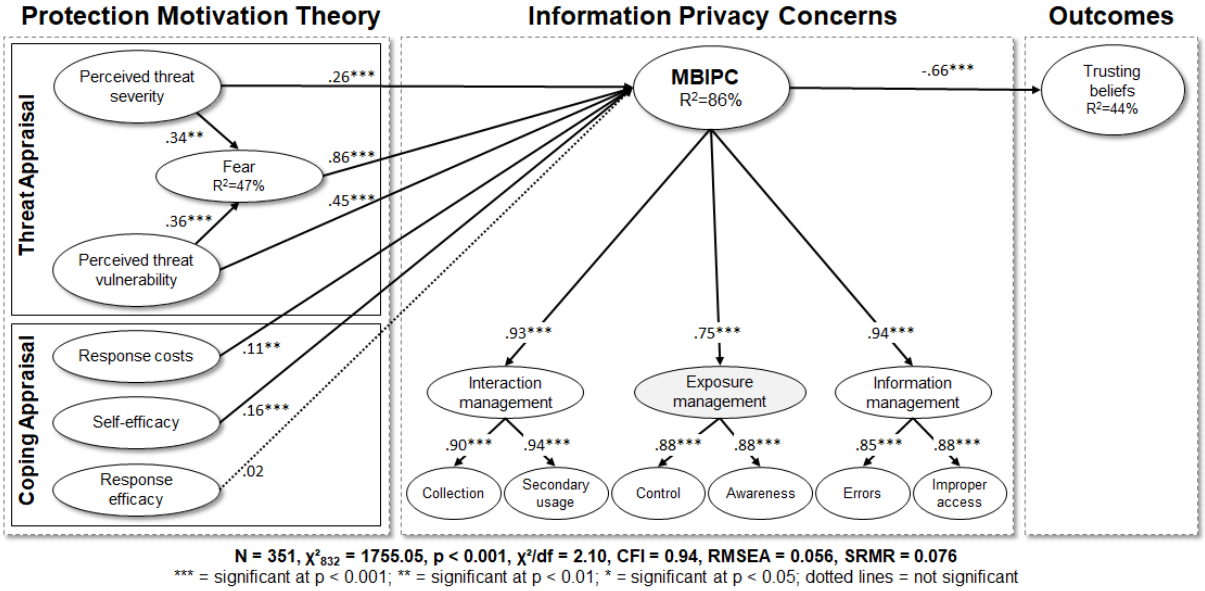
Because all survey items were measured using the same method (an online survey), the possibility exists that some of the shared variances among the constructs are due to the common method rather than the underlying relationships among the constructs. Although precautions were implemented to reduce this likelihood (e.g., randomizing the order of survey items

(Straub, Boudreau, & Gefen, 2004)), it is necessary to test for common method bias in the measurement model. We first note that no correlations shown in Table 11 are above 0.90; correlations above this threshold may indicate common method bias (Pavlou, Liang, & Xue, 2007). A more rigorous approach to testing common-methods bias is the common latent factor method, wherein the influence of a common latent "method" factor on each indicator is modeled, noting any large changes to the loading of each indicator on its corresponding construct. If "large" changes (i.e., > 0.2) are observed, the method factor is retained in the structural model to remove the method's influence from the estimated parameters in the structural model (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). Upon adding the method factor to the measurement model, no changes in standardized item loadings larger than 0.1 in magnitude were observed. We thus conclude that the common method used for measurement did not significantly impact our results.

3.5.3 Model Testing Results

We tested the theoretical model shown in Figure 8 using CBSEM.

Figure 8 – Final Model with SEM Results and a new dimension "exposure management."



The structural model produced generally acceptable indications of fit (MacKenzie et al., 2011). We identified a high modification index (109,586) between the residuals of the first-order factors of control and awareness, indicating that these two factors are correlated and suggesting the need for an additional second-order factor. Therefore, we created an alternative model that had a better performance and labeled this new dimension as "exposure management." The tested hypotheses, along with their corresponding path estimates and significance levels are summarized in Figure 8.

3.6 Discussion

The purpose of this paper was to examine the influence of PMT on PC and the consequences of this influence on trust, specifically in the context of m-banking. We tested our research model

addressing two gaps in the IS literature: the omission of fear in PMT as an antecedent of PC and no reuse of the most up-to-date PC scale as initially conceptualized.

Our model summarized the relationships among self-reported perceived threat severity, fear, perceived threat vulnerability, response costs, self-efficacy, response efficacy, MBIPC, and trusting beliefs. We found that PMT framework that was previously applied to security is also useful to predict privacy concerns. Besides to helping us to understand the factors that influence PC, we identified the role played by fear emotion. This advancement in the literature is significant because little attention has been paid to the antecedents of PC (Dinev et al., 2015; Smith et al., 2011). The fear of losing information from an m-banking activates PC which, in turn, leads the user to trust less in the platform.

3.6.1 Implication for Research

We found empirical evidence that supports and contrasts with the previous literature.

First, despite the fact that privacy concern is intuitively associated with security (Flavián & Guinalíu, 2006) and PMT has been used in the IS security literature, so far, to the best of our knowledge, no previous study has tested fear as an antecedent of PC. Our results provided substantial empirical evidence that MBIPC can be explained by the preconized components threat appraisal and coping appraisal, which leads the user to trust less in the platform (H1a, H1b, H2a, H2b, H3, H5). The positive relationships between perceived threat severity and vulnerability with MBIPC are not surprising and indeed supports prior studies developed in the context of online social networks and websites (Alashoor et al., 2017; Dinev & Hart, 2004; Mohamed & Ahmad, 2012; Seounmi Youn, 2009). Our contribution resides in the fact that we extended previous studies by including all PMT components, especially fear in the model. Moreover, to the best of our knowledge, no existing model deals with the specific characteristics of financial information privacy concerns.

Second, we used the original third-order IPC scale (Hong & Thong, 2013) to measure MBIPC. The results of our study provide evidence of the stability of this measure, helping the field be more confident about the applicability of the scale over time and in different contexts. We improved the scale and the model's performance by adding a second-order factor grouping the first-order factors control and awareness. Hong and Thong (2013) tested eight alternative models before developing the final scale and proposed as a direction for future research to "re-evaluate the lower-order dimensions of privacy concerns on a periodic basis, especially after significant social and technological changes." We addressed this direction in our study. We collected our data several years after the publication of the original paper and in another country. In this period, we witnessed the evolution of m-banking and the massive adoption of this new technology with a significant number of new features that changed the way people bank (Forrester, 2017). Moreover, American citizens are quite aware of privacy issues as compared to the past because the existing security breach notification laws require that organizations notify breaches of personally identifiable information (e.g., Equifax, Yahoo, Target, US Office, and Sony). Therefore, this new second-order dimension, named "exposure management," represents individuals' consciousness about existing controls that mitigate the risks of personal data loss. This new second-order dimension can represent an advance for the

information privacy scale in the IS field, and so we call for future studies to consider assessing this alternate proposed conceptualization.

Third, as hypothesized, response costs and self-efficacy showed significant positive effects on MBIPC (H4a, H4b). These results mean that if individuals cannot afford the costs associated with taking the adaptive coping response, then they will be more concerned with the possibility of losing personal and financial data from their mobile devices. For example, the effort necessary to protect the mobile phone with a password increases MBIPC.

Finally, although the use of a mobile phone password improves the protection of personal information and many previous studies (Table 10) have confirmed a positive relationship between response efficacy and PC (H4c), we did not find support for this hypothesis in the context of m-banking. Considering that consumers usually attribute the responsibility for protecting data to financial institutions (Javelin, 2018), we speculate that m-banking users do not see the mobile password as a safe and effective mechanism to protect the financial data against the current state of threats. Maybe it happens because recent data breaches of financial information, which have affected a significant number of individuals, showed how vulnerable technology is nowadays to prevent data losses. For instance, the 2017 Equifax breach virtually affected all U.S. adults with a Social Security Number. One could argue that there is a tiny point in being concerned about something one has no way to control, so response (in)efficacy in one's coping behavior ends up not affecting PC. Future studies are needed to examine this relationship.

3.7 Limitations and Future Research

Our study is limited to behavior occurring within a single application (m-banking). While the use of m-banking is multiplying and surpassing the use of other banking channels (Fed, 2016), and therefore deserves research focus, these findings may not generalize to other banking channels (e.g., Internet banking, ATM, or call centers) or different mobile payment and digital wallet applications (e.g., PayPal, Samsung Pay, or Apple Pay). Future research should investigate these relationships in other banking channels or financial applications to develop further insights.

Since the majority of studies using PMT was conducted in the IS security field to analyze protection behaviors against threats, the current study was conducted as an exploratory, theory-building effort. It employed a single method to collect data with MTurk, and the subjects in our sample are clearly in the population of interest, as all participants reported using m-banking. However, MTurkers are, in many ways, a group of users with unique characteristics, which may limit the generalizability of the findings. MTurkers are not the only users of m-banking technology, and statements about causal relationships presented in this model should be tested in different populations and perhaps with different methods.

Our proposed model did not support all theorized hypothesizes relationships between PMT and MBIPC (e.g., response efficacy). In our questionnaire, we asked the participants about the use of a password to protect the mobile phone and avoid losing personal information from m-banking. We believe that future studies could adapt the questionnaire and use different security measures or technologies that are perhaps more relevant to users and that are usually used in IS

security research (e.g., using a secure Wi-Fi connection, installing antivirus software, or creating backups).

Lastly, we shed light on an adapted instrument that may help in future studies about m-banking and financial information privacy. These future studies can confirm the use of the new proposed dimension of interaction management as a second-order factor.

3.8 Conclusion

This research uses the PMT and PC literature to examine how perceived threat severity, fear, perceived threat vulnerability, response costs, self-efficacy, and response efficacy impact the potential PC about the use of m-banking. Perceived threats regarding the use of m-banking could stimulate fear and PC, consequently affecting the perception of trust in this technology. We tested our model in an online survey with a sample of 351 MTurkers, restricting the location to the US only. We found strong support for most of the proposed relationships in the study. Our research has significant implications for researchers interested in privacy issues related to m-banking technology. The FSI can also benefit from this research, as our findings indicate the importance of secure privacy-related behaviors in the trust of m-banking systems.

3.9 Appendix A: Measurement Items

Table 12 – Measurement items.

Construct	**Items**
Perceived threat severity	If I were to lose information from m-banking, I would suffer many pains.
	Losing information from m-banking would cause me major problems.
Perceived threat vulnerability	My chances of losing information from m-banking in the future are high.
	I am likely to lose information from m-banking in the future.
Fear	I am frightened about the prospect of losing information from m-banking.
	I am anxious about the prospect of losing information from m-banking.
	I am worried about the prospect of losing information from m-banking.
	I am scared about the prospect of losing information from m-banking.
Response efficacy	Password protecting my phone is a good way to reduce the risk of others stealing my information.
	If I were to change my phone password once a month, I would lessen my chances of data loss.
Self-efficacy	I could password protect my phone if I had only the manual for reference.
	I could password protect my phone if I had seen someone else doing it before trying it myself.
	I could password protect my phone if I could call someone for help if I got stuck.
	I could password protect my phone if someone else helped me get started.
	I could password protect my phone if I had a lot of time to complete the job.
	I could password protect my phone if I had just the built-in help for assistance.
	I could password protect my phone if someone showed me how to do it first.
	I could password protect my phone if I had used similar phones like this one before to do the job.
Response costs	I would be discouraged from changing my phone's password during the next month because it would take too much time.
	Taking the time to change my phone's password during the next month would cause me too many problems.
	I would be discouraged from changing my phone's password at least once a month because I would feel silly doing so.
Collection	It usually bothers me when an m-banking asks me for information.
	When an m-banking asks me for information, I sometimes think twice before providing it.
	I am concerned that an m-banking collects too much information about me.

Construct	Items
Secondary use	I am concerned that when I give information to an m-banking for some reason, that m- banking would use the information for other reasons.
	I am concerned that an m-banking would sell my information in their computer databases to other companies.
	I am concerned that an m-banking would share my information with other companies without my authorization.
Control	It usually bothers me when I do not have control of information that I provide to an m-banking.
	It usually bothers me when I do not have control or autonomy over decisions about how my information is collected, used, and shared by an m-banking.
	I am concerned when control is lost or unwillingly reduced as a result of a financial transaction with an m-banking.
Awareness	I am concerned when a clear and conspicuous disclosure is not included in the online privacy policies of an m-banking.
	It usually bothers me when I am not aware or knowledgeable about how my information will be used by an m-banking.
	It usually bothers me when an m-banking seeking my information online do not disclose the way the data are collected, processed, and used.
Errors	I am concerned that an m-banking does not take enough steps to make sure that my information in their files is accurate.
	I am concerned that an m-banking does not have procedures to correct errors in my information.
	I am concerned that an m-banking does not devote enough time and effort to verifying the accuracy of my information in their databases.
Improper access	I am concerned that m-banking databases that contain my information are not protected from unauthorized access.
	I am concerned that an m-banking does not devote enough time and effort to preventing unauthorized access to my information.
	I am concerned that an m-banking does not take enough steps to make sure that unauthorized people cannot access my information stored on their computers.
Trusting beliefs	M-banking, in general, would be trustworthy in handling my information.
	M-banking would keep my best interests in mind when dealing with my information.
	M-banking would fulfill their promises related to my information.
	M-banking is in general predictable and consistent regarding the usage of my information.

4. PAPER 3: Fear of Losing Financial Information? Privacy Concerns and Protection Motivation Theory in the Context of Mobile Banking: Two Integrated Experiments.

4.1 Introduction

Mobile banking (m-banking), defined as the use of a mobile device to access a bank or credit union account, can be performed by accessing the service provider's webpage through the web browser on a mobile device, via text messaging, or by using an app downloaded to a mobile device (Fed, 2016). Mobile devices allow people to conveniently execute financial operations while reducing the costs to the financial service industry (FSI), which continues to invest in offering user-friendly applications (Forrester, 2017; Gartner, 2018). In 2017, the FSI spent US$ 364 billion worldwide on information technology (IT), or 13% of the world's total investments in IT (Deloitte, 2018, p. 5).

These investments are crucial for supporting rapid growth in the adoption of smartphones for financial services. Presently, nearly 100% of Americans aged 18 to 29 own a cell phone of some kind (Pew, 2018), and together with this massive adoption of mobile devices, there has been a move toward using mobile devices for financial services. Since 2011, the US Federal Reserve System (Fed, 2016) has been conducting an annual study to examine trends in the adoption and use of m-banking and how the evolution of mobile financial services affects consumers' interaction with financial institutions. The last published study identified that 53% of smartphone owners with a bank account had used m-banking in the 12 months prior to the survey.

The growth in the use of m-banking attests to the significant convenience of such a service; however, it also enables increased opportunities for fraud. Information systems (IS)-based financial fraud has become a major problem in recent years. In 2017, 16.7 million US consumers were victims of identity fraud, with the amount stolen reaching $16.8 billion. In the same vein, account takeover, or the use of another person's account information (e.g., a credit card number) to obtain products and services using that person's existing accounts, tripled over the past year, reaching $5.1 billion, and it continues to be one of the most challenging fraud types for consumers, with victims paying an average of $290 in out-of-pocket costs and spending 16 hours, on average, to resolve (Javelin, 2018).

Consumers usually attribute the responsibility for preventing fraud and data breaches to financial institutions (Javelin, 2018). Although technology has traditionally been blamed for showing some vulnerabilities, the literature recognizes that human behavior is still the most vulnerable link, as it facilitates the discovery of personal identity, account numbers, and passwords, thus often leading to successful financial scams (Abawajy, 2014; Malcolm et al., 2012; Terlizzi et al., 2017). Additionally, it is known that individuals are in a better position to deter technology-based fraud when they are concerned about revealing their personal information (Earp et al., 2005). Although not disclosing personal information is a critical behavior in defending one's financial assets from being misappropriated, this protective practice also prevents individuals from using financial systems in general and, in particular, from adopting m-banking (Fed, 2016).

Although they might decrease technology adoption, privacy concerns (PC), or concerns about how personal and financial information is handled by different platforms or technologies, can drive positive attitudes toward reducing vulnerabilities. Examples include avoiding the exposure of passwords, avoiding the use of public Wi-Fi networks, enrolling to receive messages about unauthorized account changes, and adopting antivirus software. The factors affecting and affected by PC are complex and require a thorough investigation (Dinev et al., 2015; Xu et al., 2011). Given the growth in the number of users of m-banking and the economic importance of the sector, this context is of particular interest. The purpose of this study is to examine the influence of Protection Motivation Theory (PMT) on PC and the consequences of this influence on intention to use, specifically in the context of m-banking.

PMT is naturally suited to information security contexts in which fear motivates users to protect their information assets (Boss et al., 2015); however, we propose that it can also be meaningfully applied to a privacy context. On the one hand, the two contexts of privacy and security are closely related. Specifically, when considering information privacy as control over access to information, security represents a means of achieving privacy (Miyazaki & Fernandez, 2001). However, security can also be viewed as a means of invading privacy, as is the case in arguments about the tradeoff of privacy vs. security, according to which if people want to feel secure, then they must accept being monitored, which necessarily implies a privacy intrusion.[6] Arguably, privacy and security are neither the same nor two opposite concepts: they are related but different. Information privacy is more than control over access to information – it is a more nuanced concept in which all-or-nothing security solutions are not useful. In many circumstances, for instance, people would be fine sharing their information with someone for a specific purpose, but they would not want that information to be used for other purposes (Belanger and Xu 2015; Martin and Shilton 2016; Nissenbaum 2004). Consider financial information: people are comfortable with their bank accessing this information so that it can provide them with financial services; however, they may not be comfortable with that information being used for marketing purposes, such as promoting third-party services. Thus, people may not be concerned about the security measures that the bank applies in regard to protecting the confidentiality, integrity, and availability (the three pillars of information security) of their information, but they may have PC associated with how that information is used. The similarities and distinctions between privacy and security make a theoretical framework previously applied to security, such as PMT, potentially but not trivially useful for privacy as well. It is crucial to understand not only the nature of PC but also the reason why people make certain privacy-related decisions for models to be useful for prediction (Bélanger & Crossler, 2011). In addition to contributing to a better theoretical understanding of the PC construct, this work contributes to the emerging privacy literature on the role of emotions (H. Li, Sarathy, & Zhang, 2008), intended as an induced affective state (P. Zhang, 2013) – specifically, in this work, fear – in privacy decision making.

