Transactions on Replication Research

Conceptual Replication DOI: 10.17705/1atrr.00040 ISSN 2473-3458

Replication of Internet Privacy Concerns in the Mobile Banking Context

Marco Alexandre Terlizzi
Sao Paulo Business School
Fundacao Getulio Vargas (FGV), Brazil
marco.terlizzi@fgv.edu.br

Laura Brandimarte
Eller College of Management
The University of Arizona, USA
lbrandimarte@email.arizona.edu

Otavio Próspero Sanchez
Sao Paulo Business School
Fundacao Getulio Vargas (FGV), Brazil
otavio.sanchez@fgv.br

Abstract:

This study is a conceptual replication of the work of Hong and Thong (2013), who developed the Internet Privacy Concerns scale to measure individuals' concerns regarding how personal information is handled by websites. We adapt the wording of the original survey items to the context of mobile banking and follow the same procedures to assess the scale. The replication results reinforce the stability and applicability of the scale over the years and in different scenarios. In contrast with the original study, however, we detect a high correlation between the Control and Awareness dimensions, suggesting the design of an additional second-order dimension that we label "exposure management" (individuals' consciousness about existing controls that mitigate the risks of personal data loss).

Keywords: Internet Privacy Concerns; Mobile Banking; IPC; CFIP; IUIPC

The manuscript was received 05/11/2018 and was with the authors 2 months for 2 revisions.

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.

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.

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, and 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 and 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, and Agarwal (2004)
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, Anton, Aiman-Smith, and Stufflebeam (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, and 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 and Xu (2015)

In this replication study, we assess the scale and nomological network of IPC in the context of mobile banking (m-banking) in order to address the lack of stability confirmation or tests in different scenarios in the literature. 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." The reuse of a scale has three advantages: (1) it advances the 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).

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; Terlizzi, Meirelles, & Cunha, 2017; Woodman et al., 1982). Second, the use of m-banking has been growing steadily (Guzraty, Kelly, Kim, & Ross, 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).

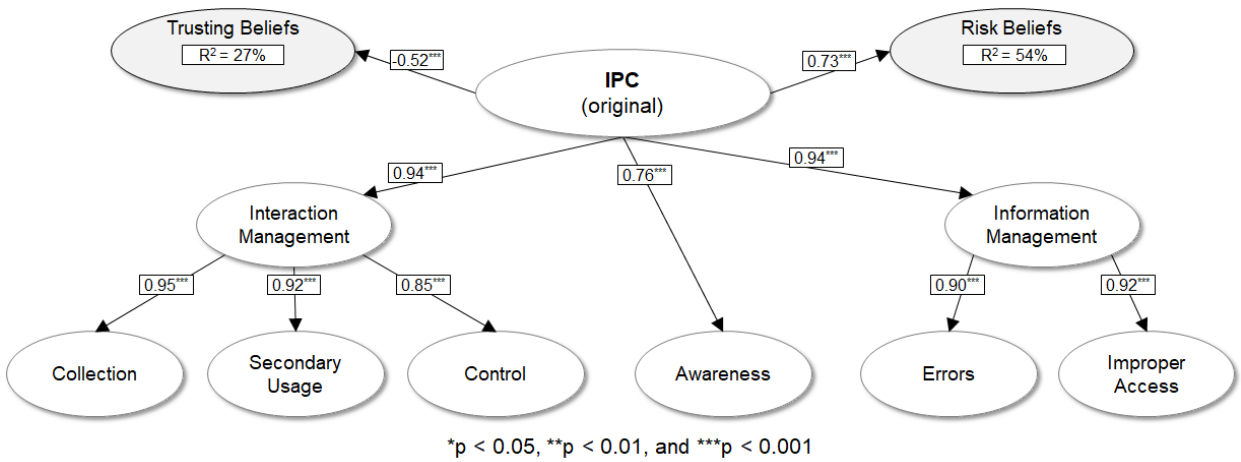


Figure 1. Results of the Original Study

Figure 1 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.

