Transactions on Replication Research

Conceptual Replication DOI: 10.17705/1atrr.00046 ISSN 2473-3458

Are all Internet Users' Information Privacy Concerns (IUIPC) Created Equal?

Miaoyi Zeng
Business Analytics, Information Systems, & Supply Chain, Florida State University
mz18q@my.fsu.edu

Shuaifu Lin
Marilyn Davies College of Business, University of Houston - Downtown
linsh@uhd.edu

Deborah J. Armstrong
Business Analytics, Information Systems, & Supply Chain, Florida State University
djarmstrong@business.fsu.edu

Abstract:

The current study is a conceptual replication of Malhotra, Kim, and Agarwal's (2004) nomological model of internet user information privacy concerns (IUIPC). We empirically tested the same hypotheses and use conceptually similar (but not exact) measures and analyses. In addition, while the original study explored privacy concerns from a customer perspective within an e-commerce context, this replication explored privacy concerns from a participant perspective within a social networking context. By this, we test the boundaries of the original theory and the strength of the relationships. The findings from this replication study were partially consistent with the original study. Specifically, the relationship between IUIPC and risk beliefs was supported, and the relationship between trusting beliefs and behavioral intention (i.e., revelation of private information) was supported. Consistent with the original study, this study found that sensitive information significantly decreased participants' intention to reveal private information. However, several other significant relationships in the original study were found non-significant in the context of this replication study. Future research is impacted by this study as we found that not all online information privacy concerns are created equal.

Keywords: Information Privacy, Trust, Risk, Replication

The manuscript was received 10/24/2019 and was with the authors 1 month for 1 revision.

1 Introduction

In general terms information privacy is the ability of an individual to control the access that others have to his/her personal information (Westin, 1967). Information privacy in an online context has been a consistent concern for individuals since the introduction of the world wide web (Hoffman, Novak, & Peralta, 1999). For example, a recent survey conducted by the United States (U.S.) Census Bureau revealed that, "Nearly three-quarters of Internet-using households had significant concerns about online privacy and security risks in 2017, while a third said these worries caused them to hold back from some online activities" (Goldberg, 2018).

In their original study, Malhotra, Kim, and Agarwal (2004) explored the influence of information privacy on customers' behavioral intention in an e-commerce setting. They developed and validated the Internet users' information privacy concerns (IUIPC) construct with three dimensions focused on an organization's privacy practices: collection, control, and awareness. Malhotra et al. (2004) found that information privacy concerns influence an individual's trusting beliefs (negatively) and risk beliefs (positively), both of which in turn influence an individual's intention to share information with the e-commerce organization. In addition, the level of sensitivity of the information (shopping preference information vs personal financial information) also influences trusting beliefs, risk beliefs, and behavioral intention (see Figure 1). The original study is a seminal article within the information privacy literature stream. As of April 1, 2020, there are 745 published articles citing Malhotra et al. (2004) in the Web of Science database, and 80 of those citations are in the AIS senior scholars' basket journals.