Differently from the second paper, in the third paper, we assessed the full proposed model and tested its stability in different situations using other research methodology (experiment) and new samples. For that, we tested our model in two different studies using deception: one

---

[6] For instance, see: https://www.wired.com/2008/01/securitymatters-0124/

lab experiment using emotion detection technology, and one online experiment. We addressed four gaps found in the IS literature: (1) the lack of a real-time and noninvasive technique for measuring fear; (2) the omission of a full nomology of PMT as an antecedent of PC; (3) the omission of fear appeal manipulations in the privacy context; and (4) no reuse of the most up-to-date PC scale as initially conceptualized (Hong & Thong, 2013).

We found that the majority of PMT constructs and the emotion of fear, never studied before in the context of privacy, influence PC. The implication is that when an m-banking user is stimulated by a fear appeal message, the fear of losing information increases, consequently activating PC and inducing the user to use this platform more securely.

This work is structured as follows. Initially, the theoretical background is outlined, including a review of the relevant literature on PMT and PC as well as the study hypotheses. Then, the methodology employed to test the research model is proposed. Finally, the study findings and their implications are discussed. This paper concludes by outlining the limitations and potential directions for future studies in this area.

4.2 Background

The "antecedents → privacy concerns → outcomes" (APCO) macro model summarized a great part of the empirical research on PC and concluded that little attention had been paid to the antecedents of PC (Smith et al., 2011). This model was subsequently enhanced by including more recent findings from the behavioral economics literature applied to IS contexts, and new propositions have been declared. For example, "message framing acts as a peripheral cue and can impact the APCO model constructs" (Dinev et al., 2015, p. 647), where the message framing might include a fear appeal message. Aligned with the existing literature, we argue that PMT can be theorized as an antecedent of PC. In the following sections, we describe the foundations of PMT and PC and the gaps identified in the literature.

4.2.1 Protection Motivation Theory

PMT was initially derived from the expectancy-value theory, which is a social cognition behavioral theory. Since its introduction in 1975, PMT has been widely adopted as a framework for predicting intervention in health-related behavior, and it has been enhanced and extended over time. Rogers (1983) updated PMT to be a more general theory to explain behaviors that avert the consequences of threats; additionally, in 2000, two relevant meta-analyses derived similar overall PMT models (Floyd et al., 2000; S. Milne et al., 2000) (Figure 9 and Figure 10).

PMT identifies two cognitive processes that are stimulated by a fear appeal and that are expected to play an essential role in protection motivation, specifically the threat appraisal process and the coping appraisal process. A fear appeal is a communication about a threat with suggestions about measures to mitigate its impact (S. Milne et al., 2000). Threat appraisal is the process of considering the severity of and vulnerability to a threat against the rewards associated with maladaptive behavior, such as saving time or avoiding trouble by not adopting the protective behavior (Floyd et al., 2000). The more serious the threat to an individual is and the more vulnerable s/he is, the more fear will be stimulated (S. Milne et al., 2000). Coping

appraisal is the process of considering one's self-efficacy, response efficacy, and the costs of performing the protective behavior (Floyd et al., 2000).

Figure 9 – The overall model of PMT (Floyd et al., 2000).

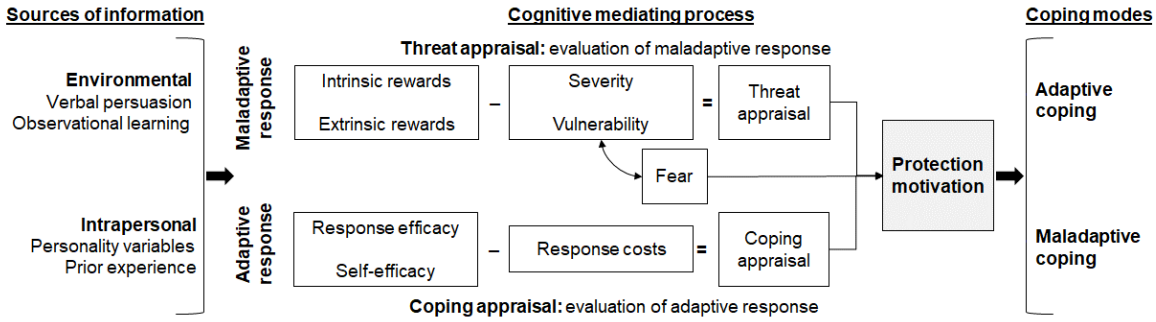
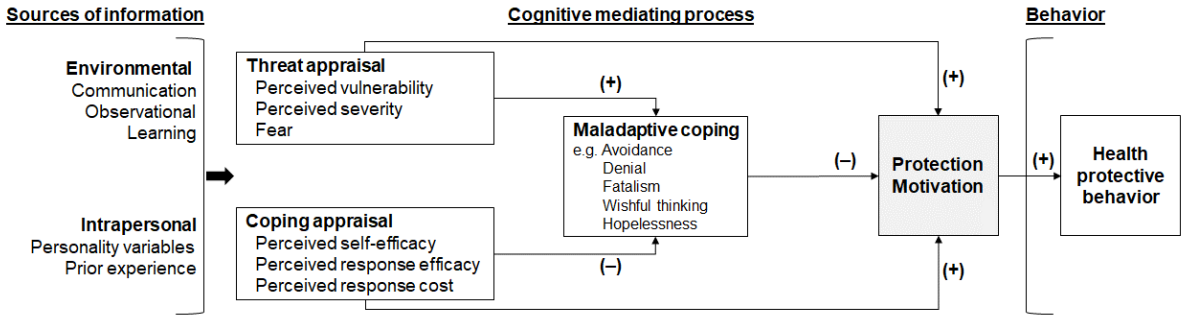


Figure 10 – The overall model of PMT (Milne et al., 2000).



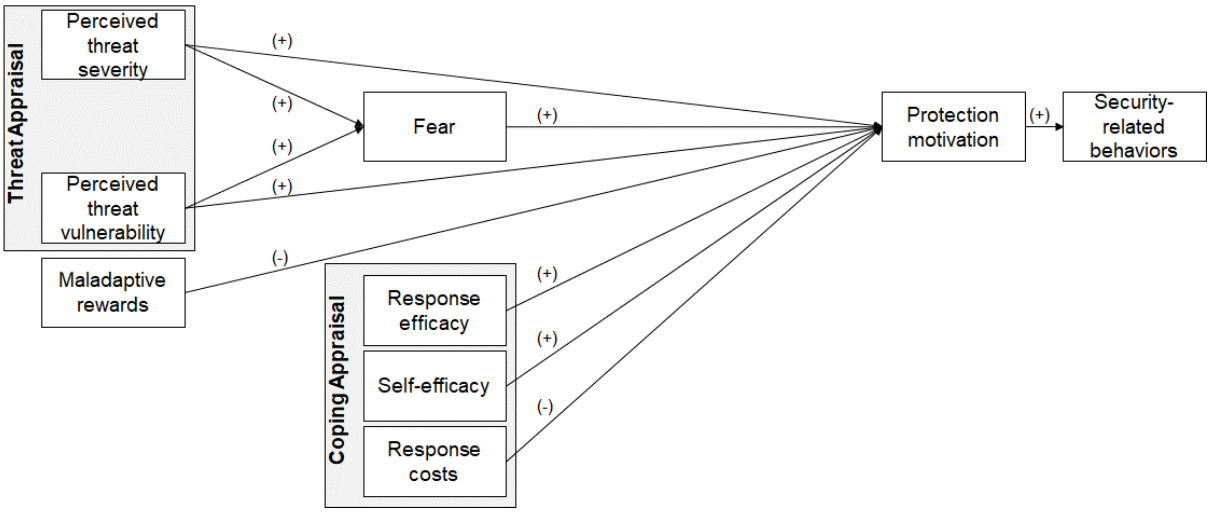
To illustrate this concept (Crossler, Long, Loraas, & Trinkle, 2014; S. Milne et al., 2000), consider a scenario in which a health education pamphlet (fear appeal) explains that increased exposure to the sun can cause skin cancer (threat appraisal) but using sunscreen reduces the probability significantly (coping appraisal). When determining whether to use sunscreen to prevent skin cancer (behavior or intention), an individual considers the probability of contracting skin cancer (perceived threat vulnerability); how severe cancer would be (perceived threat severity); the anxiety over contracting skin cancer (fear); the opportunity to not use sunscreen and get a quick suntan (maladaptive rewards); whether sunscreen will prevent skin cancer (response efficacy); confidence in the ability to use sunscreen (self-efficacy); and the cost of buying sunscreen and the time spent on applying it (response costs).

In the IS field, PMT has been used to propose new information security models (Moody et al., 2018) and to partially predict PC (Alashoor et al., 2017; Dinev & Hart, 2004; Mohamed & Ahmad, 2012; Seounmi Youn, 2009). PMT has also been used to explain an individual's motivation for applying information security protective behaviors, such as creating backups to protect computing resources, using antivirus and antispyware software, following security policies, and adopting safe behaviors on online platforms (Boehmer et al., 2015; Boss et al., 2015; Y. Chen & Zahedi, 2016; Johnston & Warkentin, 2010; Johnston et al., 2015; Liang & Xue, 2010).

To the best of our knowledge, there is only one study in the IS field that has considered the full nomology of PMT (Boss et al., 2015). However, this study (Figure 11) was developed in

the context of IS security and not in the context of IS privacy. Applying the full nomology to the PC context would further our understanding of protective privacy behaviors.

Figure 11 – Overview of the full nomology of PMT (Boss et al., 2015).



To support our hypothesis development, in Table 21 – Appendix A, we presented an overview of the findings of the previous literature, demonstrating the relationships and effect direction between PMT constructs and their outcomes. This overview was particularly crucial for understanding that the effects of PMT on protective behaviors and intentions are still not very well established or consistent. For each research, this table indicates the effect direction of each PMT construct on the dependent variable (outcome). Except for fear (only in a positive direction when included), all other constructs have mixed results in opposite directions and unsupported hypotheses. To illustrate our analyses, we present three examples with different results for the relationship between the construct self-efficacy and PC:

1. Youn (2009) proposed a positive relationship between self-efficacy and PC but found no support. Among young adolescents, confidence in their ability to protect their personal information from e-marketers may be so strong and widespread that they have little concern about the negative consequences that can be associated with information disclosure.

2. Mohamed and Ahmad (2012) proposed and found support for a positive relationship between self-efficacy and PC. Social network users who believe they can manage their privacy settings in social networking sites will be more concerned with their information privacy. This, in turn, drives them to enable the privacy measures in social networking sites instead of leaving them at the default setting.

3. Alashoor et al. (2017) proposed and found support for a negative relationship between self-efficacy and PC. Social network users who believe that they can cope with privacy threats networks tend to be less privacy concerned.

4.2.2 Information Privacy Concerns

Privacy was conceptualized in the late 18th century at the individual level as “the right to be left alone” (Warren & Brandeis, 1890). This concept has had an influence on numerous court

cases within the US concerning protecting the privacy of individuals (Smith et al., 2011). Later, the concept was explicitly defined for information privacy as the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others (Westin, 1967).

With the introduction of computers, the privacy and security of a significant amount of information stored on electronic devices became a public concern (Ware, 1973). In this way, the concept of information privacy has been highlighted as an essential research topic in many disciplines, including economics, law, marketing, psychology, and, in particular, in the IS field (Smith et al., 2011; Xu et al., 2011).

However, understanding information privacy as a concept has been proven to be a non-trivial task. Defining and measuring information privacy is complicated because the relationships depend more on perceptions than on rational assessments. It is often argued that a universally accepted conceptualization of information privacy cannot be attained due to the varying perspectives from which it is examined (Pavlou, 2011). Thus, almost all empirical information privacy research in the social sciences relies on the measurement of a privacy-related proxy of some sort (Xu et al., 2011). Specifically, in the IS field, the proxy that has been proposed to measure information privacy is referred to as information privacy concerns.

For our experimental study, we adapted the wording of the IPC scale (Hong & Thong, 2013) to the context of m-banking. We retained the 18 original items and named the new construct mobile banking information privacy concerns (MBIPC). MBIPC refer to an individual's concerns about how personal and financial information is handled in m-banking.

4.2.3 Gaps in the PMT and PC Literature

In our literature review, we identified four relevant gaps that were addressed in two separate studies (Table 13).

Table 13 – Gaps in the PC and PMT literature.

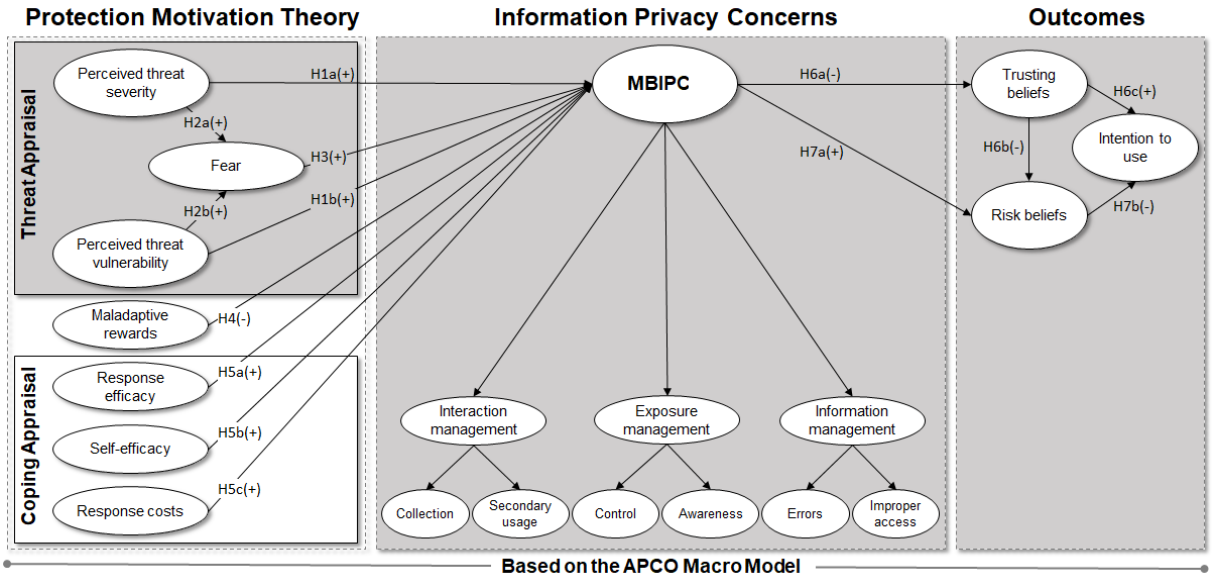
Existing Gap		**Addressed gap**	
#	**Description**	**Study 1**	**Study 2**
1. Lack of a real-time and noninvasive technique for measuring fear	To guarantee accuracy, the ideal measure of fear should be applied at the moment of occurrence using techniques different from a self-assessment, for example, using "fMRI, EEG, or other physiological techniques in a laboratory setting to capture better the extent to which fear is realized in its affective (emotional) and then cognitive forms" (Crossler et al., 2013). However, "creating a realistic fear measurement of information security behaviors under such conditions is thus highly complex and could be the 'holy grail' of this line of research" (Boss et al., 2015). To the best of our knowledge, no PMT research to date has used any of these technologies to measure fear.	X	
2. The omission of a full nomology of PMT as an antecedent of PC	In the IS security literature, some researchers have embraced PMT by using parts of it (Anderson & Agarwal, 2010; Y. Chen & Zahedi, 2016; Crossler & Bélanger, 2014; Johnston & Warkentin, 2010), and only one study has adopted its full nomology (Boss et al., 2015). In the IS privacy literature, we could not find any study that adhered to the full nomology of PMT, which would further our understanding of protective privacy behaviors (Alashoor et al., 2017).		X

Existing Gap		Addressed gap	
#	Description	Study 1	Study 2
3. No reuse of the most up-to-date PC scale as initially conceptualized	To date, the IPC scale (Hong & Thong, 2013) is recognized as the most complete and up-to-date scale in the IS field for measuring PC. IPC, a third-order latent construct, summarized the previous literature on PC from different fields. IPC was tested in the context of commercial and government websites in Hong Kong in a sequence of four studies with nearly 4,000 participants. Moreover, IPC was partially replicated in the context of mobile health applications using a second-order factor approach (Kenny & Connolly, 2017). Although IPC has been cited in 54 papers (Web of Science), none of them used the original and third-order factor scale (Appendix F).	X	X
4. The omission of fear appeal manipulations in the privacy context	To date, no study has manipulated fear appeals to stimulate threat appraisal in the privacy context. The only three studies to date that manipulated fear appeals were in the security context (Boss et al., 2015; Johnston & Warkentin, 2010; Johnston et al., 2015).	X	X

4.3 Research Model and Hypothesis Development

To attend to the purpose of this research and to address the gaps identified in the prior literature, we developed our research model, presented in Figure 12. We first leveraged PMT (antecedents) to model the relationships between the process by which individuals evaluate the threats of data loss from m-banking and PC. Then, still using PMT, we studied how individuals evaluate coping strategies to avoid data loss and their relationships with PC. Finally, we studied the impact of PC on trust, risk, and the intention to use m-banking (outcomes). The result is a model that allows us to examine the tension between m-banking users' use of this technology in a secure manner and their concerns about the privacy of their financial information, considering the degree of grave threats and possible coping strategies.

Figure 12 – Research model.



We designed and implemented two separate studies. Study 1 (Figure 12, gray boxes) was a lab experiment that involved a population of undergraduate management information system (MIS) students at a large US university. It addressed the first gap using emotion detection technology based on facial expressions and considered the PMT constructs that directly affect

fear (threat appraisal). Study 2 (Figure 12, complete model) was an online experiment that involved a population of Amazon Mechanical Turk (MTurk) workers. It addressed the second gap using the full nomology of PMT and used a self-reported measure of fear instead of emotion detection. The third and fourth gaps were addressed in both studies, as summarized in Table 13.

Considering the results shown in Table 21 – Appendix A (some mixed results in opposite directions and some unsupported hypotheses), we based our hypotheses on the foundation of PMT, and below, we explain the concepts of the constructs and the relationships in our model.