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 replicating IPC in the context of mobile banking and checking for nomological validity of its third-order conceptualization.

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. 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 (see for instance Paolacci and Chandler (2014)).

A priori sample size calculations (https://www.danielsoper.com/statcalc/calculator.aspx?id=89) 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. Census estimates (Census, 2017). Finally, our replication is composed of a similar percentage of females/males as in the original study 4.

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.

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.

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 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

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

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

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
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).

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

GFI = Goodness-of-fit, AGFI = Adjusted goodness-of-fit, NFI = Normalized fit index, CFI = Comparative fit index, RMSR = Root mean square residual, RMSEA = Root mean square error of approximation, 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** (MacKenzie, Podsakoff, & Podsakoff, 2011, p. 313) (Hair, Black, Babin, & Anderson, 2013, p. 584)
	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

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 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.

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
NNFI	0.99	0.95
NNFI = Nonnormed fit index		

The structural model's fit indices (Figure 2) 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.

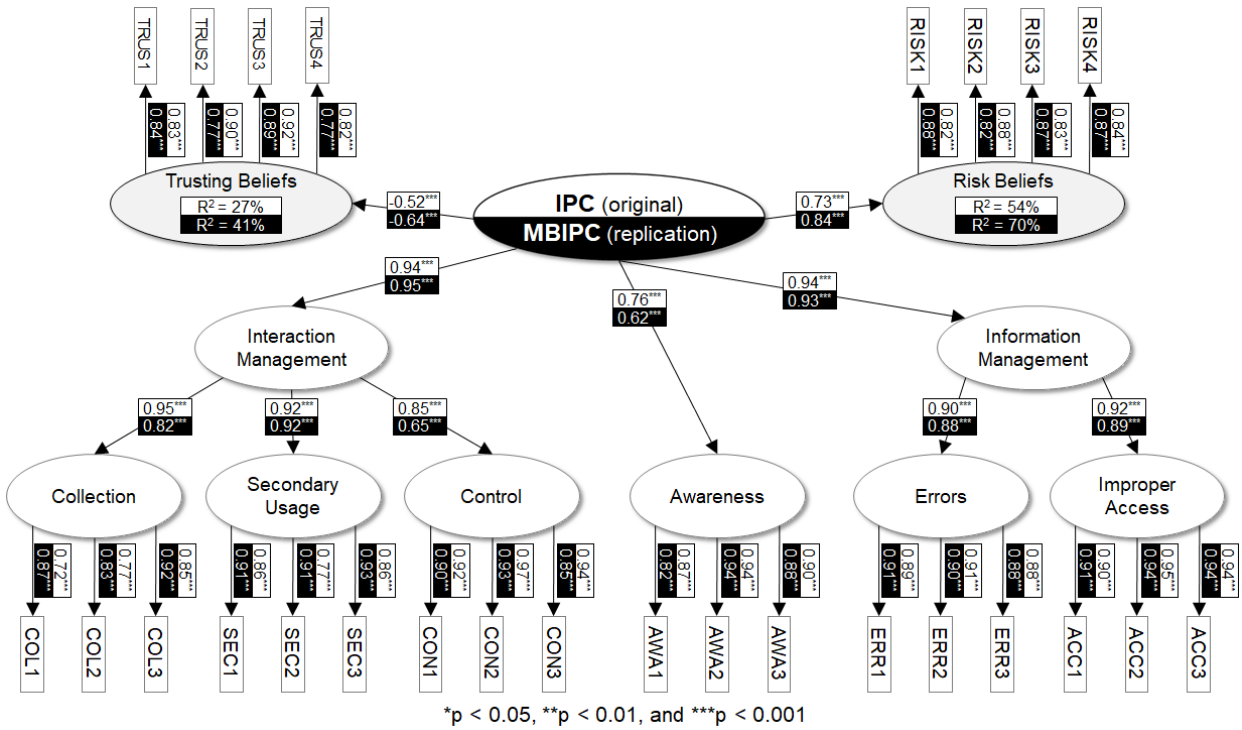


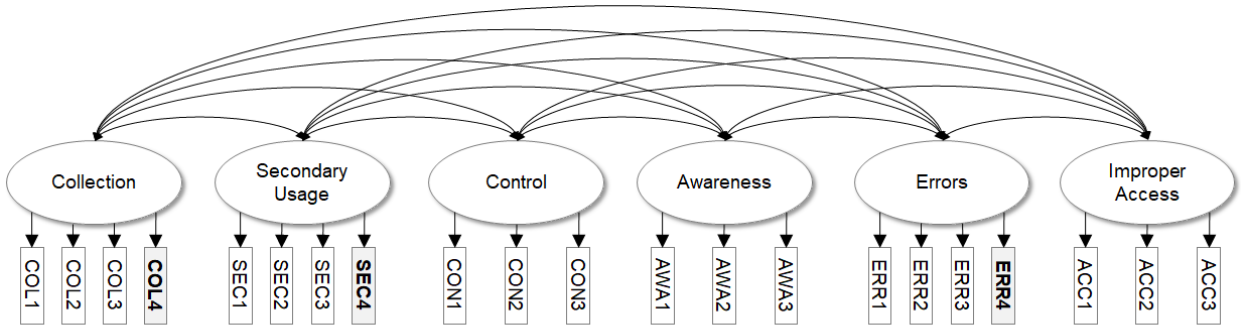
Figure 2. Results of the Original Study and Replication Study

Figure 2 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 paper's, 27% and 54% respectively. Hence, consistent with the original paper, 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, Galletta, Lowry, Moody, & Polak, 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 rsec-s (0.089) as the estimator of rs 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.

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 3) 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.



X2=485.13; df=174; X2/df=2.79; GFI=0.89; AGFI=0.86; NFI=0.94; CFI=0.96; RMSR=.058; RMSEA=0.06

Figure 3. 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 4 and Table 8) 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.

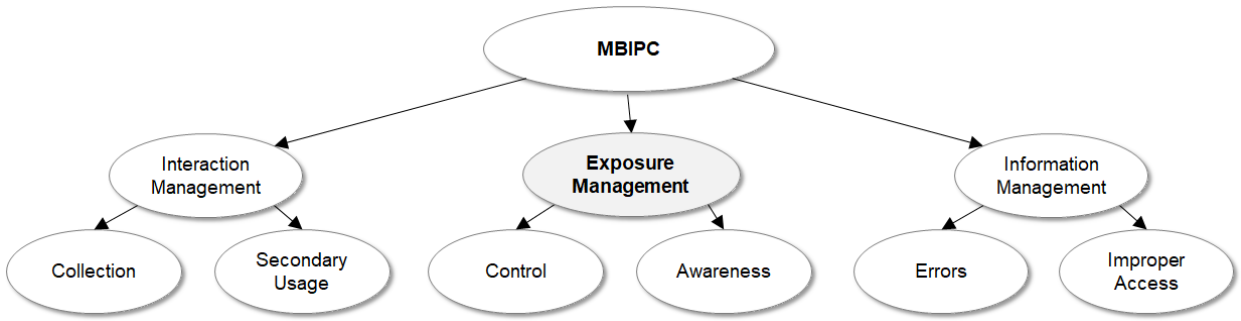


Figure 4. Alternative model 12B with a new dimension "exposure management"

Table 8: Goodness-of-Fit Statistics of the 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. Model 12B (Table 9 and Figure 5) 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 the 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