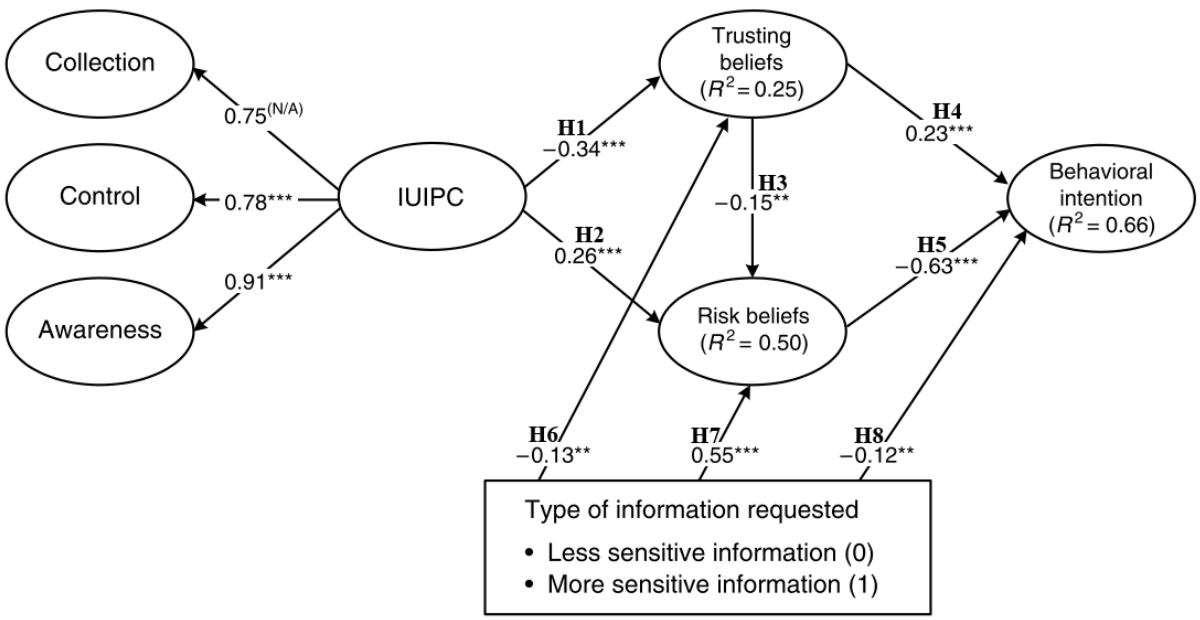

Figure 1. Research Hypotheses and Results from Original Study (Malhotra et al., 2004)

The literature around the IUIPC construct has focused on two primary domains: e-commerce and personalization; and social networking. In the e-commerce context, studies have found that privacy concerns can affect users' disclosure behavior by influencing perceived uncertainty, affect, risk perceptions, and trust (e.g., Pavlou, Liang, & Xue, 2007; Tsai, Egelman, Granor, & Acquisti, 2011; Van Slyke, Shim, Johnson, & Jiang, 2006; Wakefield, 2013). E-commerce personalization refers to the practice of creating individualized experiences on e-commerce websites by dynamically showing content based on individual browsing behavior, purchase history data, and demographics (Kumar & Benbasat, 2006). The benefits of personalization in an e-commerce context have been found to outweigh information privacy concerns (e.g., Li & Unger, 2012; Sutanto, Palme, Tan, & Phang, 2013). In the social networking context, studies have explored a variety of independent variables along with privacy concerns to explain disclosure behaviors such as affect (e.g., Yu, Au, Mu, Tang, Ren, Suslio, & Dong, 2015), trust (e.g., Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010), risk (e.g., Posey, Lowry, Roberts, & Ellis, 2010), and relationship building

(Dinev, Xu, Smith, & Hart, 2013). While these studies have utilized the IUIPC construct along with other drivers of information disclosure, to date there has been limited validation of the specific Malhotra et al. (2004) model.

We have three motivations for engaging in this conceptual replication. First, the original study was conducted in an e-commerce context. We attempt to extend the boundary of the theory, as our conceptual replication tests the model and hypotheses in a social networking context. In the e-commerce context, privacy concerns usually come from customers' apprehension about how e-commerce organizations will use their information (e.g., sell information to third parties). In the social networking site (SNS) context, users not only need to worry about the behavior of organizations (i.e., social network platforms), but more directly they need to worry about other users' (i.e., friends) behavior. For example, Ozdemir, Smith, and Benamati (2017) found a negative relationship between peer-focused privacy concerns and information disclosure in a SNS context. While replications around online privacy have been conducted, such as the 'concern for information privacy-CFIP' in a social media context (Osatuyi, 2015), or 'Internet privacy concerns' within a mobile banking context (Terlizzi, Brandimarte, & Sanchez, 2019), this replication is focused on the Malhotra et al. (2004) model.

Second, privacy concerns remain a timely topic and its importance continues to increase as we have seen from the frequent public data breaches (e.g., Kumparak, 2019) and invasive data collection (e.g., Snowden surveillance revelations). The significant interest in the topic is driven by the continuing issues that arise in the Web 2.0 environment. According to a survey conducted in early 2016, "roughly half of Americans do not trust …social media sites to protect their data" (Olmstead & Smith, 2017). Finally, it has been fifteen years since the original study, and much has changed in this time. Since 2004 just some of the related innovations include (but are not limited to) smart phones, mobile apps, Web 2.0, social networking sites like Facebook and Instagram, and cloud services. Given the significant technological changes and service shifts, it is important to empirically verify the generalizability/boundary conditions of the IUIPC and associated outcomes. As a conceptual replication, we used Malhotra et al.'s (2004) measures and adapted them to our context to test the strength of the key relationships in a SNS context.