4.3.1 Threat Appraisal

A threat appraisal consists of perceived threat severity, perceived threat vulnerability, and fear (S. Milne et al., 2000, p. 111). Perceived threat severity refers to how dangerous the individual believes that the threat would be to him/herself (S. Milne et al., 2000); from the IS perspective, it is the extent to which an individual perceives that the negative consequences caused by an IT threat are severe (Liang & Xue, 2009). Perceived threat vulnerability refers to how personally susceptible an individual feels to the communicated threat (S. Milne et al., 2000); in the IS context, it is the individual's subjective probability that the IT threat will negatively affect him/her (Liang & Xue, 2009). Reasonably, the more severe the negative consequence of the threat is perceived to be, the more likely that one will be concerned about it. Therefore, we posit the following:

> H1a: The perceived threat severity of losing personal information from m-banking will positively influence MBIPC.
>
> H1b: The perceived threat vulnerability of losing personal information from m-banking will positively influence MBIPC.

Combined with severity and vulnerability, fear has a unique role in PMT, as shown in Figure 12. Fear is a negative emotion representing a response that arises from recognizing danger. This response may include any combination of apprehension, fright, arousal, concern, worry, discomfort, or a generally negative mood, and it manifests itself emotionally, cognitively, and physically (Boss et al., 2015; Leventhal, 1970). The more vulnerable an individual feels to a threat and the more severe s/he believes it to be real, the more fear will be stimulated (S. Milne et al., 2000). Therefore, threat severity and threat vulnerability predict fear (Floyd et al., 2000). Thus, we hypothesize the following:

> H2a: The perceived threat severity of losing personal information from m-banking will positively influence the fear of data loss.
>
> H2b: The perceived threat vulnerability of losing personal information from m-banking will positively influence the fear of data loss.

Moreover, the higher the perceived threat and fear, the more likely the individual will be motivated to protect him/herself (S. Milne et al., 2000). Most of the previous IS literature has found that perceived threat severity and perceived threat vulnerability positively increase some data protective behaviors (Table 21 – Appendix A). If fear can be realistically measured, then its relationship with PC can also be explored; thus, in an ideal research scenario, a PMT study should manipulate fear appeals.

"A fear appeal is a persuasive message with the intent to motivate individuals to comply with a recommended course of action through the arousal of fear associated with a threat" (Johnston & Warkentin, 2010, p. 550). Invoking fear can lead a person to take protective actions more seriously (Leventhal, 1970; Rogers, 1975). However, considering that a persuasive message can be ignored by the participant, the measurement of fear is useful to researchers provided that it does not expose the study's goal. A fear appeal helps the individual better perceive the threat severity and understand that it is a real vulnerability that s/he should be concerned about. Therefore, we posit the following:

> H3: The fear of losing personal information from m-banking will positively influence MBIPC.

4.3.2 Maladaptive Rewards

Maladaptive rewards are general benefits from not protecting oneself, such as (perhaps mistakenly) perceived time or cost savings, as well as pleasure (e.g., the pleasure of inhaling the harmful smoke of a cigarette) or even sabotage (e.g., after a family member has a heart attack, the other members continue eating fat food instead of having healthy habits to incentivize and support the sick member) (Floyd et al., 2000). The few existing studies in the previous IS privacy literature that has investigated the influence of maladaptive rewards on protective behavior find different effects. However, the most recent study (Seounmi Youn, 2009) provides evidence of a negative effect. Furthermore, seeing social or technological benefits from an activity reduces perceived risk concerns associated with that activity (Slovic & Peters, 2006). Therefore, we hypothesize that the higher the rewards from not protecting one's financial privacy, the lower the associated concern:

H4: The maladaptive rewards from not protecting personal information while using m-banking will negatively influence MBIPC.

4.3.3 Coping Appraisal

Coping appraisal is the process of considering one's response efficacy, self-efficacy, and the costs of performing the adaptive behavior (the response recommended in the fear appeal). The threat and the associated fear can motivate an adaptive behavior if a person feels capable of coping with the threat to mitigate the risk (Floyd et al., 2000). Response efficacy represents the belief that the coping response will work and that taking the protective action will be useful in protecting oneself or others (Floyd et al., 2000). Self-efficacy refers to the perceived ability of a person to carry out the adaptive coping response (Floyd et al., 2000); in other words, it is the degree to which an individual believes that s/he has the ability to perform what is required to avoid the threat (Maddux & Rogers, 1983). Finally, response costs are any costs (e.g., monetary, personal, time, effort) associated with taking the adaptive coping response (Floyd et al., 2000). In the coping appraisal process, a person's response efficacy and self-efficacy must outweigh the response costs for engaging in the protection behavior (Rogers, 1975).

The previous IS literature has presented some mixed results (Table 21 – Appendix A). We argue that individuals who believe in the effectiveness of protective measures (response efficacy) and perceive that they can handle the threatening situation (self-efficacy) are fully

aware of the severity and vulnerability of the threat and will thus likely show higher PC. We are not aware of existing literature that studies the effect of response cost on privacy concerns, but on the same vein, we argue that if individuals deem the solution to protect their information to be beyond their resources, like effort, time or money (in our context, it means to take the necessary effort to password protect their mobile devices), then they will be more concerned with the possibility of losing personal and financial data from their mobile devices. We rely on these arguments and hypothesize the following:

H5a: Response efficacy with regard to protecting personal information while using m-banking will positively influence MBIPC.
H5b: Self-efficacy with regard to protecting personal information while using m-banking will positively influence MBIPC.
H5c: The response costs of protecting personal information while using m-banking will positively influence MBIPC.

4.3.4 MBIPC, Trusting Beliefs, Risk Beliefs, and Intention to Use

In our context, trust represents the degree to which people believe that m-banking is reliable in protecting individuals' personal information (based on Hong & Thong, 2013). Some studies have identified that the company name is the most influential factor in user confidence; thus, consumers who trust the company's reputation (e.g., the bank's reputation) are less concerned about their privacy and more willing to provide personal information (Earp & Baumer, 2003; Schoenbachler & Gordon, 2002). Therefore, companies that are positioned as "safer" or "trustworthy" on the privacy dimension have an advantage over their competitors, thus engaging customers in the continued use of their online platforms (Bowie & Jamal, 2006).

Prior studies in information privacy have empirically demonstrated that trust has a negative relationship with PC and risk beliefs but a positive relationship with the use of technology (Bansal, Zahedi, & Gefen, 2010; Hong & Thong, 2013; Malhotra et al., 2004; Sipior, Ward, & Connolly, 2013); additionally, trust has been treated as a unidimensional construct. Other examples include the following: (1) individuals with high rates of PC do not trust commercial websites (Metzger, 2004); (2) as individuals' PC increase, users report registering for websites less frequently and providing incomplete information because they have less trust in the website (Sheehan & Hoy, 1999); and (3) PC have a significant impact on the intention to continue purchasing online, with the highest negative impact being through their relationship with trust (Eastlick, Lotz, & Warrington, 2006). We replicate these relationships with our model and hypothesize the following:

H6a: MBIPC will negatively influence m-banking users' trusting beliefs in this technology.
H6b: M-banking users' trusting beliefs in this technology will negatively influence their risk beliefs in this technology.
H6c: M-banking users' trusting beliefs in this technology will positively influence their intention to use m-banking.

The concept of risk is usually associated with the likelihood of an adverse result. In the context of this research, risk refers to the expectation that the potential for loss is associated

with the release of personal information to the m-banking technology (based on Hong & Thong, 2013).

When information flows across a personal boundary, individuals engage in an evaluation of the extent of the uncertainty involved – e.g., who might gain access to the data and how it might be used (Petronio, 2002). The higher the uncertainty is, the higher individuals perceive the privacy risk to be. If an individual perceives high risks of data loss, then his/her concerns about what may happen to that information will be higher (Laufer & Wolfe, 1977). The prior privacy literature has empirically verified that PC have a positive relationship with risk beliefs (Hong & Thong, 2013; Malhotra et al., 2004) and have treated risk beliefs as a unidimensional construct. Additionally, some e-commerce and social network studies have verified the adverse effect of perceived risk on intentions to continue conducting transactions or adopting a technology (Jarvenpaa & Tiller, 1999; Norberg, Horne, & Horne, 2007; Pavlou, 2003; Pavlou & Gefen, 2004). We replicate these relationships with our model and hypothesize the following:

> H7a: MBIPC will positively influence m-banking users' risk beliefs in this technology.
> H7b: M-banking users' risk beliefs in m-banking will negatively influence their intention to use this technology.

4.4 Methodology, Analysis, and Results

To achieve the increased generalizability necessary for an improved PMT model that addresses the identified research opportunities, we conducted empirical studies under two different scenarios. Both scenarios used deception in an attempt to increase the participants' PC and fear of using m-banking. The first study used fear appeals in a lab experiment with students where we could record a video with the facial reactions of the individuals in an attempt to relate them to the emotions felt during each phase of the experiment. The videos were later analyzed to measure the participants' fear using the FaceReader software. FaceReader can detect emotional expressions in the face as well as humans can, identifying six basic emotions, i.e., happiness, sadness, anger, surprise, fear, and disgust, in addition to a neutral state (Lewinski, den Uyl, & Butler, 2014), and assigning a decimal value between 0 and 1 (0 = emotion absent, 1 = emotion fully present) to each of the six basic emotions (Loijens, Krips, Kuilenburg, & Ivan, 2015). The second study was conducted on Amazon MTurk, where we also measured maladaptive rewards, response efficacy, self-efficacy and response costs to achieve the full PMT nomology. Since Study 2 was not conducted in the lab, the easy recording and sharing of videos were not feasible. Therefore, we used a self-reported measure of fear.

Before running Studies 1 and 2, we conducted a pilot study involving 20 master's and undergraduate students to assess the strength of the manipulations, gauge the clarity of the questions, and verify the clarity and conciseness of the experimental procedure and instructions. Based on the participants' feedback, we clarified and streamlined the experimental instructions, reorganized the instrument layout, and reworded some items.

In the analysis, we begin by assessing the manipulation checks. Then, we detail the data validation procedures to establish the construct validity and reliability of the measurement items used. After establishing these necessary preconditions, we proceed to evaluate the proposed

model using SEM. All of the data validation and model testing were completed using IBM® SPSS® AMOS software (Arbuckle, 2015).

4.4.1 Study 1 – Participants

The model was tested with m-banking users recruited from undergraduate courses at a large university in the US. Undergraduate student subjects are appropriate for this context (D. Compeau, Marcolin, Kelley, & Higgins, 2012) since they are heavy users of m-banking (Fed, 2016) and nearly 100% of Americans aged 18 to 29 own a cell phone of some kind (Pew, 2018). Of the 400 students invited to participate for extra credit, 215 accepted the invitation, and 186 participated. The sample consisted of 180 usable responses (after filtering out 6 participants who either missed attention checks, gave up in the middle of the experiment, or asked to withdraw their records after reading the debriefing letter at the end of the study). The students ranged in age from 18 to 29 years old; 47% were male, and 49% were employed. The time spent (in seconds) individually completing the survey was as follows: $\bar{x}_{\text{duration}} = 915.7$, $\tilde{x}_{\text{duration}} = 888$, SD = 223.3.

4.4.2 Study 1 – Design

To address the first issue of our model (a real-time measure of fear), we designed a laboratory experiment in which we recorded the sessions and analyzed the videos using Noldus FaceReader. This design provided a controlled environment where we could set up the computers according to our needs and record the fear emotion in real time during the fear appeal. We also considered that the personal relevance of a fear appeal is crucial for capturing the interest of the audience (Johnston et al., 2015). Thus, to increase external validity, we simulated a phishing attack via email where it would be possible to collect financial information from the participants' smartphones. A phishing attack is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party (Jagatic, Johnson, Jakobsson, & Menczer, 2007). This aspect was particularly important because we wanted to increase the likelihood that the fear appeal message would be perceived as legitimate and represent a threat to the participant's data.

We used the Qualtrics survey software to design the questionnaire and the fear appeal manipulations. The participants used Google Chrome running in the kiosk mode (full screen) to avoid checking the URL of the questionnaire and the URL of the fear appeal messages. We also removed the company and university logos from the questionnaire. We used the Open Broadcaster software to record both the participants' face and screen.

FaceReader is uniquely well suited to measuring fear for several reasons. First, people naturally and unconsciously express negative emotions, such as fear, through the movement of their facial muscles (McIntosh, Zajonc, Vig, & Emerick, 1997). Second, FaceReader classifies an individual's physiological state along emotional dimensions in a quantitative manner; the software assigns a value between 0 and 1 to each of the six basic emotions (happiness, surprise, anger, sadness, disgust, and fear) (Loijens et al., 2015). Third, with regard to the participant, it registers emotional measurement in an unobtrusive and unnoticed manner (Breaban & Noussair, 2018). Furthermore, the facial expressions corresponding to the six basic emotions appear to be common to all cultures (Ekman, 2007; Ekman & Friesen, 1971), allowing the

replication of the results. Last but not least, this software has been widely used in scientific research in different fields, including IS (Breaban & Noussair, 2018; Goldberg, 2014; Nwadike, Groß, & Coopamootoo, 2016; Schouten, Venneker, Bosse, Cremers, & Neerincx, 2017; Weth, Raab, & Carbon, 2015).

4.4.3 Study 1 – Procedures and Manipulation

The procedures were approved by the university institutional review board (IRB) before we conducted the experiment. We invited students via email, informing them that the survey's goal was to investigate whether emotions were associated with m-banking PC. We also informed them that a webcam would be used to record the session and that the video would be used only by the research team for scientific purposes. To participate, the student had to be an m-banking user and bring their smartphone to the lab on the session day. Table 14 presents the procedures executed in the laboratory experiment.

Table 14 – Procedures executed in the laboratory experiment.

Procedure	Description
1. Preliminary instructions	We verbally instructed the participants that the session was being recorded and that they had to complete a survey on an online platform.
2. Consent form	On the platform, the participants agreed to participate in using the online consent form.
3. Attention check	The participants completed an attention check (Appendix B).
4. Quiz (distractor)	The participants completed a quiz about brands that took approximately two-three minutes. The quiz was created as a distractor to give the participants some time to relax and shift their focus away from the webcam.
5. Provide email address	The participants provided their email addresses.
6. Lock the computer	The platform locked the computer screen, waiting for a six-digit code password.
7. Send phishing email with the unlock code	The platform sent an email with a link that was accessible only via the participant's smartphone (left side of Figure 16 – Appendix C). If the participants tried to access the code using a computer, then the system presented the message "Sorry! This page can be viewed only on a mobile phone".
8. Access the unlock code in the smartphone	When accessing the link, the participants received a six-digit code and were informed that by continuing the experiment, they allowed the collection of their device ID, settings and financial information from their mobile phones (right side of Figure 16 – Appendix C). Note, during the sessions, three participants refused to continue the survey and asked to leave the lab after reading the message on their smartphones (they still received extra credit for their course).
9. Unlock the computer	The participants typed the six-digit code on the computer to unlock the screen and proceed with the survey.
10. Redirect to a different server	The platform presented a message on the screen informing the participants that they were being redirected to a different server outside the university, and the screen blinked. Note, the participants were redirected to a different website but on the same secure server of the university.
11. Fear appeal message	The platform presented the fear appeal message (duration of 30 seconds) informing the participants that their mobile phone passwords were being checked. In the low fear appeal manipulation, we presented an animated image designed with soft colors to demonstrate the unsuccessful attempt to collect financial data from the participants' smartphone (Figure 17 – Appendix C). In the high fear appeal manipulation, we presented a similar animated image but using dark colors and demonstrating a successful attempt to collect financial information from the participants' smartphone (Figure 18 – Appendix C). In the control group, we presented an attention check unrelated to the fear appeal message.
12. Redirect back to survey	The platform presented a new message on the screen informing the participants that they were being redirected back to the survey, and the screen blinked again.
13. Safety tips	The participants were asked whether they wanted to know three safety tips to protect themselves against financial identify fraud; the options were "show me" or "skip." The "show me" option presented the security tips, and the "skip" option hid the message.

Procedure	Description
14. Survey questionnaire	The participants proceeded to complete the survey questionnaire (Table 22 – Appendix D).
15. Debriefing form	At the end of the survey, we presented the debriefing form with the option for the participants to withdraw their records and still obtain course credit and an optional field to collect feedback.

4.4.4 Study 1 – Measures

To test the hypothesized relationships, measures were adopted from prior research and modified to assess the constructs described in the research model. The reuse of an existing validated scale has at least two advantages: (1) by building on prior work, it advances state of the art, and (2) it ensures that the current research is of high quality (Preibusch, 2013).

The measures used in this study are summarized in Table 22 (Appendix D). The measures for MBIPC were operationalized as an individual's perception of his/her concern over how personal information is handled by m-banking and adapted from Hong and Thong (2013). This scale contains a third-order factor with three second-order factors. Interaction management is the ability of an individual to manage the collection and subsequent use of his/her personal information by m-banking technologies. Information management is the individual's perception of how an m-banking technology handles personal data. Exposure management is the individual's consciousness regarding existing controls that mitigate the risks of personal data loss. The measures for PMT (except fear) are taken from Boss et al. (2015), previously developed by S. Milne, Orbell, and Sheeran (2002). The measures for trusting beliefs and risk beliefs are from Hong and Thong (2013), previously developed by Malhotra et al. (2004). The measures for intention to use come from Xu and Teo (2004), previously developed by Gefen, Karahanna, and Straub (2003) and Venkatesh, Morris, Davis, and Davis (2003).

Finally, we measured fear using FaceReader, which assigns a decimal value between 0 and 1 (0 = emotion absent, 1 = emotion fully present) for each of the six basic emotions (Loijens et al., 2015) on a frame-by-frame basis (30 fps). To compute the fear variable, because we were mainly interested in the peak event of fear during the manipulation, we used the maximum rate reported while the participants were watching the 30-second fear appeal message or completing the attention check (control group). In addition to the constructs in the theoretical model, we included gender, age, and educational level as demographic variables.

4.4.5 Study 1 – Manipulation Check

Table 15 summarizes the manipulation check for Study 1. Our manipulations were in the right direction for all constructs in our model. A comparison of the control group with the others shows that our manipulations were significant for the majority of constructs. The acceptance rate of the message executed by clicking the "show me" button was consistent and slightly higher for the high fear appeal (90%) than for the low fear appeal (88%).