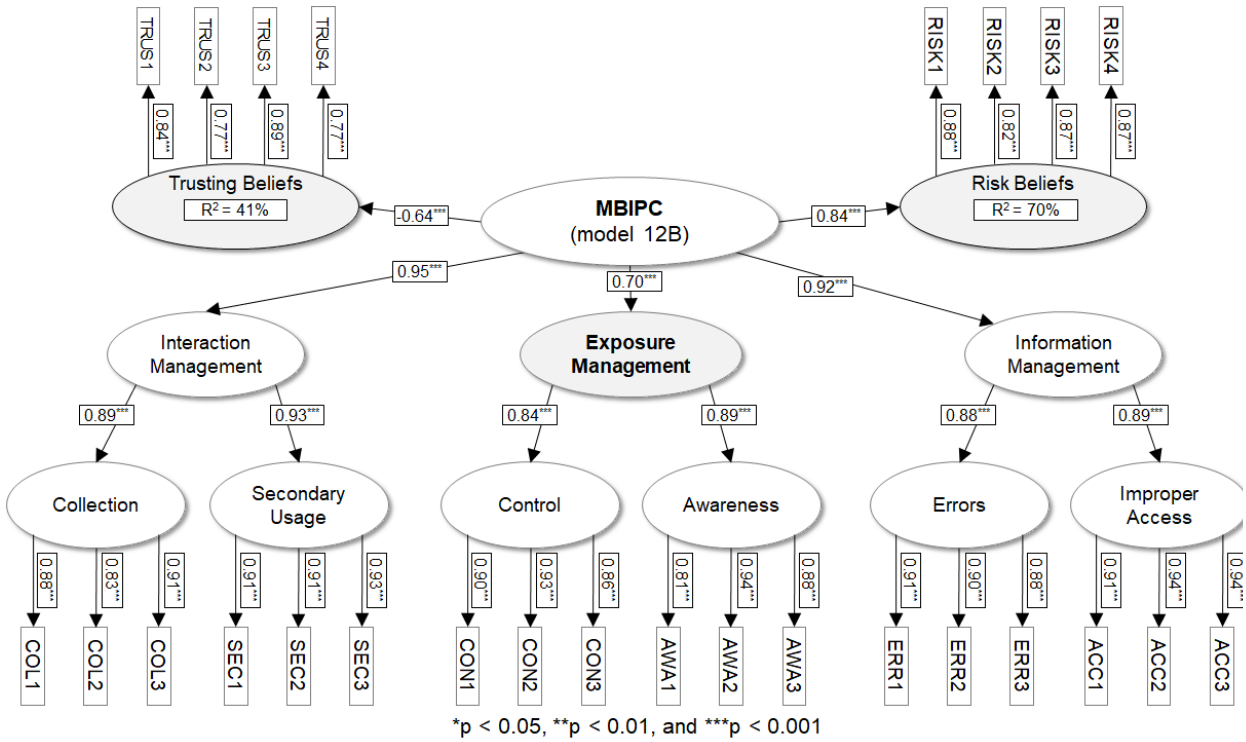


Figure 5. Results of alternative model 12B

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 wide 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.*

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 perfectly 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 (e.g., (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.

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.

Acknowledgments

The authors would like to thank Dr. Matthew Jensen, Senior Editor of the AIS-TRR, Dr. Taylor Wells, Managing Editor of the AIS-TRR, and the two anonymous reviewers who provided many valuable comments that helped to improve the paper.

References

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

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. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017-A1036.

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.

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.

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.

Census. (2017). The nation's median age continues to rise. Retrieved from https://www.census.gov/content/dam/Census/library/visualizations/2017/comm/cb17-100-median-age.pdf

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

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.

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

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.

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

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

Forrester. (2017). North American Mobile Banking Benchmark: User Experience, 2017. Retrieved 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 from https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

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.

Guzraty, T., Kelly, C., Kim, Y., & Ross, E. (2017, 01/2017). The winning formula for omnichannel banking in North America. *Retail Banking Insights*, 9, 9.

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

Hong, W., & Thong, J. Y. L. (2013). Internet privacy concerns: An Integrated conceptualization and four empirical studies. *MIS Quarterly*, 37(1), 275-298.

Jia, H., & Xu, H. (2015). Measuring individuals' concerns over collective privacy on social networking sites. Paper presented at ICIS 2015 Proceedings, Fort Worth, Texas, USA.

Kenny, G., & Connolly, R. (2017). Examining citizens' health information privacy concerns: An extension of the IPC instrument. Paper presented at AMCIS 2017 Proceedings, Boston, MA, USA.

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.

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.

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.

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.

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

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

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

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

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

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.