2 Method

In the original study, participants were "household respondents" with 53% of the sample age 35 or older. The replication study collected data from undergraduate business students at a large southeastern university in the U.S. As of February 2020, 72% of all U.S. adults and 90% of 18-29-year-old U.S. adults use at least one social media site[1]. In addition, the largest SNS age cohorts are 25-29-year-old in Facebook and 18-24-year-old in Instagram, Snapchat, and Twitter[2] (see Table 1). Therefore, the sample of 18-to-25-year-old is appropriate for the study context. The participants were "active" users,[3] since they had visited a SNS within the last 30 days. The questionnaire was given to 265 participants; 246 completed the first stage survey (a 93% response rate) and 195 took the second stage survey. As a result of data cleansing, 168 responses were valid for further analysis. See Table 1 for the demographics of the final sample.

Table 1. Demographics

Gender	Female = 52%	**Tenure in the SNS**	Less than 2 years = 9%
	Male = 48%		2-4 years = 22%
Age	18-25 = 97%		4-6 years = 36%
	26 or above = 3%		6 years or more = 33%
Native Language	English = 90%	**Number of Connections**	Less than 200 = 18.5%
	Spanish = 8%		201-400 = 22.6%
	Other = 2%		401-600 = 17.2%

[1] "Social media fact sheet" (https://www.pewresearch.org/internet/fact-sheet/social-media/), retrieved on 02/16/2020.
[2] "Social media demographics that matter to marketers in 2020" (https://blog.hootsuite.com/social-media-demographics/#general), retrieved on 02/16/2020.
[3] Facebook help page "What is a monthly active user?" (https://www.facebook.com/help/work/1101646006616660?helpref=uf_permalink), retrieved on 05/22/2018.

Table 1. Demographics			
Education	High School Diploma = 45%		601-800 = 11.3%
	Associates Degree = 48%		801 or above = 30.4%
	Bachelors/ Degree = 7%	**Weekly Hours Spent in SNS**	Less than 2 hours = 14%
Largest SNS Age Cohort*	Facebook = 25 - 29		3-6 hours = 30%
	Instagram = 18 - 24		7-10 hours = 27%
	Snapchat = 18 - 24		11-14hours = 14%
	Twitter = 18 - 24		15-18 hours = 6%
Social Networking Site	Facebook = 35.1%		19 or above = 9%
	Instagram = 29.2%		
	Snapchat = 20.8%		
	Twitter = 8.3%		
	Other = 6.6%		
* Source: https://blog.hootsuite.com/social-media-demographics/#general			

2.1 Data Collection Procedure

Similar to the original study, we designed the questionnaire with two different scenarios (i.e., low versus high information sensitivity) to investigate how individuals' privacy-related behaviors differ based on the type of information to be shared. In scenario A (less sensitive information), participants were asked by their friends to share (on their SNS) photos taken at 2:00 p.m., in a local park, where they are sitting around a picnic table, eating bar-b-que and drinking tea. In scenario B (more sensitive information), participants were asked by their friends to share (on their SNS) photos taken at 2:00 a.m., in a local nightclub, where they are sitting around a table drinking (alcohol) and some were smoking/vaping. Participants were randomly assigned to one of the two scenarios and were presented with the same measurement items. We collected data using an online self-report survey instrument. To minimize the possibility of common method variance, we collected the data in two stages (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003), with a minimum of 14 days between the two surveys (Johnson, Rosen, & Djurdjevic, 2011). Several attention check questions, which are questions are designed to check whether participants are reading the questions or skipping to the answer choices (Oppenheimer, Meyvis, & Davidenko, 2009), were inserted into the survey instrument. This was done as a manipulation check and allowed us to eliminate inattentive participants from the data analysis.