Table 15 – Effectiveness of the fear appeal manipulations for study 1.

Condition	n	Severity	Vulnerability	Fear	MBIPC	Intention to Use	Message Accept
Full sample	180	5.33 (1.74)	4.27 (1.58)	0.0147 (0.0166)	4.68 (1.34)	2.53 (1.71)	n/a
High fear appeal	59	5.72 (1.11)	4.65 (1.32)	0.0212 (0.0184)	4.99 (1.19)	2.31 (1.36)	0.90 (0.31)
Low fear appeal	60	5.51 (1.49)	4.58 (1.44)	0.0156 (0.0164)	4.83 (1.11)	2.63 (1.8)	0.88 (0.32)
No fear appeal	61	4.77 (2.27)	3.61 (1.74)	0.0075 (0.0117)	4.22 (1.57)	2.66 (1.91)	n/a
t-statistic (high vs. low)		0.88 (n/s)	0.31 (n/s)	1.75 (n/s)	0.76 (n/s)	-1.08 (n/s)	0.26 (n/s)
t-statistic (low vs. no)		2.11***	3.33*	3.12***	2.46**	-0.10 (n/s)	n/a
t-statistic (no vs. high)		-2.90***	-3.70*	-4.87***	-3.01*	1.16**	n/a

Notes: ***p < 0.001; **p < 0.01; *p < 0.05; n/s = not significant; n/a = not applicable; the first numbers in the cells are means; the numbers in parentheses are SDs.

4.4.6 Study 1 – Measurement Validation

All measures adopted for this study have been previously modeled and measured as reflective, first-order or third-order constructs (Boss et al., 2015; Hong & Thong, 2013; Xu & Teo, 2004). We thus follow the previous literature, and the measures developed for this study were similarly theorized and intended as reflective measures.

Since most constructs and many relationships of the hypothesized model were derived from the prior literature, we chose to use confirmatory factor analysis (CFA) to validate the measurement model. CFA is appropriate in situations where theory suggests known relationships among the indicators and their intended factors (Hair et al., 2013). The measurement model exhibited an acceptable fit to the data (χ^2_{495} = 686.81, p < 0.001, χ^2/df = 1.39, CFI = 0.97, TLI = 0.96, RMSEA = 0.047, SRMR = 0.044). The recommended values for a model with more than 30 observed variables and N < 250 are as follows: χ^2 with significant p-values expected, CFI or TLI ≥ 0.92, RMSEA < 0.08, and SRMR < 0.09 (Hair et al., 2013, p. 584). Satisfied that the model was acceptable for the preliminary stage, we could then calculate the correlations, reliabilities, and average variance extracted (AVE) values to further aid in establishing factorial validity. These metrics are summarized in Table 16.

Table 16 – Reliabilities, AVEs, means, standard deviations, and correlations for study 1.

Construct	CR	AVE	Mean	SD	1	2	3	4	5	6	7	8	9	10	11	12
1. Perceived severity	.88	.79	5.33	1.74	.89											
2. Perceived vulnerability	.84	.72	4.27	1.58	.56	.85										
3. Collection	.90	.75	4.67	1.54	.47	.48	.86									
4. Secondary usage	.92	.80	4.51	1.64	.44	.49	.80	.90								
5. Control	.91	.77	5.05	1.50	.62	.51	.75	.80	.88							
6. Awareness	.90	.74	4.87	1.56	.64	.47	.74	.73	.83	.86						
7. Errors	.89	.72	4.43	1.49	.52	.55	.77	.83	.80	.76	.85					
8. Improper access	.93	.81	4.55	1.58	.47	.48	.84	.70	.66	.74	.82	.90				
9. Trusting beliefs	.86	.60	4.70	1.08	-.18	-.42	-.38	-.47	-.31	-.32	-.46	-.36	.78			
10. Risk beliefs	.91	.71	3.95	1.36	.41	.39	.75	.69	.65	.62	.74	.67	-.54	.84		
11. Intention to use	.97	.90	2.53	1.71	-.24	-.18	-.21	-.20	-.17	-.26	-.22	-.17	.16	-.21	.95	
12. Fear	-	-	.0147	.0166	.41	.42	.36	.45	.39	.43	.43	.40	-.17	.28	-.07	-
13. Self-esteem (MV)	-	-	5.57	0.86	.01	-.02	.10	.06	.12	.16	.13	.08	.10	.05	.04	.15

Notes: N = 180; CR = composite reliability; AVE = average variance extracted; SD = standard deviation; MV = marker variable; the bold values along the diagonal are the square root of the AVE.

To demonstrate factorial validity, the AVE for a construct should be > 0.5 (convergent validity) (Hair et al., 2013). Additionally, discriminant validity is demonstrated when the square root of a construct's AVE is higher than the correlation between that construct and all other

constructs in the model (Hair et al., 2013). As shown in Table 16, the constructs in the model meet all of these criteria. To establish reliability, the composite reliability (CR) value should be ≥ 0.7 (Fornell & Larcker, 1981; Nunnally & Bernstein, 1994). The computed reliability values shown in Table 16 indicate satisfactory reliabilities.

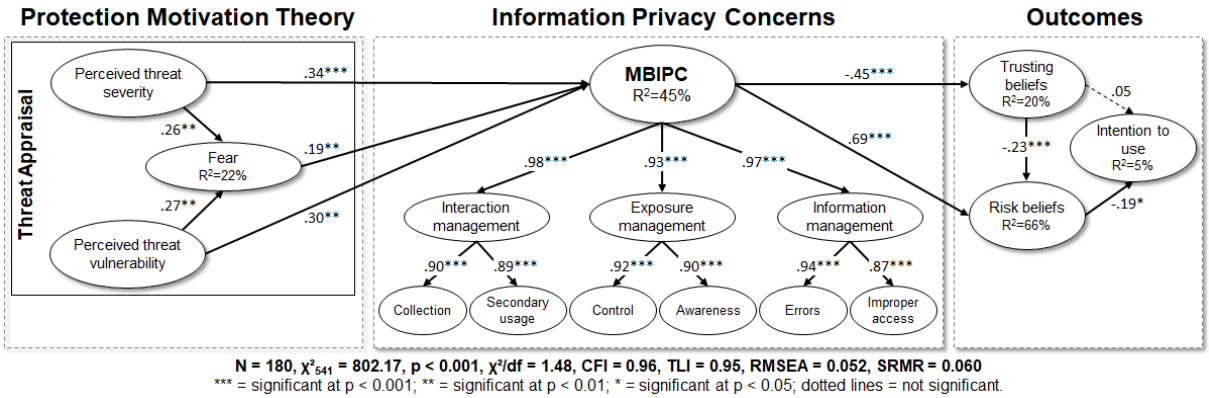
Because all survey items were measured using the same method (an online survey), the possibility exists that some of the shared variances among the constructs are due to the common method rather than the underlying relationships among the constructs. Although precautions were implemented to reduce this likelihood (e.g., randomizing the order of survey items (Straub et al., 2004)), it is necessary to test for common method bias in the measurement model. We first note that no correlations shown in Table 16 are above 0.90; correlations above this threshold may indicate common method bias (Pavlou et al., 2007). A more rigorous approach to testing common method bias is the marker variable test (Lindell & Whitney, 2001; Malhotra et al., 2006), which we conducted using self-esteem (Rosenberg, 1965) as a marker variable. The correlations between the marker and the other variables in the model were small (Table 16), giving a good signal that the marker worked. The fact that the signal swings from positive to negative was also good. We analyzed the correlations between the marker and all other constructs. We choose r2-s (-0.02) as the estimator of rs in equation 4 (Lindell & Whitney, 2001) (the second-least correlation was chosen for a more conservative approach); the results suggested that common method variance did not present a significant threat to our analysis.

Having established the validity and reliability of the constructs measured, we proceed to describe the SEM analysis of the structural model.

4.4.7 Study 1 – Model Results

We tested the partial theoretical model shown in Figure 12 (threat appraisal) using SEM. The structural model produced generally acceptable indications of fit (Hair et al., 2013, p. 584, N<250 and m≥30). The hypothesized relationships shown in the final model in Figure 13 were tested in conjunction with the SEM analyses. The tested hypotheses, along with their corresponding path estimates and significance levels, are summarized in Table 20.

Figure 13 – Final model results for study 1.



4.4.8 Study 2 – Participants

The model was tested with Amazon MTurk users (MTurkers), restricting the location to the US only and the sample to m-banking users only. For completion of the study, we compensated the participants $1. MTurkers are appropriate for this context because they allow us to focus on users who are familiar with online platforms and to generalize the results to the US population (Steelman et al., 2014). The sample consisted of 375 usable responses (after filtering out 25 participants who either missed attention check questions or asked to withdraw their records after reading the debriefing letter at the end of the survey). This sample was 51% male; 87% were employed, and 56% reported having a bachelor's degree or higher as their educational level. The participants were adults ($\bar{x}_{\text{age}}$ = 34.7, $\tilde{x}_{\text{age}}$ = 37, SD = 10.6), and the median age of the sample was close to the median age of the US population, which is 37.9 (Census, 2017). The experiment could be completed at any time before the 30-day deadline; however, it took only six hours to achieve our goal of 400 responses. We paid only the MTurkers who completed the survey; the time spent (in seconds) individually completing the survey was as follows: $\bar{x}_{\text{duration}}$ = 846.4, $\tilde{x}_{\text{duration}}$ = 734, SD = 411.4.

4.4.9 Study 2 – Design

To address the second issue of our model (a full nomology of PMT), we designed an experiment to be run on MTurk. In contrast to the lab experiment, we wanted to collect the results from participants using their computers on the Internet. On the one hand, the use of the participants' personal property (i.e., software, computer, mobile, and data on the participant's device) was essential to increase the personal relevance of the fear appeal message, thus making it more salient and capturing the attention of the audience (Johnston et al., 2015). On the other hand, this strategy generated some complaints from the MTurkers during the fear appeal manipulation.

Considering that MTurk has a policy[7] prohibiting the collection of MTurkers' email addresses, instead of sending a link via email, we simulated a fake webpage and shortened the corresponding URL using the bit.ly platform, thus decreasing the probability that the participants could verify the domain of the landing page before clicking on it. We also used the Qualtrics survey software to design the questionnaire and the fear appeal manipulation, removing the company and university logos from the questionnaire. In contrast to Study 1, it was not technically possible to record the participants' sessions because we did not have control of the participants' computers; thus, we used a self-reported measure of fear and removed the quiz (distractor) from the questionnaire. Furthermore, it was not possible to run the participants' browser in the kiosk mode; thus, we used bit.ly to hide the URL.

4.4.10 Study 2 – Procedures and Manipulation

Identical to Study 1, the procedures were also approved by the university IRB before we conducted the experiment. Before accepting the work, the MTurkers were informed that the survey was exclusively for m-banking users, and we asked them not to participate if they had

[7] https://www.mturk.com/acceptable-use-policy.

never used this technology before. Table 17 presents the procedures executed in the online experiment.

Table 17 – Procedures executed in the online experiment.

Procedure	Description
1. Preliminary instructions	After reading the instructions on MTurk, the participants clicked on the hit (link) and were redirected to answer the survey on the online platform.
2. Consent form	On the platform, the participants agreed to participate in using the online consent form.
3. Attention check	The participants completed an attention check (Appendix B).
4. No quiz	Different from Study 1, the participants were not recorded; thus, the distractor was not necessary. Therefore, we removed the quiz.
5. No email address	Different from Study 1, MTurk policy prohibits the collection of MTurkers' email addresses.
6. Lock the computer	The platform locked the computer screen, waiting for a six-digit code password. In the screen, we informed the participants that a link should be accessed using a smartphone.
7. Fake page with the unlock code	The link was accessible only on the participants' mobile device. If the participants tried to access the code using a computer, then the system presented the message "Sorry! This page can be viewed only on a mobile phone".
8. Access the unlock code in the smartphone	When accessing the link, shortened using the bit.ly service, the participants received a six-digit code and were informed that by continuing the experiment, they allowed the collection of their device ID, settings and financial information from their mobile phones (right side of Figure 16 – Appendix C).
9. Unlock the computer	The participants typed the six-digit code on the computer to unlock the screen and proceed with the survey.
10. Same as Study 1	From this point onward, the experiment followed the same procedures as those in Study 1 (see questionnaire in Table 23, Appendix D).

4.4.11 Study 2 – Measures

As in Study 1, measures were adopted from the literature and modified to assess the constructs described in the research model. The measures used in this study are summarized in Table 23 (Appendix D). To avoid an underidentified model and following the best practices of structural equation modeling (SEM) (Hair et al. 2013, p. 608), instead of using the perceived threat severity and perceived threat vulnerability constructs, which have only two items, we used the constructs with three items from Boss et al. (2015), previously developed by Johnston et al. (2015). Concerning the fear variable, considering the impossibility of using FaceReader as we did in Study 1, we used a self-reported scale of fear from Boss et al. (2015), previously developed by Milne et al. (2002).

4.4.12 Study 2 – Manipulation Check

Table 18 summarizes the manipulation check for Study 2. Our manipulations were significant and in the right direction for the majority of constructs in our model (control group vs. others), which is very similar to Study 1. The acceptance rate of the message executed by clicking the "show me" button was consistent and slightly higher for the high fear appeal (82%) than for the low fear appeal (76%).

Table 18 – Effectiveness of the fear appeal manipulations for study 2.

Condition	n	Severity	Vulnerability	Fear	MBIPC	Intention to Use	Accept Message
Full sample	375	5.49 (1.29)	4.31 (1.24)	4.47 (1.55)	4.62 (1.4)	5.97 (1.17)	n/a
High fear appeal	124	5.70 (1.07)	4.58 (1.18)	4.80 (1.46)	4.87 (1.26)	5.89 (1.33)	0.82 (0.38)
Low fear appeal	126	5.58 (1.28)	4.34 (1.18)	4.58 (1.5)	4.83 (1.36)	5.90 (1.19)	0.76 (0.43)
No fear appeal	125	5.19 (1.44)	4.02 (1.31)	4.04 (1.59)	4.14 (1.47)	6.12 (0.93)	n/a
t-statistic (high vs. low)		0.84 (n/s)	1.57 (n/s)	1.15 (n/s)	0.26 (n/s)	-0.07 (n/s)	1.33**
t-statistic (low vs. no)		2.27*	2.03*	2.79**	3.83***	-1.68 (n/s)	n/a
t-statistic (no vs. high)		-3.20**	-3.50**	-3.92***	-4.19***	1.65 (n/s)	n/a

Notes: ***p < 0.001; **p < 0.01; *p < 0.05; n/s = not significant; the first numbers in the cells are means; the numbers in parentheses are SDs.

4.4.13 Study 2 – Measurement Validation

As in Study 1, we followed the prior literature, and the measures developed for this study were similarly theorized and intended as reflective measures. We checked that the measurement model exhibited an acceptable fit to the data (χ^2_{1475} = 2504.88, p < 0.001, χ^2/df = 1.70, CFI = 0.94, TLI = 0.94, RMSEA = 0.043, SRMR = 0.038). Next, we calculated the correlations, reliabilities, and AVEs to further aid in establishing factorial validity. As shown in Table 19, for all constructs, the AVE was > 0.5, the square root of the AVE was higher than the correlation between that construct and all other constructs in the model, and the CR was ≥ 0.7, indicating satisfactory reliabilities.

Table 19 – Reliabilities, AVEs, means, standard deviations, and correlations for study 2.

Construct	CR	AVE	Mean	SD	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1. Perceived severity	.92	.80	5.49	1.29	**.89**															
2. Fear	.92	.75	4.47	1.55	.55	**.87**														
3. Perceived vulnerability	.80	.57	4.31	1.24	.42	.76	**.76**													
4. Maladaptive rewards	.80	.57	3.42	1.43	.08	.05	.14	**.76**												
5. Response efficacy	.81	.59	5.96	0.88	.31	.12	-.02	-.30	**.76**											
6. Self-efficacy	.91	.60	5.70	1.03	.17	-.05	-.05	-.12	.54	**0.77**										
7. Response costs	.81	.52	2.47	1.22	-.25	.04	.11	.42	-.59	-.44	**.72**									
8. Collection	.90	.74	4.46	1.60	.28	.62	.58	-.03	-.03	-.01	.12	**.86**								
9. Secondary usage	.92	.79	4.36	1.70	.19	.58	.52	-.03	-.03	-.04	.18	.81	**.89**							
10. Control	.90	.76	4.91	1.50	.39	.67	.60	-.05	.13	.09	-.02	.81	.77	**.87**						
11. Awareness	.92	.79	4.91	1.53	.36	.62	.56	-.08	.15	.11	-.02	.74	.73	.86	**.89**					
12. Errors	.92	.78	4.44	1.57	.27	.64	.56	.02	.01	-.05	.15	.80	.84	.80	.74	**.89**				
13. Improper access	.94	.85	4.61	1.67	.27	.63	.58	.07	.03	.03	.15	.76	.81	.76	.75	.84	**.92**			
14. Trusting beliefs	.85	.58	4.82	1.03	-.07	-.37	-.40	.02	.30	.19	-.06	-.50	-.58	-.45	-.41	-.55	-.52	**.76**		
15. Risk beliefs	.89	.66	3.83	1.33	.24	.62	.62	.06	-.11	-.15	.32	.75	.75	.68	.59	.76	.74	-.63	**.81**	
16. Intention to use	.96	.84	5.97	1.17	.03	-.24	-.22	-.05	.34	.30	-.24	-.27	-.26	-.18	-.13	-.29	-.26	.53	-.48	**.92**
17. Self-esteem (MV)	-	-	5.15	1.20	.09	-.06	-.10	-.14	.22	.11	-.11	-.08	-.13	-.04	-.08	-.07	-.08	.23	-.17	.07

Notes: N = 375; CR = composite reliability; AVE = average variance extracted; SD = standard deviation; MV = marker variable; the bold values along the diagonal are the square root of the AVE.

As in Study 1, we implemented precautions to reduce common method bias and conducted the marker variable test, using self-esteem as a marker variable. The correlations between the marker and the other variables in the model were small (Table 19), giving a good signal that the marker worked. The fact that the signal swings from positive to negative was also good. We analyzed the correlations between the marker and all other constructs. We choose r2-s (-0.06) as the estimator of rs in equation 4 (Lindell & Whitney, 2001); the results suggested that common method variance did not present a significant threat to our analysis.