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.

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

Simcox, T., & Fiez, J. A. (2014). Collecting response times using Amazon Mechanical Turk and Adobe Flash. *Behavior Research Methods*, 46(1), 95-111.

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

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167-196.

Soper, D. S. (2018). A-priori sample size calculator for structural equation models. Retrieved from http://www.danielsoper.com/statcalc

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.

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.

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.

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

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.

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.

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 a mobile banking. Based on Hong and Thong (2013) and previously designed by Smith et al. (1996).

1. It usually bothers me when a mobile banking app or website asks me for personal information.
2. When a mobile banking app or website asks me for personal information, I sometimes think twice before providing it.
3. I am concerned that a mobile banking app or website collects too much personal information about me.
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 a 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).

1. 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.
2. I am concerned that a mobile banking app or website would sell my personal information in their computer databases to other companies.
3. I am concerned that a mobile banking app or website would share my personal information with other companies without my authorization.
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 a mobile banking are inadequate. Based on Hong and Thong (2013) and previously designed by Smith et al. (1996).

1. 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.
2. I am concerned that mobile banking apps or websites do not have adequate procedures to correct errors in my personal information.
3. 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.
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 a 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).

1. I am concerned that mobile banking databases that contain my personal information are not protected from unauthorized access.
2. I am concerned that mobile banking apps or websites do not devote enough time and effort to preventing unauthorized access to my personal information.
3. 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.

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).

1. It usually bothers me when I do not have control of personal information that I provide to a mobile banking app or website.
2. 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.
3. 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 a mobile banking. Based on Hong and Thong (2013) and previously designed by Malhotra et al. (2004).

1. I am concerned when a clear and conspicuous disclosure is not included in the online privacy policies of mobile banking apps or websites.
2. 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.
3. 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).

1. Mobile banking apps and websites, in general, would be trustworthy in handling my personal information.
2. Mobile banking apps and websites would keep my best interests in mind when dealing with my personal information.
3. Mobile banking apps and websites would fulfill their promises related to my personal information.
4. 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 the mobile banking. Based on Hong and Thong (2013) and previously used by Malhotra et al. (2004).

1. In general, it would be risky to give my personal information to mobile banking apps or websites.
2. There would be a high potential for loss associated with giving my personal information to mobile banking apps or websites.
3. There would be too much uncertainty associated with giving my personal information to mobile banking apps or websites.
4. Providing mobile banking apps or websites with my personal information would involve many unexpected problems.Xx

* = Items 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).

About the Authors

Marco Alexandre Terlizzi is a PhD candidate of Business Administration at Sao Paulo Business School from Fundacao Getulio Vargas, Brazil. His research interests revolve around information privacy, security and project management. He serves on the review board for Project Management Journals and Conferences. His research has appeared in journals such as International Journal of Project Management, and Journal of Applied Security Research.

Laura Brandimarte is an Assistant Professor of Management Information Systems at the Eller College of Management, University of Arizona. She obtained her PhD in Public Policy and Management at Carnegie Mellon University. Her research focuses on the behavioral aspects of privacy and security decision making. Her work has been published in major journals, including Science, Journal of Experimental Psychology: General, Journal of Experimental Social Psychology, and ACM Computing Surveys. Her research was also covered by several media outlets, including The New York Times and Pacific Standard. She serves on the Program Committee of several Workshops and Conferences, including the Workshop on the Economics of Information Security.

Otavio Próspero Sanchez is an Associate Professor of IS and Quantitative Methods in FGV - Fundacao Getulio Vargas, Sao Paulo. Previously, he acted as a senior executive of tech companies subsidiaries in Brazil and LA. He holds a Ph.D. and M.Sc. in Business from FGV and a Bachelors in Industrial Electronics from FEI. Currently, his primary research interests direct to Behavioral IS, ranging from topics as gig work, trust, privacy issues, and security, especially in healthcare and recommendation systems. Professor Sanchez's research has appeared in such journals as Communications of the ACM, Information Systems Frontiers, International Journal of Project Management and numerous international conferences.