In the first stage, participants responded to the questions measuring personal disposition factors and context-specific factors. When responding to questions regarding personal disposition factors such as information privacy concerns, participants were asked to rate their level of agreement with the measurement items in general (not specific to any SNS or scenario). When answering questions regarding context-specific factors including information trusting beliefs and information privacy risk beliefs, participants were asked to think about a specific SNS that they used the most during the past 30 days. In the second stage, each participant responded to questions measuring private disclosure referencing the scenario provided.

There are three dimensions of information privacy concerns: collection, control, and awareness (Malhotra et al., 2004). We modified items in the collection dimension of information privacy concerns to reflect the nature of the information flow[4] in SNSs. In the current study, the measure reflects the degree to which an individual is concerned about private information divulged to his/her social network members and was adapted based on similar measures in the literature (Jiang, Heng, & Choi, 2013; Wheeless & Grotz, 1976). Table 2 provides a summary of the measurement scales used in the replication study. See Appendix A, Table A1 for the measurement items for each construct. All items used a seven-point Likert-type scale ranging from "strongly disagree" (1) to "strongly agree" (7). Following the decision rules described by Jarvis, MacKenzie, and Podsakoff (2003) and MacKenzie, Podsakoff, and Jarvis (2005), and consistent with

[4] The original items in the collection dimension reflect an organization collecting private information from business-to-consumer transactions. In SNSs the individual shares private information with his/her social network members.

previous research on online privacy management (Child, Pearson, & Petronio, 2009; Malhotra et al., 2004), trusting beliefs and privacy risk beliefs were modeled as first-order reflective constructs. We modeled information privacy concerns as a reflective first-order and reflective second-order construct (Child et al., 2009; Malhotra et al., 2004).

Table 2. Summary of Constructs and Measures

Construct and Definition	# of Items	Measure
Information Privacy Concerns: An individual's worries about SNS members' information privacy practices. **Collection dimension:** The degree to which an individual is concerned about the private information disclosed to SNS members relative to the benefits received. **Control dimension:** The degree to which an individual is concerned about her freedom to approve, modify, or delete his or her private information. **Awareness dimension:** The degree to which an individual is concerned about his or her knowledge of the SNS members' information privacy practices.	14	Adapted from Malhotra et al. (2004)
Information Trusting Beliefs: The degree to which an individual believes that his or her SNS members will behave in a dependable manner regarding the individual's private information.	7	Adapted from Malhotra et al. (2004)
Information Privacy risk Beliefs: An individual's perception of the likelihood of loss due to sharing private information with his or her SNS members.	4	Adapted from Malhotra et al. (2004)
Private Disclosure*: An individual voluntarily and intentionally revealing private information to his or her SNS members.	5	Adapted from Jiang et al. (2013)
* Malhotra used 'Intention to Give Information' as the dependent variable. This concept was captured using a seven-point semantic scale and four response pairs for the prompt, "Given this hypothetical scenario, specify the extent to which you would reveal the information through the Internet."		

We included several factors as control variables, because while they were not included in the research model, they have been suggested in the literature to have an influence on privacy-related attitudes and behaviors (Malhotra et al., 2004; Posey et al., 2010; Tifferet, 2019; Xu, Teo, Tan, & Agarwal, 2009). These variables include gender, native language, education, tenure in the SNS, number of connections in the SNS, and weekly hours spent in SNS (see Appendix A, Table A2 for a description of these measures). We did not collect from our respondents the following: general internet experience, the experience of identification falsification, media exposure, and experience as a victim. We determined that the intent of several of these controls were captured with the tenure in the SNS question, and the remainder were not relevant in the SNS context.

3 Results

3.1 Methodological Differences

This study was a conceptual replication, and as such there are a few differences in the methods employed from the original study. In the original study, the authors conducted their SEM statistical tests using LISREL (Widaman, 1985; Williams, Cote, & Buckley, 1989); the replication study used SmartPLS (Podsakoff et al., 2003; Ringle, Wende, & Will, 2005). While the original study collected the data about independent and dependent variables in one survey, the replication study collected the data in two stages with a minimum of 14 days between the two surveys and added a marker variable to address common method bias (Lindell & Whitney, 2001; Podsakoff et al., 2003). In the original study two items for trusting beliefs (i.e., ITB1 and ITB2) and one item for risk beliefs (i.e., IRB5) were removed due to low factor loadings; whereas in the

replication study items three items for information privacy concerns (collection - IPC5, control - IPC9, and awareness - IPC12) were removed.