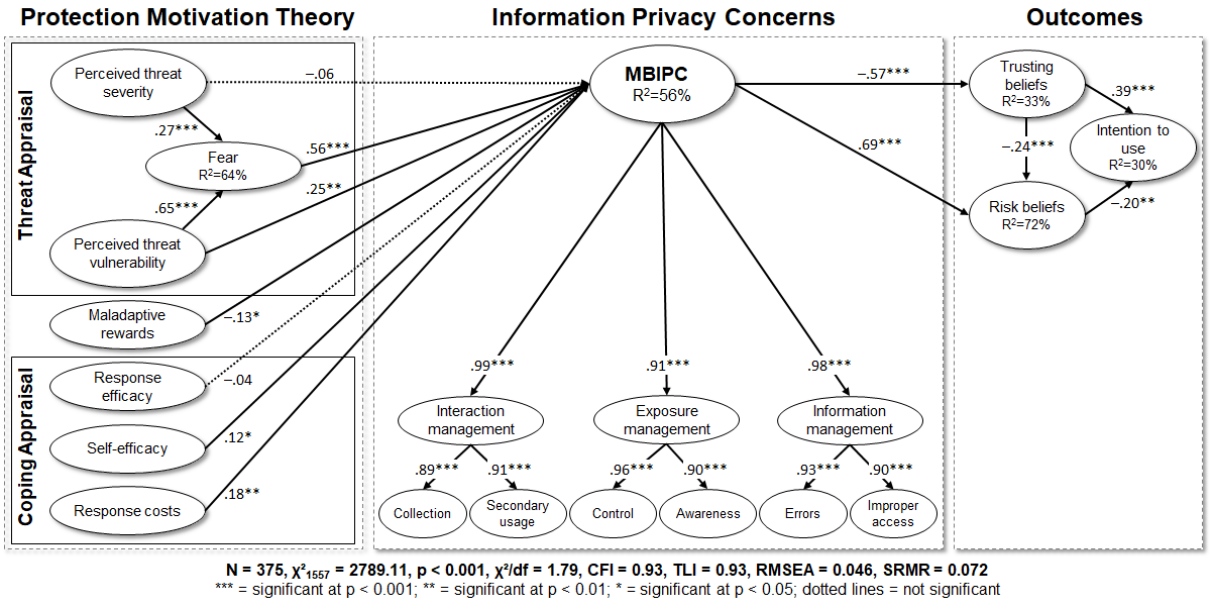
Having established the validity and reliability of the constructs measured, we proceed to describe the SEM analysis of the structural model.

4.4.14 Study 2 – Model Results

We tested the theoretical model shown in Figure 12 using SEM. Fitting the structural model to the data produced generally acceptable indications of fit (Hair et al., 2013, p. 584, N>250 and m≥30). The hypothesized relationships shown in the final model in

Figure 14 were tested in conjunction with the SEM analyses.

Figure 14 – Final model results for study 2.



4.4.15 Hypothesis Testing Results for Studies 1 and 2

Table 20 presents the tested hypotheses, along with their corresponding path estimates and significance levels for Studies 1 and 2.

Table 20 – Hypothesis testing results for Studies 1 and 2.

Hypothesis	Study 1		Study 2	
	Path Est.	Support?	Path Est.	Support?
H1a. Perceived threat severity → (+) MBIPC	.34***	Yes	-.06 (n/s)	No
H1b. Perceived threat vulnerability → (+) MBIPC	.30**	Yes	.25**	Yes
H2a. Perceived threat severity → (+) Fear	.26**	Yes	.27***	Yes
H2b. Perceived threat vulnerability → (+) Fear	.27**	Yes	.65***	Yes
H3. Fear → (+) MBIPC	.19**	Yes	.56***	Yes
H4. Maladaptive rewards → (-) MBIPC	n/a		-.13*	Yes
H5a. Response efficacy → (+) MBIPC	n/a		-.04 (n/s)	No
H5b. Self-efficacy → (+) MBIPC	n/a		.12*	Yes
H5c. Response costs → (+) MBIPC	n/a		.18**	Yes
H6a. MBIPC → (-) Trusting beliefs	-.45***	Yes	-.57***	Yes
H6b. Trusting beliefs → (-) Risk beliefs	-.23***	Yes	-.24***	Yes
H6c. Trusting beliefs → (+) Intention to use	.05 (n/s)	No	.39***	Yes
H7a. MBIPC → (+) Risk beliefs	.69***	Yes	.69***	Yes
H7b. Risk beliefs → (-) Intention to use	-.19*	Yes	-.20**	Yes
Notes: ***p < 0.001; **p < 0.01; *p < 0.05; n/s = not significant; n/a = not applicable.				

4.5 Discussion

The purpose of this paper was to examine the influence of PMT on PC and the consequences of this influence on the intention to use, specifically in the context of m-banking. We tested our research model in two different studies addressing four gaps in the IS literature:

1. The lack of a real-time and noninvasive technique for measuring fear.
2. The omission of a full nomology of PMT as an antecedent of PC.
3. No reuse of the most up-to-date PC scale as initially conceptualized.
4. The omission of fear appeal manipulations in the privacy context.

Our model summarized the relationships among perceived threat severity, perceived threat vulnerability, fear, maladaptive rewards, response efficacy, self-efficacy, response costs, MBIPC, trusting beliefs, risk beliefs, and intention to use. Study 1, a lab experiment at a large US university, considered the PMT constructs that directly affect fear (threat appraisal) and used emotion detection technology to measure fear. Study 2, an online experiment on MTurk, considered the full nomology of PMT and used a self-reported scale to measure fear.

We found that the PMT theoretical framework that was previously applied to security is also useful for privacy, helping us understand some factors that influence PC, including a new antecedent to PC – the fear emotion. This advance in the literature is significant because, as we know, little attention has been paid to the antecedents of PC (Dinev et al., 2015; Smith et al., 2011). When m-banking users are stimulated by fear appeal messages, the fear of losing personal information while using this platform increases, consequently activating PC and inducing the user to use this platform more securely.

4.5.1 Implications for Research

In our study, we identified five main contributions to research.

First, we used emotion detection technology to measure fear (in real time and noninvasively), reducing the method bias (Burton-Jones, 2009) introduced by a self-reported scale and reflecting in the Path Estimates (Fear → MBIPC) that is .19 on the first study and .56 on second study. We found that fear can be stimulated by a fear appeal message and that it increases PC. Moreover, the facial expressions corresponding to the six basic emotions identified using FaceReader are common to all cultures (Ekman, 2007; Ekman & Friesen, 1971), allowing the replication of our results in different samples.

Second, as the full nomology of PMT has been tested in the IS security literature, we applied the full nomology of PMT to privacy, which is intuitively associated with security (Flavián & Guinalíu, 2006). However, the association between the full nomology of PMT and PC in the IS literature has, perhaps surprisingly, not yet been studied.

Third, we used the original third-order IPC scale (Hong & Thong, 2013) to measure MBIPC. The results of our study provide evidence of the stability of this measure, helping the field be more confident about the applicability of the scale over time and in different contexts. Moreover, to the best of our knowledge, no existing model deals with the specific characteristics of financial information privacy.

Fourth, no previous study has manipulated fear appeal messages in the IS privacy context. The tests of our research (manipulation checks) demonstrated that manipulating high and low fear appeal messages significantly influenced threat appraisal and MBIPC. Intention to use was also significantly influenced by a high fear appeal message (Study 1). Our results are aligned with previous IS security research (Boss et al., 2015): if a fear appeal message is presented to individuals, then they will be more receptive to the proposed action and more concerned about the privacy of their personal and financial data. Consequently, more privacy-concerned individuals will be more careful when using m-banking, including the possibility of reducing its use.

Fifth, as predicted, in both studies, perceived threat severity and perceived threat vulnerability significantly influenced fear of data loss (H2a and H2b), which, in turn, positively influenced MBIPC (H3). Perceived threat vulnerability also positively influenced MBIPC (H1b); however, we did not find support for the relationship between perceived threat severity and MBIPC (H1a) in Study 2. The positive relationship between perceived threat severity and vulnerability with PC is not surprising and indeed supports prior studies developed in the context of online social networks and websites (Alashoor et al., 2017; Dinev & Hart, 2004; Mohamed & Ahmad, 2012). Our contribution resides in the fact that we extended previous studies by including fear in the model. The model testing results provided substantial empirical evidence that fear of data loss is influenced by severity and vulnerability and increases MBIPC. The prior literature tested a similar relationship in the context of IS security (e.g., Boss et al. (2015)), but this relationship is new in the IS privacy context.

Additionally, we found further results that are not new to the field but can also constitute a contribution to future research. We found empirical evidence that supports and contrasts with the previous literature.

As hypothesized, maladaptive rewards had a negative effect on MBIPC (H4), which is consistent with several previous IS security studies (Table 21 – Appendix A), and one IS privacy study that used the concept of maladaptive rewards as information disclosure benefits (Seounmi Youn, 2009). In the context of our research, individuals see some benefits in not using a secure Wi-Fi connection, and these benefits reduce their PC, despite the nature of the data.

Although a secure Wi-Fi connection improves the protection of personal information and many previous studies (Table 21 – Appendix A) have confirmed a positive relationship between response efficacy and MBIPC (H5a), we did not find support for this hypothesis in the context of m-banking. Considering that consumers usually attribute the responsibility for protecting data to financial institutions (Javelin, 2018), we speculate that m-banking users are not aware of the importance of using a secure Wi-Fi connection while transacting in this platform. Future studies are needed to examine this relationship.

As hypothesized, self-efficacy has a positive effect on MBIPC (H5b). This result means that individuals who perceive that they can handle the threatening situation are persons who are aware of the severity and vulnerability of the threat and will likely show higher PC. However, we found mixed results in previous IS privacy studies, with positive, negative and unsupported

results (Table 21 – Appendix A). More work is needed to uncover the mechanisms leading to different results.

Response costs positively and significantly influenced MBIPC (H5c). This result means that higher costs of using a secure Wi-Fi connection increased individuals' PC. We speculate that if individuals cannot afford the costs associated with taking the adaptive coping response (in our context, using a secure Wi-Fi connection), then they will be more concerned with the possibility of losing personal and financial data from their mobile devices. We recognize, however, that further research is necessary to investigate this relationship.

The model also hypothesized several outcomes typically used in the IS privacy literature (H6a, H6b, H6c, H7a, H7b). We provided compelling evidence that MBIPC play an essential role in the intention of users to adopt this technology. The fact that users who are more concerned about privacy trust less and see more risk in this specific technology support prior findings (Hong & Thong, 2013). Additionally, we confirmed that trustable and low-risk technologies, such as m-banking, influence the behavior of users to adopt or continue to use these technologies (Malhotra et al., 2004). Understanding this phenomenon in different contexts is essential to consolidate theories and advance science (Dennis & Valacich, 2014; Niederman & March, 2015). Furthermore, we are discussing financial information, a highly sensitive type of data (Culnan, 1993; Woodman et al., 1982) that, if leaked, can be disastrous for individuals and organizations (Goode et al., 2017). Our results thus constitute a contribution to our understanding of PC about financial data and their impact on the use and adoption of m-banking technologies.

4.5.2 Implications for Practice

This research has implications for practitioners in the financial industry involved with the security of m-banking applications and consumers.

We found that fear of data loss, especially in a scenario of high fear appeal, influences users' concerns about how their personal and financial information is handled in m-banking, reducing trust and, consequently, reducing the intention to use this technology. Presently, we live in an era in which people have to handle so much information that they do not exactly know whether and to what degree they should be concerned about privacy (Acquisti et al., 2015).

If the financial industry wishes for people to use m-banking technologies, then it should invest more in security technologies to avoid identity fraud and data breaches. Moreover, if banks want to educate their clients to use m-banking more securely (e.g., using m-banking only with a secure Wi-Fi connection), they can implement fear appeal messages in their applications. When a security message indicating a high-threat situation is presented to users, they are more receptive to the indicated countermeasure message, mitigating the risk of attacks and reducing financial losses for both clients and banks.

4.5.3 Limitations and Future Research

We understand that a controlled laboratory setting (Study 1) was much more likely to raise the participants' suspicion that the message was part of the experiment and would decrease the perceived threat of the phishing message. During the experiment, the students possibly

recognized that the threat had been directed from secure university servers and not from an external attack. The ideal scenario would be to test the fear appeal messages in the real world, establishing a partnership with a financial institution and implementing the messages in the application for a selected sample of clients.

Our study is also limited to behavior occurring within a single application (m-banking). While the use of m-banking is multiplying and surpassing the use of other banking channels (Fed, 2016), and therefore deserves our focus, these findings may not generalize to other banking channels (e.g., Internet banking, ATM, or call centers) or different mobile payment and digital wallet applications (e.g., PayPal, Samsung Pay, or Apple Pay). Future research should investigate these relationships in other banking channels or financial applications to develop further insights.

Furthermore, in line with the APCO framework, our model conceptualizes risk beliefs as an outcome variable that is directly affected by MBIPC. Future work could test whether and under what circumstances (e.g., generic definitions vs. specific applications) risk beliefs affect MBIPC. For instance, Dinev and Hart (2006) define vulnerability as "the perceived potential risk when personal information is revealed," thus treating risk as a threat appraisal construct equivalent to perceived threat vulnerability. define risk as "uncertainty about who has access to the information and how it is used," while "privacy concerns are beliefs about who has access to information that is disclosed." In such contexts, one would model risk as an antecedent to PC rather than as an outcome variable.

Finally, our proposed model did not support all hypothesized relationships between PMT and MBIPC, especially response efficacy. In our questionnaire, we asked the participants about the use of secure/insecure Wi-Fi while using m-banking. We believe that future studies could adapt the questionnaire and use different security measures that are perhaps more relevant to users and that are usually used in IS security research (e.g., using a strong mobile password, installing antivirus software, or creating backups).

4.6 Conclusion

This research uses the PMT (Rogers, 1975) and PC literature (Hong & Thong, 2013; Malhotra et al., 2004; Smith et al., 1996) to examine how fear, coping appraisal and the perceived threat of losing personal information impact the potential PC about the use of m-banking. Perceived threats regarding the use of m-banking could stimulate fear and PC, consequently affecting the perception of risk, trust, and the intention to use this technology. We tested our model in two different studies. In the first, we ran the partial model in a lab experiment with 180 students and used emotion detection to measure fear. In the second, we ran the complete model in an online experiment with a sample of 375 MTurkers, restricting the location to the US only. We found strong support for most of the proposed relationships in both studies. Our research has significant implications for researchers interested in privacy issues related to m-banking technology. The FSI can also benefit from this research, as our findings indicate the importance of secure privacy-related behaviors in the intention to use m-banking.

4.7 Appendix A: Relationship Between PMT and Outcomes

Table 21 – Relationship between PMT and outcomes in the IS literature (reverse chronological order).

PMT and effect direction							Outcomes	Method	Author(s)
Threat			Mal	Coping					
PS	PV	Fe		RE	SE	RC			
	+				(-)		Privacy concerns over social network sites (model 1)	A survey of 208 undergraduate and graduate students in the US	(Alashoor et al., 2017)
n/s	+			+	+	(-)	Adoption of QR codes as an authentication service	A survey of 112 college students in the US	(Yang et al., 2017)
+	+			+	+		Online protective actions	A survey of 480 students in the US and 238 social network users in China	(Y. Chen & Zahedi, 2016)
(-)	+			n/s	+	+	Online unsafety behavior, such as using unauthorized software	A survey of 505 teachers in Taiwan	(Chou & Chou, 2016)
n/s	n/s			+	+	n/s	The protective behavior of securing desktops	A survey of 241 undergraduates in the US	(Hanus & Wu, 2016)
(-)	n/s			+	(-)	(-)	Online safety behaviors (PS and SE in the opposite direction of that hypothesized)	A survey with 988 Amazon Mechanical Turk users	(Tsai et al., 2016)
n/s	n/s			+	+		Adoption of security behaviors	Two studies with 565 and 206 undergraduates in the US	(Boehmer et al., 2015)
+	+	+		+	+	(-)	Protective behavior (backups in a high fear appeal scenario)	A longitudinal study with 104 MBA students in the US	(Boss et al., 2015)
+	+	+	(-)	+	+	(-)	Protective behavior (backups in a high fear appeal scenario)	Experimental survey with 327 undergraduates in the US	
+	+		n/s	+	+	(-)	Malware avoidance behavior across different contexts at university and at home	A survey of 252 higher education students in Australia	(Dang-Pham & Pittayachawan, 2015)
+	n/s			+	+		Compliance with information security policies	An experimental survey of 559 employees in Finland.	(Johnston et al., 2015)
n/s	n/s			+	+	n/s	Intention to comply with a hypothetical BYOD policy	A survey of 360 students and employees in the US	(Crossler et al., 2014)
+	n/s			+	+	(-)	Behavior to comply with an actual BYOD policy	A survey of 84 MBA students, undergraduates, and employees	
+	(-)			+	+	(-)	Unified security practices (PV in the opposite direction)	A survey of 279 participants	(Crossler & Bélanger, 2014)
+	n/s			+	+	(-)	Adoption of antivirus software and strong passwords	A survey of 77 freshmen in the US (hands-on safety training)	(Meso, Ding, & Xu, 2013)
n/s	+				+	(-)	Adoption of home privacy concerns security behavior	A survey of 184 participants (snowball method)	(Claar & Johnson, 2012)
(-)	+			+	+	n/s	Intention to comply with information security policies (PS in the opposite direction)	A survey of 124 business managers and IT professionals in Canada	(Ifinedo, 2012)
					+		Coping behaviors to fight identity theft	A survey of 117 undergraduates in the US	(Lai, Li, & Hsieh, 2012)
+	n/s			+	+		Protective behavior against online harassment	A survey of 537 high school students in Singapore	(Lwin, Li, & Ang, 2012)
+	+			n/s	+		Information privacy concerns with social networking sites	A survey of 340 undergraduates in Malaysia	(Mohamed & Ahmad, 2012)
+	n/s			+	+	(-)	Online safety behaviors, such as deleting suspicious emails	A survey of 202 college students in Korea	(Yoon, Hwang, & Kim, 2012)

PMT and effect direction							Outcomes	Method	Author(s)
Threat			Mal	Coping					
PS	PV	Fe		RE	SE	RC			
+	+			+	+	(-)	Intention to adopt antiplagiarism software	A survey of 218 faculty members in the US	(Y. Lee, 2011)
				+	n/s	n/s	Behavior to adopt antiplagiarism software		
				+	+		Intention to practice safe computing at home	A survey of 101 undergraduates in the US	(Anderson & Agarwal, 2010)
(-)	n/s			+	+		Installation of antispyware software	A survey of 215 faculty, staff, and students at a large university in the US	(Johnston & Warkentin, 2010)
+	+			+	+	(-)	Intentions and behaviors associated with antispyware	A survey of 152 business students in the US	(Liang & Xue, 2010)
				n/s	+		Motivation to comply with information security policies	A survey of 917 employees in Finland	(Siponen, Pahnila, & Mahmood, 2010)
					+		Online information privacy protection behavior	A survey of 285 middle school students in the US	(Chai, Bagchi-Sen, Morrell, Rao, & Upadhyaya, 2009)
+	n/s			+	+	n/s	Intention to use antispyware software	A survey of 232 undergraduates in the US	(Gurung, Luo, & Liao, 2009)
+	n/s			+	+	(-)	Intention to comply with information security policy	A survey of 312 employees from 78 organizations	(Herath & Rao, 2009)
+	+			+	+	(-)	Intention to adopt antimalware	A survey of 239 SMB executives in the US	(Y. Lee & Larsen, 2009)
n/s	+				+		Online shopping protective behavior (model 8)	A survey of 449 online shoppers in the US	(G. R. Milne, Labrecque, & Cromer, 2009)
n/s	+				+	n/s	Secure email behavior	A survey of 134 employees in Singapore	(Ng, Kankanhalli, & Xu, 2009)
	+		(-)		n/s		Privacy concerns and resulting practices of protective privacy behavior, such as fabrication	A survey of 144 middle school students in the US	(Seounmi Youn, 2009)
n/s	n/s	+		+		(-)	Intention to use strong Passwords	A survey of 182 students in the US	(L. Zhang & McDowell, 2009)
n/s	+			+	+		Online protection behavior (use of antivirus, antispyware and antimalware software)	A survey of 272 college students (Internet users) in the US	(D. Lee, Larose, & Rifon, 2008)
(-)	(-)			(-)	(-)	(-)	The omission of subjective and objective online safety measures	Survey and log files among 588 workers in a technology-oriented company	(Workman et al., 2008)
(-)	(-)		+				Willingness to provide information to a website (contrary to protective behavior)	A survey of 326 high school students in the US	(S. Youn, 2005)
(-)	n/s			(-)	(-)	(-)	The decision to implement security features on domestic wireless networks	A survey of 189 home users associated with the National University of Singapore	(Woon, Tan, & Low, 2005)
	+						Internet privacy concerns	A survey of 369 students and employees in the US	(Dinev & Hart, 2004)
+ (-) n/s	+ (-) n/s	+	+ (-) n/s	+ (-) n/s	+ (-) n/s	+ (-) n/s	**Summary**		

Note: Threat = threat appraisal; Coping = coping appraisal; PS = perceived threat severity; PV = perceived threat vulnerability or susceptibility; Fe = fear; Mal = maladaptive rewards; RE = response efficacy; SE = self-efficacy; RC = response costs; n/s = not significant.

4.8 Appendix B: Attention Check for Studies 1 and 2

Figure 15 – Attention check for studies 1 and 2.

Mobile Banking

In this survey, we will use the term mobile banking app when referring to mobile banking. The US Federal Reserve (FED) defines **mobile banking** as using "*a mobile phone to access your bank or credit union account. This can be done either by accessing your bank or credit union's web page through the web browser on your mobile phone, via text messaging, or by using an app downloaded to your mobile phone.*"

https://www.federalreserve.gov/consumerscommunities/mobile_finance.htm

In order to facilitate our research on information privacy concerns we are interested in whether you actually take the time to read the directions; if not, then some of our questions will be useless. So, in order to demonstrate that you have read the instructions, please ignore the question below. Instead, select only the bank whose name starts with the letter "W" (i.e., "Wells Fargo") and proceed to the next screen. Thank you very much.

Which of these banks do you know?
(click on all that apply)

- ☐ Ally Bank
- ☐ Bank of America
- ☐ Capital One
- ☐ Citi
- ☐ Goldman Sachs
- ☐ HSBC
- ☐ JPMorgan Chase
- ☐ Morgan Stanley
- ☐ SunTrust
- ☐ US Bank
- ☐ Wells Fargo
- ☐ None of them

4.9 Appendix C: Screenshots of the Experiments

Figure 16 – Email and webpage with six-digit code (access allowed only via a smartphone).

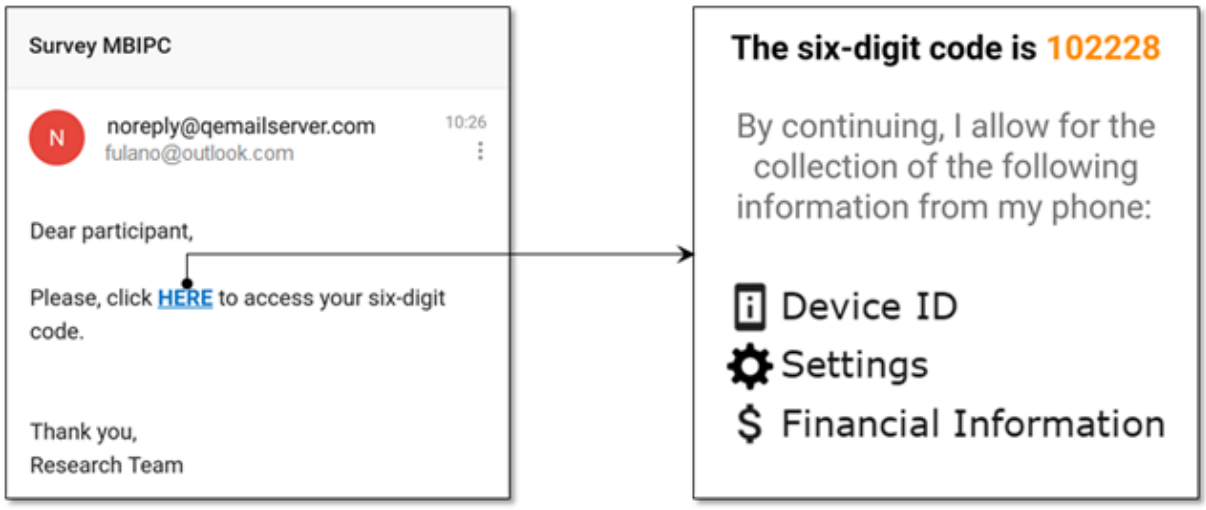


Figure 17 – Low fear appeal message.

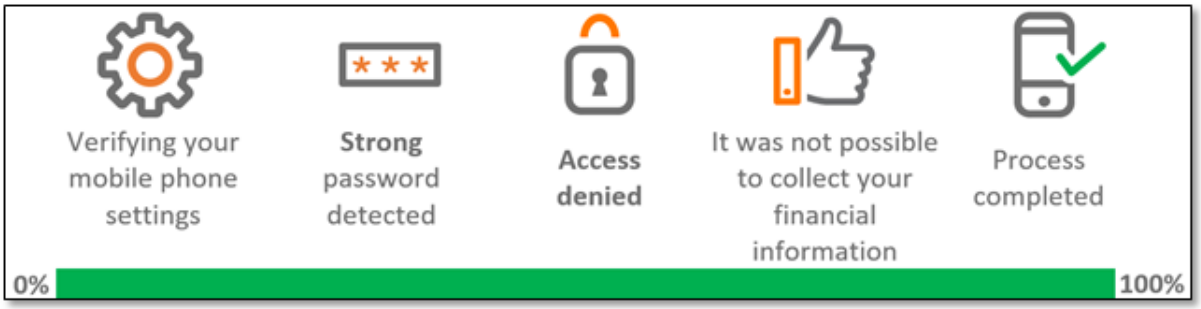
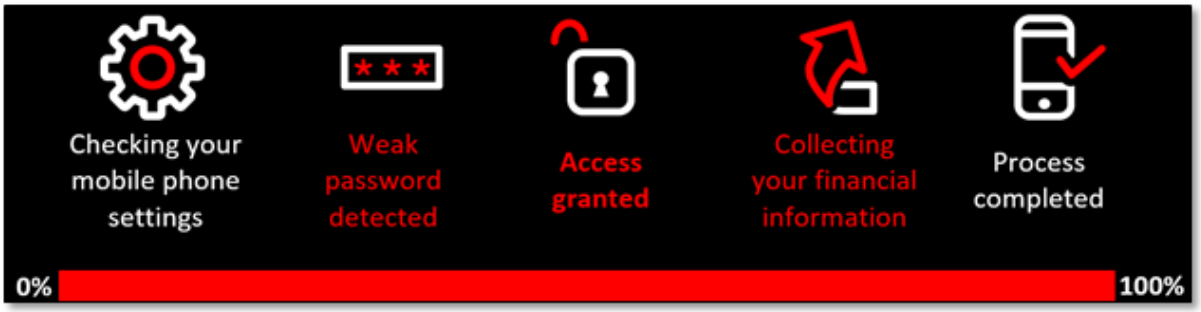


Figure 18 – High fear appeal message.



4.10 Appendix D: Measurement Items for Studies 1 and 2

Table 22 – Measurement items for study 1.

Construct	Code	Items
Perceived threat severity (Boss et al., 2015; S. Milne, Orbell, & Sheeran, 2002)	PS1	If I were to lose personal information from mobile banking, I would suffer much pain.
	PS2	Losing personal information from mobile banking would cause me major problems.
Perceived threat vulnerability (Boss et al., 2015; S. Milne et al., 2002)	PV1	My chances of losing personal information from mobile banking in the future are high.
	PV2	I am likely to lose personal information from mobile banking in the future.
Collection (Hong & Thong, 2013; Smith et al., 1996)	COL1	It usually bothers me when mobile banking asks me for personal information.
	COL2	When mobile banking asks me for personal information, I sometimes think twice before providing it.
	COL3	I am concerned that mobile banking collects too much personal information about me.
Unauthorized secondary use (Hong & Thong, 2013; Smith et al., 1996)	SEC1	I am concerned that when I give personal information to mobile banking for some reason, that mobile banking will use the information for other reasons.
	SEC2	I am concerned that mobile banking would sell my personal information in their computer databases to other companies.
	SEC3	I am concerned that mobile banking would share my personal information with other companies without my authorization.
Errors (Hong & Thong, 2013; Smith et al., 1996)	ERR1	I am concerned that mobile banking does not take enough steps to make sure that my personal information in their files is accurate.
	ERR2	I am concerned that mobile banking does not have adequate procedures to correct errors in my personal information.
	ERR3	I am concerned that mobile banking does not devote enough time and effort to verifying the accuracy of my personal information in their databases.
Improper access (Hong & Thong, 2013; Smith et al., 1996)	ACC1	I am concerned that mobile banking databases that contain my personal information are not protected from unauthorized access.
	ACC2	I am concerned that mobile banking does not devote enough time and effort to preventing unauthorized access to my personal information.
	ACC3	I am concerned that mobile banking does not take enough steps to make sure that unauthorized people cannot access my personal information stored on their computers.
Control (Hong & Thong, 2013; Malhotra et al., 2004)	CON1	It usually bothers me when I do not have control of personal information that I provide to mobile banking.
	CON2	It usually bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by mobile banking.
	CON3	I am concerned when control is lost or unwillingly reduced as a result of a financial transaction with mobile banking.
Awareness (Hong & Thong, 2013; Malhotra et al., 2004)	AWA1	I am concerned when a clear and conspicuous disclosure is not included in the online privacy policies of mobile banking.
	AWA2	It usually bothers me when I am not aware or knowledgeable about how my personal information will be used by mobile banking.
	AWA3	It usually bothers me when mobile banking seeking my information online do not disclose the way the data are collected, processed, and used.
Trusting beliefs (Hong & Thong, 2013; Malhotra et al., 2004)	TRUS1	Mobile banking, in general, would be trustworthy in handling my personal information.
	TRUS2	Mobile banking would keep my best interests in mind when dealing with my personal information.
	TRUS3	Mobile banking would fulfill their promises related to my personal information.
	TRUS4	Mobile banking is in general predictable and consistent regarding the usage of my personal information.

Construct	Code	Items
Risk beliefs (Hong & Thong, 2013; Malhotra et al., 2004)	RISK1	In general, it would be risky to give my personal information to mobile banking.
	RISK2	There would be a high potential for loss associated with giving my personal information to mobile banking.
	RISK3	There would be too much uncertainty associated with giving my personal information to mobile banking.
	RISK4	Providing mobile banking with my personal information would involve many unexpected problems.
Intention to use (Gefen, Karahanna, & Straub, 2003; Venkatesh, Morris, Davis, & Davis, 2003; Xu & Teo, 2004)	USE1	I plan to use mobile banking while connected to a public Wi-Fi in the next 3 months.
	USE2	Assuming I had access to mobile banking, I intend to use it while connected to a public Wi-Fi in the next 3 months.
	USE3	Given that I had access to mobile banking, I predict that I would use it while connected to a public Wi-Fi in the next 3 months.
	USE4	I would use a mobile banking app while connected to a public Wi-Fi for online transactions in the next 3 months.
	USE5	While connected to a public Wi-Fi, I am very likely to provide mobile banking apps with the information that is necessary to serve my needs in the next 3 months better.
Notes: All items were measured using 7-point Likert-type scales from 1 = strongly disagree to 7 = strongly agree; R = reverse-coded item.		

Table 23 – Measurement items for study 2.

Construct	Code	Items
Perceived threat severity (Boss et al., 2015; Johnston & Warkentin, 2010)	PS1	If I lose personal information from m-banking, it will be severe.
	PS2	If I lose personal information from m-banking, it will be serious.
	PS3	If I lose personal information from m-banking, it will be significant.
Perceived threat vulnerability (Boss et al., 2015; Johnston & Warkentin, 2010)	PV1	My personal information is at risk due to the use of m-banking.
	PV2	It is likely that I will lose personal information from m-banking.
	PV3	It is possible that I will lose personal information from m-banking.
Fear (Boss et al., 2015; S. Milne et al., 2002)	PF1	I am frightened about the prospect of losing personal information from m-banking.
	PF2	I am anxious about the prospect of losing personal information from m-banking.
	PF3	I am worried about the prospect of losing personal information from m-banking.
	PF4	I am scared about the prospect of losing personal information from m-banking.
Maladaptive rewards	MAL1	Not using a secure Wi-Fi connection with my mobile phone saves me some time.
	MAL2	Not using a secure Wi-Fi connection with my mobile phone saves me some effort in setting it up.
	MAL3	Not using a secure Wi-Fi connection with my mobile phone makes it easier for me to use all its functionalities (e.g., streaming from blocked websites).
Response efficacy (Boss et al., 2015; Johnston & Warkentin, 2010)	RE1	A secure Wi-Fi connection works for protection.
	RE2	A secure Wi-Fi connection is effective for protection.
	RE3	When using a secure Wi-Fi connection, my mobile phone is more likely to be protected.
Self-efficacy (Boss et al., 2015; D. R. Compeau & Higgins, 1995)	CSE1	I could set up a secure Wi-Fi connection on my mobile phone if I had seen someone else doing it before trying it myself.
	CSE2	I could set up a secure Wi-Fi connection on my mobile phone if I could call someone for help if I got stuck.
	CSE3	I could set up a secure Wi-Fi connection on my mobile phone if someone else helped me get started.
	CSE4	I could set up a secure Wi-Fi connection on my mobile phone if I had a lot of time to complete the job.
	CSE5	I could set up a secure Wi-Fi connection on my mobile phone if I had just the built-in help for assistance.
	CSE6	I could set up a secure Wi-Fi connection on my mobile phone if someone showed me how to do it first.
	CSE7	I could set up a secure Wi-Fi connection on my mobile phone if I had used phones similar to this one before doing the job.
Response costs (Boss et al., 2015; S. Milne et al., 2002)	RC1	The costs of using a secure Wi-Fi connection on my mobile phone outweigh the benefits.
	RC2	I would be discouraged from using a secure Wi-Fi connection on my mobile phone because doing so would take too much time.
	RC3	Using a secure Wi-Fi connection on my mobile phone would cause me too many problems.
	RC4	I would be discouraged from using a secure Wi-Fi connection on my mobile phone because I would feel silly doing so.
Intention to use (Gefen et al., 2003; Venkatesh et al., 2003; Xu & Teo, 2004)	USE1	I will use mobile banking for online transactions in the next 3 months.
	USE2	I am very likely to provide m-banking with the information that is necessary to serve my needs in the next 3 months better.
	USE3	Assuming I had access to m-banking, I intend to use it in the next 3 months.
	USE4	Given that I had access to m-banking, I predict that I will use it in the next 3 months.
	USE5	I plan to use m-banking in the next 3 months.
All items were measured using 7-point Likert-type scales from 1 = strongly disagree to 7 = strongly agree; R = reverse-coded item; The collection, unauthorized secondary use, errors, improper access, control, awareness, and trusting beliefs constructs are the same as those used in Study 1.		

4.11 Appendix E: Key Terms and Concepts

Table 24 – Key terms and concepts (in alphabetical order).