3.2 Assessment of Response Bias and Common Method Variance

Response bias was assessed using the Armstrong and Overton (1977) procedure. The sample was divided into early and late responders. An analysis of variance comparing early and late responders indicated a nonsignificant difference for all of the demographic variables, the scenario assigned, and dependent variable (private disclosure). In addition to using reverse scored items and the two-phase data collection procedure, two statistical analyses were conducted to assess potential common method bias in the results. First, Harman's one-factor test showed the first factor accounted for 29.9% of the total variance in private disclosure. Second, we performed a marker variable test as suggested by Lindell and Whitney (2001). We used two variables that should have no relationship with the constructs of interest: (1) satisfaction with a car insurance company, and (2) the intention to take a long trip soon. The smallest correlation was 0.002, suggesting no correction was needed (based on Jayachandran, Sharma, Kaufman, & Raman, 2005; Richardson, Simmering, & Sturman, 2009). Taken together, the results indicate that common method bias is unlikely to be a serious concern with this data. Partial least squares (PLS) was used for data analysis using a two-step approach. First, the measurement model was evaluated to assess the validity and reliability of the measures, then the structural model was evaluated to assess the hypotheses.

3.3 Measurement Model

The data analysis began by assessing the psychometric adequacy of the measurement model. The measures are reliable, as the composite reliabilities of all the constructs/dimensions ranged from 0.85 to 0.95 which are within the appropriate range (Bagozzi & Yi, 1988; Garver & Mentzer, 1999). See Table 3 for the mean, standard deviation, composite reliability, average variance extracted (AVE) and correlations for each variable. The means for privacy concerns and private disclosure were relatively consistent in both the replication study and the original study; whereas the means for risk beliefs (O = 4.56, R = 5.23) and trusting beliefs (O = 3.24, R = 4.34) were quite different between the two studies.

Table 3. Descriptive Statistics, Correlations, and Measurement Model Statistics

Variable	Mean	Std	ICR	AVE	1	2	3	4	5	6
1. Privacy Concerns, Awareness	5.80	1.16	.97	.90	**.95**					
2. Privacy Concerns, Collection	5.60	0.98	.87	.69	.52**	**.83**				
3. Privacy Concerns, Control	5.61	1.21	.95	.84	.45**	.47**	**.92**			
4. Trusting Beliefs	4.34	1.18	.95	.73	.01	.04	-.01	**.85**		
5. Risk Beliefs	5.23	1.17	.93	.77	.48**	.43**	.47**	-.09	**.88**	
6. Private Disclosure	3.47	1.35	.91	.68	-.19*	-.09	-.15	.20**	-.14	**.82**

Square root of the average variance extracted (AVE) is in bold on the diagonal.
ICR denotes internal composite reliability.
Significance level of correlations: ** p < .01; * p < .05

Table 4. Descriptive Statistics, Correlations, and Measurement Model Statistics, continued

Variable	Mean	Std	ICR	AVE	7	8	9	10	11	12	13
1. Privacy Concerns, Awareness	5.80	1.16	.97	.90	.07	.08	-.03	-.20**	-.03	.16*	.17*
2. Privacy Concerns, Collection	5.60	0.98	.87	.69	.13	-.05	-.03	-.20**	.13	.14	.08
3. Privacy Concerns, Control	5.61	1.21	.95	.84	.11	.07	.03	-.13**	.11	.17*	.02
4. Trusting Beliefs	4.34	1.18	.95	.73	-.03	.06	.00	.01	-.02	.01	.17*
5. Risk Beliefs	5.23	1.17	.93	.77	.15*	.03	-.06	-.13	.04	.18*	.13
6. Private Disclosure	3.47	1.35	.91	.68	.01	.03	-.04	.04	-.08	.00	.05
7. Age	1.04	0.33	1.00	1.00	1.00	-.12	.11	-.12	-.04	.09	-.17*