Term/Concept	Definition (Citation)
Awareness	The degree to which a person is concerned about his/her awareness of information privacy practices by m-banking (Hong & Thong, 2013; Malhotra et al., 2004).
Collection	The degree to which a person is concerned about the amount of individual-specific data possessed by m-banking (Hong & Thong, 2013; Smith et al., 1996).
Control	The degree to which a person is concerned that he/she does not have adequate control over his/her personal information held by m-banking (Hong & Thong, 2013; Malhotra et al., 2004).
Coping appraisal	The process of considering one's self-efficacy, response efficacy, and the costs of performing the adaptive behavior or the response advocated in the fear appeal (Floyd et al., 2000).
Errors	The degree to which a person is concerned that protections against deliberate and accidental errors in the personal data collected by m-banking are inadequate (Hong & Thong, 2013; Smith et al., 1996).
Extrinsic maladaptive rewards	Extrinsic rewards for engaging in the maladaptive response of not protecting oneself, such as monetary compensation (Boss et al., 2015; Floyd et al., 2000).
Fear	A negatively valanced emotion representing a response that arises from recognizing danger. This response may include any combination of apprehension, fright, arousal, concern, worry, discomfort, or a general negative mood, and it manifests itself emotionally, cognitively, and physically (Leventhal, 1970; McIntosh et al., 1997; Osman, Barrios, Osman, Schneekloth, & Troutman, 1994; Witte, 1992, 1996, 1998).
Fear appeal	A purposefully generated message that is carefully designed and manipulated, first, to raise perceptions of threat severity and vulnerability and the subsequent fear and, then, to invoke one's sense of self-efficacy and response efficacy, all of which are intended to overcome maladaptive rewards and response costs and subsequently change one's intentions toward an adaptive response (Boss et al., 2015; Floyd et al., 2000; S. Milne et al., 2000).
Improper access	The degree to which a person is concerned that the personal information held by m-banking is readily available to people not adequately authorized to view or work with the data (Hong & Thong, 2013; Smith et al., 1996).
Intention to use	Individuals' willingness to use m-banking while connected to a public Wi-Fi connection (Gefen et al., 2003; Venkatesh et al., 2003; Xu & Teo, 2004).
Intrinsic maladaptive rewards	Intrinsic rewards for engaging in the maladaptive response of not protecting oneself, such as maintaining pleasure or exacting revenge (Boss et al., 2015; Floyd et al., 2000).
Maladaptive rewards	The general rewards (intrinsic and extrinsic) of not protecting oneself, contrary to the fear appeal (Boss et al., 2015; Floyd et al., 2000).
Mobile banking information privacy concerns (MBIPC)	An individual's concerns about how personal and financial information is handled in m-banking.
Perceived threat severity	"How serious the individual believes that the threat would be" to him/herself (Boss et al., 2015; S. Milne et al., 2000, p. 108).
Perceived threat vulnerability	"How personally susceptible an individual feel to the communicated threat" (Boss et al., 2015; S. Milne et al., 2000, p. 108).
Response costs	"Any costs (e.g., monetary, personal, time, effort) associated with taking the adaptive coping response" (Boss et al., 2015; Floyd et al., 2000, p. 411).
Response efficacy	"The belief that the adaptive response [coping] will work, that taking the protective action will be effective in protecting the self or others" (Boss et al., 2015; Floyd et al., 2000, p. 411).
Risk beliefs	The expectation that a high potential for loss is associated with the release of personal information to m-banking (Hong & Thong, 2013; Malhotra et al., 2004).
Self-efficacy	"The perceived ability of the person to carry out the adaptive [coping] response" (Boss et al., 2015; Floyd et al., 2000, p. 411).
Threat appraisal	The process of considering the severity of and vulnerability to a threat against the maladaptive rewards associated with maladaptive behavior, such as saving time or avoiding trouble by not following the response advocated in the fear appeal (Floyd et al., 2000).
Trusting beliefs	The degree to which people believe that m-banking is dependable in protecting individuals' personal information (Hong & Thong, 2013; Malhotra et al., 2004).
Unauthorized secondary use	The degree to which a person is concerned that their personal information is collected by m-banking for one purpose but is used for another secondary purpose without authorization by the individual (Hong & Thong, 2013; Smith et al., 1996).

4.12 Appendix F: Papers in Web of Science that Cited the Internet Privacy Concerns

Table 25 – List of 54 papers in Web of Science that cited the Internet Privacy Concerns scale (in alphabetical order of author).

#	**Author(s)**	**Paper**
1	(Addae, Brown, Sun, Towey, & Radenkovic, 2017)	Measuring attitude towards personal data for adaptive cybersecurity.
2	(Alashoor et al., 2017)	Familiarity with big data, privacy concerns, and self-disclosure accuracy in social networking websites: An APCO model.
3	(Baek, 2014)	Changing the default setting for information privacy protection: What and whose personal information can be better protected?
4	(Bartsch & Dienlin, 2016)	Control your Facebook: An analysis of online privacy literacy.
5	(Benamati, Ozdemir, & Smith, 2017)	An empirical test of antecedents - privacy concerns - outcomes model.
6	(Benson, Saridakis, & Tennakoon, 2015)	Information disclosure of social media users Does control over personal information, user awareness and security notices matter?
7	(Berezowska, Fischer, Ronteltap, van der Lans, & van Trijp, 2015)	Consumer adoption of personalized nutrition services from the perspective of a risk-benefit trade-off.
8	(Bernstein, 2017)	Making transparency: The evolution of observation in management theory.
9	(Borena, Belanger, & Ejigu, 2015)	Information privacy protection practices in Africa: A review through the lens of critical social theory.
10	(Buettner, 2015)	Analyzing the problem of employee internal social network site avoidance: Are users resistant due to their privacy concerns?
11	(Chang & Chen, 2014)	Aligning principal and agent's incentives: A principal-agent perspective of social networking sites.
12	(Chatterjee, Moody, Lowry, Chakraborty, & Hardin, 2015)	Strategic relevance of organizational virtues enabled by information technology in organizational innovation.
13	(W. Chen & Scott, 2014)	Shoppers' perceived embeddedness and its impact on purchasing behavior at an organic farmers' market.
14	(Choi, Jiang, Ramesh, & Dong, 2015)	Privacy tradeoff and social application usage.
15	(Dienlin & Metzger, 2016)	An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample.
16	(Dinev et al., 2015)	Informing privacy research through information systems, psychology, and behavioral Economics: Thinking outside the "APCO" box.
17	(Ertz, Durif, & Arcand, 2018)	Business at the fingertips of consumers: a scale for measuring resale motivations in online settings.
18	(Gao & Waechter, 2017)	Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation.
19	(Gao, Waechter, & Bai, 2015)	Understanding consumers' continuance intention towards mobile purchase: A theoretical framework and empirical study - A case of China.
20	(Guo, Zhang, & Sun, 2016)	The privacy-personalization paradox in m-Health services acceptance of different age groups.
21	(Gurung & Raja, 2016)	Online privacy and security concerns of consumers.
22	(James, Warkentin, & Collignon, 2015)	A dual privacy decision model for online social networks.
23	(Karwatzki, Trenz, Tuunainen, & Veit, 2017)	Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organizational influence.
24	(H. Li, Luo, Zhang, & Xu, 2017)	Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors.
25	(K. Li, Lin, & Wang, 2015)	An empirical analysis of users' privacy disclosure behaviors on social network sites.
26	(K. Li, Wang, Li, & Che, 2016)	Information privacy disclosure on social network sites.
27	(L. Li, Gao, & Mao, 2014)	Research on IT in China: a call for greater contextualization.
28	(Liu, Shan, Bonazzi, & Pigneur, 2014)	Privacy as a tradeoff: Introducing the notion of privacy calculus for context-aware mobile applications.
29	(Lowry, Moody, & Chatterjee, 2017)	Using IT design to prevent cyberbullying.
30	(Mamonov & Benbunan-Fich, 2017)	Exploring factors affecting social e-commerce service adoption: The case of Facebook Gifts.

#	Author(s)	Paper
31	(Moshki & Barki, 2016)	An exploratory study on behavioral and emotional coping with IT-enabled government surveillance.
32	(Nunan & Di Domenico, 2017)	Big data: A normal accident waiting to happen?
33	(Ozdemir, Smith, & Benamati, 2017)	Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study.
34	(Pan, Wan, Fan, Liu, & Archer, 2017)	Raising the cohesion and vitality of online communities by reducing privacy concerns.
35	(Park & Chung, 2017)	Health privacy as sociotechnical capital.
36	(Pentina, Zhang, Bata, & Chen, 2016)	Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison.
37	(Pinho, Franco, & Mendes, 2018)	Web portals as tools to support information management in higher education institutions: A systematic literature review.
38	(Ruivo, Oliveira, & Santos, 2015)	Measuring customer data protection in nearshores.
39	(Ruivo, Santos, & Oliveira, 2014)	Data protection in services and support roles - qualitative research amongst ICT professionals
40	(Ruivo, Santos, & Oliveira, 2015)	Success Factors for Data Protection in Services and Support Roles: Combining Traditional Interviews with Delphi Method
41	(Sigmund, 2014)	Privacy in the information society: how to deal with its ambiguity.
42	(Sokolovska & Kocarev, 2018)	Integrating technical and legal concepts of privacy.
43	(Spiekermann, Acquisti, Boehme, & Hui, 2015)	The challenges of personal data markets and privacy.
44	(Triberti & Barello, 2016)	The quest for engaging AmI: Patient engagement and experience design tools to promote effective assisted living.
45	(Vance, Anderson, Kirwan, & Eargle, 2014)	Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG).
46	(Windels et al., 2018)	My friend likes this brand: Do ads with social context attract more attention on social networking sites?
47	(Xiao & Benbasat, 2018)	An empirical examination of the influence of biased personalized product recommendations on consumers' decision making outcomes.
48	(X. Zhang, Guo, Wu, Lai, & Vogel, 2017)	Exploring the inhibitors of online health service use intention: A status quo bias perspective.
49	(Zhou, 2015)	The effect of network externality on mobile social network site continuance.
50	(Zhou, 2016a)	The effect of perceived justice on LBS users' privacy concern.
51	(Zhou, 2016b)	Understanding continuance usage of mobile social network sites.
52	(Zhou, 2017)	Understanding location-based services users' privacy concern An elaboration likelihood model perspective.
53	(Zhou & Li, 2014)	Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern.
54	(Zhu, Ou, van den Heuvel, & Liu, 2017)	Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making.

5. GENERAL CONCLUSION

This thesis analyzed the antecedents and consequences of PC in the context of m-banking, which we define as MBIPC. We used PMT as the theoretical perspective. Due to the complexity of the theme, this study was conducted in three papers.

The first paper (Chapter 2) focused on developing and assessing the MBIPC scale. In the last three decades, many studies have been perfecting an instrument to measure information privacy concerns; however, privacy attitudes are often measured in an ad hoc manner using questionnaires instead of reusing measurement instruments. The reuse of a scale has two main advantages: it advances state of the art to build on prior work, and it makes high-quality measures available for the current research (Preibusch, 2013). Thus, based on these arguments, instead of developing a new scale from scratch to measure MBIPC, we replicated the IPC scale adjusting the original survey items to the context of mobile banking and followed the same procedures of the original study to assess the scale. This replication study supports the findings of the original research, demonstrating that the initially developed scale is stable over time and applicable to different contexts, both technical and cultural. Therefore, we shed light on an adapted instrument that may help in future studies about m-banking and financial information privacy.

In the second paper (Chapter 3), we used the PMT and PC literature to examine how perceived threat severity, perceived threat vulnerability, fear, response costs, self-efficacy, and response efficacy impact MBIPC. Perceived threats regarding the use of m-banking could stimulate fear and PC, consequently affecting the perception of trust in this technology. We found strong support for most of the proposed relationships in the study. Our contribution resides in the fact that we extended previous studies by including PMT components, especially fear in the model. Moreover, to the best of our knowledge, no existing model deals with the specific characteristics of financial information privacy concerns.

In the third paper (Chapter 4) we tested our full model in two different studies using deception: one lab experiment using emotion detection technology, and one online experiment. We found that the majority of PMT constructs and the emotion of fear, never studied before in the context of privacy, influence PC. The implication is that when an m-banking user is stimulated by a fear appeal message, the fear of losing information increases, consequently activating PC and inducing the user to use this platform more securely.

Finally, these three studies make a contribution to the APCO framework. This framework summarized a significant part of the empirical research on PC and concluded that little attention had been paid to the antecedents of PC (Smith et al. 2011; Dinev et al. 2015, p. 647). Furthermore, despite the fact that PC is intuitively associated with security (Flavián and Guinalíu, 2006) and PMT has been used in the IS security literature, so far, to the best of our knowledge, no previous study has tested the full nomology of PMT as an antecedent of PC. Thus, expanding the existing literature, we theorized and tested PMT as an antecedent of PC. Our results provided substantial empirical evidence that MBIPC can be explained by the preconized components of PMT.

6. REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237-248.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

Addae, J. H., Brown, M., Sun, X., Towey, D., & Radenkovic, M. (2017). Measuring attitude towards personal data for adaptive cybersecurity. *Information and Computer Security, 25*(5), 560-579.

Alashoor, T., Han, S., & Joseph, R. C. (2017). Familiarity with Big Data, Privacy Concerns, and Self-disclosure Accuracy in Social Networking Websites: An APCO Model. *Communications of the Association for Information Systems, 41*, 62-96.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643.

Arbuckle, J. L. (2015). *Amos™ 23 User's Guide*. Crawfordville, FL: Amos Development Corporation.

Baek, Y. M. B., Young; Jeong, Irkwon; Kim, Eunmee; Rhee, June Woong. (2014). Changing the default setting for information privacy protection: What and whose personal information can be better protected? *Social Science Journal, 51*(4), 523-533.

Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems, 49*(2), 138-150.

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56*, 147-154.

Bearden, W. O., & Netemeyer, R. G. (1999). *Handbook of marketing scales: Multi-item measures for marketing and consumer behavior research*. Thousand Oaks, CA, USA: Sage.

Bélanger, F., & Crossler, R. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly, 35*(4), 1017-A1036.

Belanger, F., & Xu, H. (2015). The role of information systems research in shaping the future of information privacy. *Information Systems Journal, 25*(6), 573-578.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society, 20*(5), 313-324.

Benamati, J. H., Ozdemir, Z. D., & Smith, H. J. (2017). An empirical test of an Antecedents - Privacy Concerns - Outcomes model. *Journal of Information Science, 43*(5), 583-600.

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users Does control over personal information, user awareness and security notices matter? *Information Technology & People, 28*(3), 426-441.

Berezowska, A., Fischer, A. R. H., Ronteltap, A., van der Lans, I. A., & van Trijp, H. C. M. (2015). Consumer adoption of personalised nutrition services from the perspective of a risk-benefit trade-off. *Genes and Nutrition, 10*(6).

Bernstein, E. S. (2017). Making Transparency Transparent: The Evolution of Observation in Management Theory. *Academy of Management Annals, 11*(1), 217-266.

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: towards an intervention strategy for college students. *Behaviour & Information Technology, 34*(10), 1022-1035.

Borena, B., Belanger, F., & Ejigu, D. (2015). *Information Privacy Protection Practices in Africa: A Review Through the Lens of Critical Social Theory*. Paper presented at 48th Hawaii International Conference on System Sciences (pp. 3490-3497).

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & 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.

Bowie, N. E., & Jamal, K. (2006). Privacy Rights on the Internet: Self-regulation or Government Regulation? *Business Ethics Quarterly, 16*(3), 323-342.

Breaban, A., & Noussair, C. N. (2018). Emotional State and Market Behavior. *Review of Finance, 22*(1), 279-309.

Buettner, R. (2015). *Analyzing the Problem of Employee Internal Social Network Site Avoidance: Are Users Resistant due to their Privacy Concerns?* Paper presented at 48th Hawaii International Conference on System Sciences (pp. 1819-1828).

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on psychological science, 6*(1), 3-5.

Burton-Jones, A. (2009). Minimizing Method Bias through Programmatic Research. *MIS Quarterly, 33*(3), 445-471.

Census. (2017). *The Nation's Median Age Continues to Rise*. Retrieved March 21, 2019, from https://www.census.gov/content/dam/Census/library/visualizations/2017/comm/cb17-100-median-age.pdf

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and Online Information Privacy: An Exploratory Study of Preteens and Early Teens. *IEEE Transactions on Professional Communication, 52*(2), 167-182.

Chang, L., & Chen, J. V. (2014). Aligning principal and agent's incentives: A principal-agent perspective of social networking sites. *Expert Systems with Applications, 41*(6), 3091-3104.

Chatterjee, S., Moody, G., Lowry, P. B., Chakraborty, S., & Hardin, A. (2015). Strategic Relevance of Organizational Virtues Enabled by Information Technology in Organizational Innovation. *Journal of Management Information Systems, 32*(3), 158-196.

Chen, W., & Scott, S. (2014). Shoppers' perceived embeddedness and its impact on purchasing behavior at an organic farmers' market. *Appetite, 83*, 57-62.

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly, 40*(1), 205-222.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling *Methodology for business and management. Modern methods for business research* (Vol. 295, pp. 295-336). Mahwah, NJ, US: Lawrence Erlbaum Associates Publishers.

Choi, B. C. F., Jiang, Z. J., Ramesh, B., & Dong, Y. (2015). *Privacy Tradeoff and Social Application Usage*. Paper presented at 48th Hawaii International Conference on System Sciences (pp. 304-313).

Chou, H. L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior, 65*, 334-345.

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems, 52*(4), 20-29.

Compeau, D., Marcolin, B., Kelley, H., & Higgins, C. (2012). Research commentary—Generalizability of information systems research using student subjects—A reflection on our practices and recommendations for future research. *Information Systems Research, 23*(4), 1093-1109.

Compeau, D. R., & Higgins, C. A. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly, 19*(2), 189-211.

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 45*(4), 51-71.

Crossler, R., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.

Crossler, R., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209-226.

Crump, M. J., McDonnell, J. V., & Gureckis, T. M. (2013). Evaluating Amazon's Mechanical Turk as a tool for experimental behavioral research. *Plos One, 8*(3), e57410.

Culnan, M. J. (1993). "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. *MIS Quarterly, 17*(3), 341-363.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security, 48*, 281-297.

Deloitte. (2018). Pesquisa de Tecnologia Bancária 2018. 2018. Retrieved March 21, 2019, from https://www2.deloitte.com/content/dam/Deloitte/br/Documents/financial-services/Pesquisa%20Deloitte%20Febraban%202018.pdf

Dennis, A. R., & Valacich, J. S. (2014). A replication manifesto. *AIS Transactions on Replication Research, 1*(1), 1.

Dienlin, T., & Metzger, M. J. (2016). An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative US Sample. *Journal of Computer-Mediated Communication, 21*(5), 368-383.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology, 23*(6), 413-422.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*(1), 61.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research, 26*(4), 639-655.