Table 4. Descriptive Statistics, Correlations, and Measurement Model Statistics, continued											
8. Connections	5.70	2.95	1.00	1.00		1.00	.08	-.13	-.01	.44**	.14
9. Education	1.63	0.62	1.00	1.00			1.00	.03	.10	.19*	.06
10. Gender	n/a	n/a	1.00	1.00				1.00	.12	-.09	-.22**
11. Language	3.53	1.74	1.00	1.00					1.00	.12	.03
12. SNS Tenure	5.44	1.90	1.00	1.00						1.00	.15
13. Hrs in SNS	5.14	2.39	1.00	1.00							1.00
Square root of the average variance extracted (AVE) is in bold on the diagonal. ICR denotes internal composite reliability. Significance level of correlations: ** p < .01; * p < .05											

We conducted a confirmatory factor analysis to obtain the preliminary evidence for convergent and discriminant validity (see Appendix B, Tables B1 and B2 for factor loadings). The results show that all of the item loadings were above 0.60 on the latent constructs/dimensions, and below 0.50 on the other constructs/dimensions (Hair, Anderson, Tatham, & Black, 1998). Due to low factor loadings three items of information privacy concerns (IPC5, IPC9, IPC12) were removed. For convergent validity we note that the AVE's were all about 0.50 (Chin, 1998a; 1998b) with the lowest AVE of 0.68 (private disclosure) indicating that the items for each measure did converge. For second-order reflective constructs, measures show convergent validity when the path coefficient of a dimension loading onto its latent construct is significant. For information privacy concerns, all three dimensions had significant path coefficients (see Figure 2). Thus, convergent validity is indicated for the measures. Discriminant validity was assessed using the Fornell and Larcker (1981) test. Each latent variable correlation is less than the square root of the AVE of that variable (see Table 3). The measures demonstrated adequate construct validity and thus proceeded to the structural model.

3.4 Structural Model

Figure 2 graphically represents that results of the structural model test. We used the PLS bootstrapping technique with 5,000 resamples and 168 cases (Chin, 2001). Consistent with Malhotra et al. (2004) control variables were entered as predictors of trusting beliefs, risk beliefs, and private disclosure. The variables in the replication model explained 4% of the variance in trusting beliefs, 35% of the variance in risk beliefs, and 13% of the variance in private disclosure. Among the control variables, the only significant influence was from hours per week spent on a SNS to trusting beliefs ($\beta = 0.18$, $p < .05$). Overall, we found partial support for the proposed model within this context with Hypotheses 2, 4, and 8 being supported, and Hypotheses 1, 3, 5, 6, and 7 not supported. See Table 4 for the detailed hypothesis results.

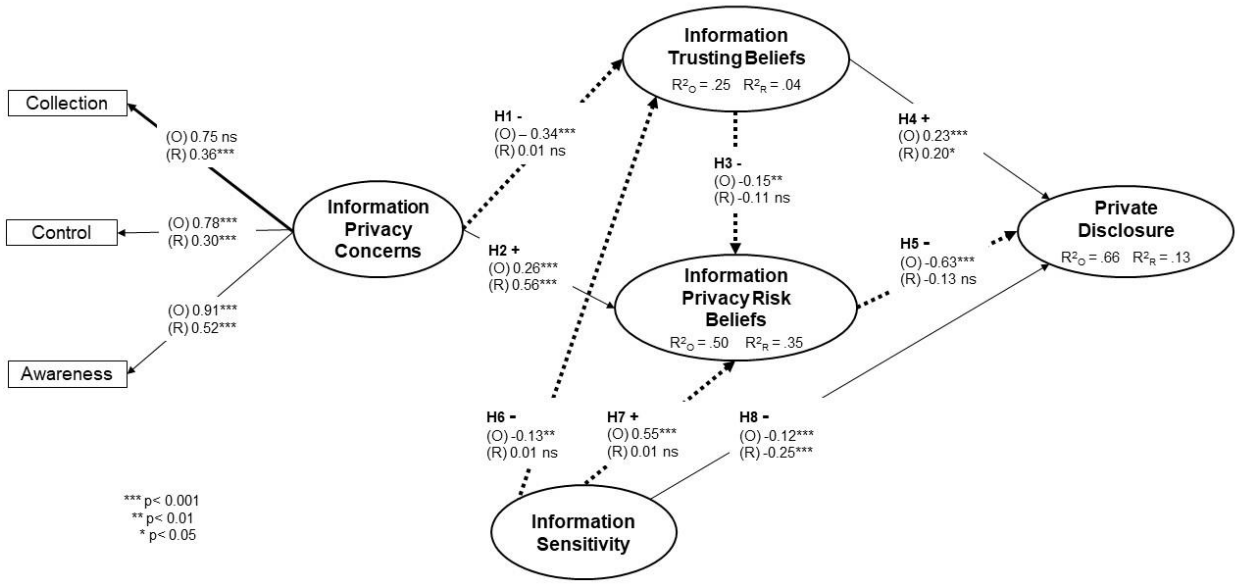

Figure 2. Hypotheses and Results from Original Study (O) and Replication Study

Figure 2 Notes:

Thin solid lines (⟶): Significant and consistent result. Significant in this replication and the original study.

Bold solid lines (⟶): Significant and inconsistent result. Significant in this replication study but non-significant in the original study.

Bold dashed lines (⇢): Nonsignificant and inconsistent result. Nonsignificant in this replication study but significant in the original study.

Table 5. Results of the Hypothesis Testing in the Original Study and Replication Study

H#	Hypothesis	Original Research	Replication Research
1	Internet users' information privacy concerns will have a negative effect on trusting beliefs.	Supported	Not Supported
2	Internet users' information privacy concerns will have a positive effect on risk beliefs.	Supported	Supported
3	Trusting beliefs will have a negative effect on risk beliefs.	Supported	Not Supported
4	Trusting beliefs will have a positive effect on intention to reveal personal information.	Supported	Supported
5	Risk beliefs will have a negative effect on intention to reveal personal information.	Supported	Not Supported
6	A marketer's request for [Posting on a SNS] more sensitive information will have a negative effect on trusting beliefs.	Supported	Not Supported
7	A marketer's request for [Posting on a SNS] more sensitive information will have a positive effect on risk beliefs.	Supported	Not Supported

Table 5. Results of the Hypothesis Testing in the Original Study and Replication Study			
8	A marketer's request for [Posting on a SNS] more sensitive information will have a negative effect on intention to reveal personal information.	Supported	Supported

4 Discussion and Implications

Results from the replication study revealed mixed support for the original study's findings. In terms of consistent results, our findings did support Internet users' information privacy concerns (IUIPC) as a second-order reflective construct composed of three first-order constructs: collection, control, and awareness. Consistent with Malhotra et al. (2004), IUIPC positively and significantly influenced users' risk beliefs (β = 0.56, $p < .001$), and that trusting beliefs positively and significantly influenced users' intention to disclose private information (β = 0.20, $p<.05$). Finally, information sensitivity negatively and significantly influenced users' intention to disclose private information (β = -0.25, $p<.001$).

The replication study also revealed a few potentially non-generalizable relationships. The loading between collection and IUIPC is statistically significant in our results while it was not in the original study. Consistent with Ozdemir, Smith, and Benamati (2017), we believe this result is due to the context – as individuals were allowing SNS members (i.e., friends) to "collect" information as opposed to an organization. So, within a SNS context, friends sharing ownership of one's information is a privacy concern.

A main finding from the replication study was that IUIPC had no relationship with the user's trusting beliefs (H1) within a SNS context. The small amount of variance in trusting beliefs explained is likely due to the significant influence of time spent per week in a SNS as trust is positively influenced by familiarity (Kim, Ferrin, & Rao. 2008), which can develop via interactions over time. In addition, one's social network members are already "friends", so they have been pre-vetted. We speculate that other factors, such as social presence or disposition to trust may explain more variance in trusting beliefs within a SNS context (Ridings, Gefen, & Arinze, 2002). Another explanation for this finding may be that trust is not a simple, one dimensional construct. Future research might explore the impact of levels of trust (e.g., interpersonal, group), and dimensions of trust (e.g., competence, benevolence, integrity; Gefen 2002) within the SNS context. Using a more fine-grained perspective of the trust construct may reveal aspects of trust that are related to IUIPC within the SNS context.