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

Earp, J. B., & Baumer, D. (2003). Innovative Web Use to Learn about Consumer Behavior and Online Privacy. *Communication of the ACM, 46*(4), 81-83.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment. *Journal of Business Research, 59*(8), 877-886.

Economist. (2017, 09/16/2017). The big data breach suffered by Equifax has alarming implications. *Economist*. Retrieved March 21, 2019, from https://www.economist.com/news/finance-and-economics/21728956-financial-industry-worries-about-who-next-big-data-breach-suffered

Ekman, P. (2007). *Emotions revealed: Recognizing faces and feelings to improve communication and emotional life*: Macmillan.

Ekman, P., & Friesen, W. V. (1971). Constants across cultures in the face and emotion. *Journal of personality and social psychology, 17*(2), 124.

Ertz, M., Durif, F., & Arcand, M. (2018). Business at the fingertips of consumers: a scale for measuring resale motivations in online settings. *International Review of Retail Distribution and Consumer Research, 28*(1), 92-114.

Fed. (2016). Consumers and Mobile Financial Services. Retrieved March 21, 2019, from https://www.federalreserve.gov/consumerscommunities/mobile_finance.htm

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

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

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 39-50.

Forrester. (2017). North American Mobile Banking Benchmark: User Experience, 2017. Retrieved March 21, 2019, from https://www.forrester.com/Mobile-Banking

Fort, K., Adda, G., & Cohen, K. B. (2011). Amazon mechanical turk: Gold mine or coal mine? *Computational Linguistics, 37*(2), 413-420.

FTC. (2017). The Equifax Data Breach: What to Do. Retrieved March 21, 2019, from https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

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

Gao, L., Waechter, K. A., & Bai, X. (2015). Understanding consumers' continuance intention towards mobile purchase: A theoretical framework and empirical study - A case of China. *Computers in Human Behavior, 53*, 249-262.

Gartner. (2018). 2019 CIO Agenda: Banking and Investment Services Industry Insights. Retrieved March 21, 2019, from https://www.gartner.com/document/3891248

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51-90.

Goldberg, J. H. (2014). Measuring software screen complexity: Relating eye tracking, emotional valence, and subjective ratings. *International Journal of Human-Computer Interaction, 30*(7), 518-532.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). Users Compensation as a Data Breach Recovery Action: An Investigation of the Sony Playstation Network Breach. *MIS Quarterly, 41*(3).

Goodman, J. K., Cryder, C. E., & 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.

Guo, X., Zhang, X., & Sun, Y. (2016). The privacy-personalization paradox in mHealth services acceptance of different age groups. *Electronic Commerce Research and Applications, 16*, 55-65.

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: an empirical investigation. *Information Management & Computer Security, 17*(3), 276-289.

Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumers. *Information and Computer Security, 24*(4), 348-371.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2013). *Multivariate Data Analysis* (7th edition ed.). NY: Pearson.

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management, 33*(1), 2-16.

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

Hong, W., & Thong, J. Y. L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly, 37*(1), 275-298.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100.

James, T. L., Warkentin, M., & Collignon, S. E. (2015). A dual privacy decision model for online social networks. *Information & Management, 52*(8), 893-908.

Jarvenpaa, S. L., & Tiller, E. H. (1999). Integrating market, technology, and policy opportunities in e-business strategy. *The Journal of Strategic Information Systems, 8*(3), 235-249.

Javelin. (2018). Identity Fraud: Fraud Enters a New Era of Complexity. Retrieved March 21, 2019, from https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin

Jia, H., & Xu, H. (2015). *Measuring Individuals' Concerns over Collective Privacy on Social Networking Sites.* Paper presented at ICIS 2015 Proceedings.

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

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113-134.

Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (2017). Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems, 26*(6), 688-715.

Kenny, G., & Connolly, R. (2017). *Examining Citizens' Health Information Privacy Concerns: An Extension of the IPC Instrument*. Paper presented at 2017 AMCIS Proceedings.

Lai, F., Li, D., & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems, 52*(2), 353-363.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues, 33*(3), 22-42.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology, 27*(5), 445-454.

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems, 50*(2), 361-369.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Leventhal, H. (1970). Findings and Theory in the Study of Fear Communications. *Advances in Experimental Social Psychology, 5*, 119-186.

Lewinski, P., den Uyl, T. M., & Butler, C. (2014). Automated facial coding: Validation of basic emotions and FACS AUs in FaceReader. *Journal of Neuroscience, Psychology, and Economics, 7*(4), 227.

Li, H., Luo, X., Zhang, J., & Xu, H. (2017). Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information & Management, 54*(8), 1012-1022.

Li, H., Sarathy, R., & Zhang, J. (2008). The role of emotions in shaping consumers' privacy beliefs about unfamiliar online vendors. *Journal of Information Privacy and Security, 4*(3), 36-62.

Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information & Management, 52*(7), 882-891.

Li, K., Wang, X., Li, K., & Che, J. (2016). Information privacy disclosure on social network sites An empirical investigation from social exchange perspective. *Nankai Business Review International, 7*(3), 282-300.

Li, L., Gao, P., & Mao, J.-Y. (2014). Research on IT in China: a call for greater contextualization. *Journal of Information Technology, 29*(3), 208-222.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *MIS Quarterly*, 71-90.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394.

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

Litman, L., Robinson, J., & Rosenzweig, C. (2015). The relationship between motivation, monetary compensation, and data quality among US-and India-based workers on Mechanical Turk. *Behavior research methods, 47*(2), 519-528.

Liu, Z., Shan, J., Bonazzi, R., & Pigneur, Y. (2014). *Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications.* Paper presented at 47th Hawaii International Conference on System Sciences (pp. 1063-1072).

Loijens, L., Krips, O., Kuilenburg, U. M., & Ivan, P. F. (2015). *Facereader 6.1 Reference Manual*. Wageningen, NL: Noldus Information Technology.

Lowry, P. B., Moody, G. D., & Chatterjee, S. (2017). Using IT Design to Prevent Cyberbullying. *Journal of Management Information Systems, 34*(3), 863-901.

Lwin, M. O., Li, B., & Ang, R. P. (2012). Stop bugging me: An examination of adolescents' protection behavior against online harassment. *Journal of Adolescence, 35*(1), 31-41.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques. *MIS Quarterly, 35*(2), 293-334.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479.

Malcolm, P., Cate, J., Kathryn, P., Agata, M., & Marcus, B. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security, 20*(1), 18-28.

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Management Science, 52*(12), 1865-1883.

Malhotra, N. K., Sung, S. K., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355.

Mamonov, S., & Benbunan-Fich, R. (2017). Exploring factors affecting social e-commerce service adoption: The case of Facebook Gifts. *International Journal of Information Management, 37*(6), 590-600.

Martin, K., & Shilton, K. (2016). Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology, 67*(8), 1871-1882.

McIntosh, D. N., Zajonc, R. B., Vig, P. S., & Emerick, S. W. (1997). Facial movement, breathing, temperature, and affect: Implications of the vascular theory of emotional efference. *Cognition & Emotion, 11*(2), 171-196.

McKinsey. (2017, 01/2017). The Winning Formula for Omnichannel Banking in North America. *Retail Banking Insights, 9*, 9.

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security, 9*(1), 47-67.

Metzger, M. J. (2004). Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication, 9*(4).

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs, 43*(3), 449-473.

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British journal of health psychology, 7*(2), 163-184.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106-143.

MirandaVsArizona. (1966). *384 U.S. 436*. US Supreme Court: JUSTIA Retrieved March 21, 2019, from https://supreme.justia.com/cases/federal/us/384/436/.

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

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, 28*(6), 2366-2375.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1).

Moshki, H., & Barki, H. (2016). *An Exploratory Study on Behavioral and Emotional Coping with IT-Enabled Government Surveillance*. Paper presented at 49th Annual Hawaii International Conference on System Sciences (pp. 3636-3645).

NCSL. (2018). Security Breach Notification Laws. Retrieved March 21, 2019, from http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Ng, B.-Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Niederman, F., & March, S. (2015). Reflections on replications. *AIS Transactions on Replication Research, 1*(1), 1-16.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev., 79*, 119.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs, 41*(1), 100-126.

Nunan, D., & Di Domenico, M. (2017). Big Data: A Normal Accident Waiting to Happen? *Journal of Business Ethics, 145*(3), 481-491.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed. ed.): New York: McGraw-Hill.

Nwadike, U., Groß, T., & Coopamootoo, K. P. L. (2016). Evaluating Users' Affect States: Towards a Study on Privacy Concerns. In A. Lehmann, D. Whitehouse, S. Fischer-Hübner, L. Fritsch, & C. Raab (Eds.), *Privacy and Identity Management* (pp. 248-262). Cham: Springer International Publishing.

Osatuyi, B. (2015). Empirical examination of information privacy concerns instrument in the social media context. *AIS Transactions on Replication Research, 1*(1), 1-14.

Osman, A., Barrios, F. X., Osman, J. R., Schneekloth, R., & Troutman, J. A. (1994). The Pain Anxiety Symptoms Scale: psychometric properties in a community sample. *Journal of behavioral medicine, 17*(5), 511-522.

Ozdemir, Z. D., Smith, H. J., & Benamati, J. H. (2017). Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems, 26*(6), 642-660.

Pan, Y., Wan, Y., Fan, J., Liu, B., & Archer, N. (2017). Raising the Cohesion and Vitality of Online Communities by Reducing Privacy Concerns. *International Journal of Electronic Commerce, 21*(2), 151-183.

Paolacci, G., & Chandler, J. (2014). Inside the Turk: Understanding Mechanical Turk as a participant pool. *Current Directions in Psychological Science, 23*(3), 184-188.

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running Experiments on Amazon Mechanical Turk. *Judgment and Decision Making, 5*(5), 9.

Park, Y. J., & Chung, J. E. (2017). Health privacy as sociotechnical capital. *Computers in Human Behavior, 76*, 227-236.

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce, 7*(3), 101-134.

Pavlou, P. A. (2011). State of the information privacy literature: where are we now and where should we go? *MIS Quarterly, 35*(4), 977-988.

Pavlou, P. A., & Gefen, D. (2004). Building Effective Online Marketplaces with Institution-Based Trust. *Information Systems Research, 15*(1), 37-59.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. *MIS Quarterly*(1), 105.

Peer, E., Vosgerau, J., & Acquisti, A. (2014). Reputation as a sufficient condition for data quality on Amazon Mechanical Turk. *Behavior research methods, 46*(4), 1023-1031.

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior, 65*, 409-419.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*: Suny Press.

Pew, R. C. (2018). Mobile Fact Sheet. Retrieved March 21, 2019, from http://www.pewinternet.org/fact-sheet/mobile/

Pinho, C., Franco, M., & Mendes, L. (2018). Web portals as tools to support information management in higher education institutions: A systematic literature review. *International Journal of Information Management, 41*, 80-92.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies, 71*(12), 1133-1143.

Rand, D. G. (2012). The promise of Mechanical Turk: How online labor markets can help theorists run behavioral experiments. *Journal of theoretical biology, 299*, 172-179.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), 93-114.

Rogers, R. W. (1983). *Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation*.

Rosenberg, M. (1965). *Society and the adolescent self-image*. Princeton, NJ: Princeton University Press.

Ross, A. (2015, 09/09/2015). 11 data breaches that stung US consumers. *Bloomberg*. Retrieved March 21, 2019, from http://www.bankrate.com/finance/banking/us-data-breaches-1.aspx#slide=5

Ruivo, P., Oliveira, T., & Santos, V. (2015). *Measuring customer data protection in nearshores.* Paper presented at 2015 Conference on Enterprise Information Systems (Vol. 64, pp. 610-617).

Ruivo, P., Santos, V., & Oliveira, T. (2014). *Data protection in services and support roles - a qualitative research amongst ICT professionals.* Paper presented at 2014 Conference on Enterprise Information Systems (Vol. 16, pp. 710-717).

Ruivo, P., Santos, V., & Oliveira, T. (2015). Success Factors for Data Protection in Services and Support Roles: Combining Traditional Interviews with Delphi Method. *International Journal of Human Capital and Information Technology Professionals, 6*(3), 56-70.

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and customer willingness to provide information in database-driven relationship marketing. *Journal of Interactive Marketing, 16*(3), 2-16.

Schouten, D. G., Venneker, F., Bosse, T., Cremers, A., & Neerincx, M. A. (2017). A Digital Coach that Provides Affective and Social Learning Support to Low-Literate Learners. *IEEE Transactions on Learning Technologies, 11*(1), 67-80.

Sheehan, K. B., & Hoy, M. G. (1999). Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *Journal of Advertising, 28*(3), 37-51.

Sigmund, T. (2014). *Privacy in the Information Society: How to Deal with its Ambiguity?* (Vol. 43).

Simcox, T., & Fiez, J. A. (2014). Collecting response times using amazon mechanical turk and adobe flash. *Behavior research methods, 46*(1), 95-111.

Sipior, J. C., Ward, B. T., & Connolly, R. (2013). Empirically assessing the continued applicability of the IUIPC construct. *Journal of Enterprise Information Management, 26*(6), 661-678.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43*(2), 64-71.

Sirletti, S., & Robinson, E. (2016, 26/07/2016). Hackers Breach 400,000 UniCredit Bank Accounts for Data. *Bloomberg*. Retrieved March 21, 2019, from https://www.bloomberg.com/news/articles/2017-07-26/unicredit-says-400-000-clients-affected-by-security-breach

Slovic, P., & Peters, E. (2006). Risk perception and affect. *Current Directions in Psychological Science, 15*(6), 322-325.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly, 35*(4), 980-A927.

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

Sokolovska, A., & Kocarev, L. (2018). Integrating Technical and Legal Concepts of Privacy. *Ieee Access, 6*, 26543-26557.

Soper, D. S. (2018). A-priori Sample Size Calculator for Structural Equation Models. Internet. Retrieved March 21, 2019, from http://www.danielsoper.com/statcalc

Spiekermann, S., Acquisti, A., Boehme, R., & Hui, K.-L. (2015). The challenges of personal data markets and privacy. *Electronic Markets, 25*(2), 161-167.

Sprouse, J. (2011). A validation of Amazon Mechanical Turk for the collection of acceptability judgments in linguistic theory. *Behavior research methods, 43*(1), 155-167.

Steelman, Z. R., Hammer, B. I., & Limayem, M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly, 38*(2), A1-A20.

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

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68*(3), 459-468.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *The Communications of the Association for Information Systems, 13*(1), 63.

Terlizzi, M. A., Meirelles, F. d. S., & Cunha, M. A. V. C. d. (2017). Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance. *Journal of Applied Security Research, 12*(2), 224-252. doi:10.1080/19361610.2017.1277886

Triberti, S., & Barello, S. (2016). The quest for engaging AmI: Patient engagement and experience design tools to promote effective assisted living. *Journal of Biomedical Informatics, 63*, 150-156.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective. *Computers & Security, 59*, 138-150.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG). *Journal of the Association for Information Systems, 15*(10), 679-722.

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

Ware, W. H. (1973). *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. Washington: US Department of Health, Education & Welfare.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220.

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

Westland, C. J. (2010). Lower bounds on sample size in structural equation modeling. *Electronic Commerce Research and Applications, 9*(6), 476-487.

Weth, K., Raab, M. H., & Carbon, C.-C. (2015). Investigating emotional responses to self-selected sad music via self-report and automated facial analysis. *Musicae Scientiae, 19*(4), 412-432.

Windels, K., Heo, J., Jeong, Y., Porter, L., Jung, A. R., & Wang, R. (2018). My friend likes this brand: Do ads with social context attract more attention on social networking sites? *Computers in Human Behavior, 84*, 420-429.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*(4), 329-349.

Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of health communication, 1*(4), 317-342.

Witte, K. (1998). Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. In P. A. Anderson & L. K. Guerrero (Eds.), *Handbook of Communication and Emotion: Research, Theory, and Contexts* (pp. 423-450). San Diego, CA: Academic Press.

Woodman, R. W., Ganster, D. C., Adams, J., McCuddy, M. K., Tolchinsky, P. D., & Fromkin, H. (1982). A Survey of Employee Perceptions of Information Privacy in Organizations. *Academy of Management Journal, 25*(3), 647-663.

Woon, I., Tan, G.-W., & Low, R. (2005). *A Protection Motivation Theory Approach to Home Wireless Security*. Paper presented at the ICIS 2005 Proceedings.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Xiao, B., & Benbasat, I. (2018). An empirical examination of the influence of biased personalized product recommendations on consumers' decision making outcomes. *Decision Support Systems, 110*, 46-57.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems, 12*(12), 798-824.

Xu, H., & Teo, H.-H. (2004). *Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective.* Paper presented at the ICIS 2004 Proceedings.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2012). Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information Systems Research, 23*(4), 1342-1363.

Yang, J., Zhang, Y., & Lanting, C. J. M. (2017). Exploring the Impact of QR Codes in Authentication Protection: A Study Based on PMT and TPB. *Wireless Personal Communications, 96*(4), 5315-5334.

Yoon, C., Hwang, J.-W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education, 23*(4), 407.

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86-110.

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents. *Journal of Consumer Affairs, 43*(3), 389-418.

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce, 8*(3-4), 180-197.

Zhang, P. (2013). The affective response model: A theoretical framework of affective concepts and their relationships in the ict context. *MIS Quarterly, 37*(1), 247-274.

Zhang, X., Guo, X., Wu, Y., Lai, K.-h., & Vogel, D. (2017). Exploring the inhibitors of online health service use intention: A status quo bias perspective. *Information & Management, 54*(8), 987-997.

Zhou, T. (2015). The effect of network externality on mobile social network site continuance. *Program-Electronic Library and Information Systems, 49*(3), 289-304.

Zhou, T. (2016a). The effect of perceived justice on LBS users' privacy concern. *Information Development, 32*(5), 1730-1740.

Zhou, T. (2016b). Understanding Continuance Usage of Mobile Social Network Sites. *International Journal of Mobile Human Computer Interaction, 8*(3), 38-51.

Zhou, T. (2017). Understanding location-based services users' privacy concern An elaboration likelihood model perspective. *Internet Research, 27*(3), 506-519.

Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior, 37*, 283-289.

Zhu, H., Ou, C. X. J., van den Heuvel, W. J. A. M., & Liu, H. (2017). Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making. *Information & Management, 54*(4), 427-437.