Contrary to the original study, the negative relationship between trusting beliefs and risk beliefs (H3) was not statistically significant (β = -.12, ns). Also, the negative relationship between risk beliefs and intention to disclose private information (H5) was not statistically significant (β = -.13, ns). One possible explanation for these non-significant findings is the objects (e.g., the trustee) of the user's beliefs in the e-commerce context and social network context are different. The continuous reports of online information leaks (e.g., Facebook-Cambridge Analytica), government monitoring (e.g., Snowden revelations) and sale of personal information (e.g., Unroll.me, Ever) has created a climate of cynicism toward online privacy. "The issue of who is gathering information and what information is being gathered is considered to be an important dimension of privacy control by nearly all American adults" (Madden & Rainie, 2015). In the e-commerce context, the objects of trusting beliefs and risk beliefs are retailers. For example, in the original study Malhotra et al. (2004) asked participants if they trust online companies to keep their best interests in mind when dealing with their information.

In our replication project, the object of trusting beliefs and privacy risk beliefs were members of the individual's online social network. Lowry, Cao, and Everard's (2011) study argued that in the social networking context, people's disclosure behavior is more intentional and their target object (i.e., audience) is someone they already know. The difference in findings might be explained by overlaying the communication privacy management (CPM) theory (Petronio, 1991, 2002) with IUIPC theory to address private disclosure. CPM theory explains how individuals reveal or conceal private information to/from confidants by establishing a collective privacy boundary around the information. Within the SNS context the individual initially trusts that a SNS member will not allow access to the collectively held information to unauthorized others. But when an individual's information boundary is disrupted (e.g., private information is shared), individuals engage in privacy management behavior to restore the boundary. Exploring the information boundaries may explain why risk is not as influential within the SNS context.

Information sensitivity is a measure of the level of the perceived potential loss associated with the disclosure of information. Information that is more personally identifying is perceived as more sensitive (Malheiros, Preibusch, & Sasse, 2013). In the original study, the level of sensitivity of the information being shared significantly affected trusting beliefs, privacy risk beliefs, and intention to disclose private information. Less sensitive information referred to an individual's shopping preferences, and more sensitive information referred to an individual's financial information. In the replication study, low sensitivity information referred to posting pictures of oneself at an afternoon picnic in the park, and high sensitivity information referred to posting pictures of oneself at a club late at night/early in the morning. In the replication study, the sensitivity of the information did not influence the individuals' beliefs regarding trust and risk but did negatively influence their intention to disclose information. So while the participants in the replication study believe that their SNS 'friends' will behave toward all of their information in a dependable manner (trusting beliefs), and do not perceive a high likelihood of loss in sharing private information (risk beliefs), they still are less inclined to share more sensitive information in their online social network (private disclosure).

Different types of information can be associated with different levels of sensitivity and risk (Milne, Pettinico, Hajjat, & Markos, 2017; Schomakers, Lidynia, Müllmann, & Ziefle, 2019). For example, credit card numbers are most often associated with monetary risk, whereas one's social network profile relates more to social and psychological risks. As information sensitivity is an individual perception, the type of information being shared may influence an individual's perceived level of sensitivity. For example, a college student might perceive social information more valuable than monetary information, whereas a working professional might perceive monetary information as more sensitive. Future research may want to further explore the impact of different types of information and the associated sensitivity on information disclosure.

As we have discussed, user's information privacy concerns in a SNS may have two foci: concerns toward the members of his/her online social network, and concerns toward the social networking platform. In the replication study, the level of information sensitivity may be less related to users' trust beliefs and risk beliefs toward participants' known members, but it may be more related to users' trust beliefs and risk beliefs about other unknown breaches and the social networking platform. Individuals frequently do not read privacy/disclosure statements when signing up for apps (e.g., Rice & Bogdanov, 2019; Milne, Culnan, & Greene, 2006). According to a poll of 4000 individuals conducted in 2019, 56% of respondents said they either "always" or "usually" accept the privacy policy without reading it and younger adults (age 18-24) are even more willing to skip reading the privacy policies (Hart, 2019). For example, using an email digest service it owns, Slice collected customers' emailed Lyft receipts from their inboxes and sold the anonymized data to Uber (Biddle, 2017); and millions of images stored by Ever, a photo album app, were used to train facial recognition systems (Quach, 2019). In each of these examples, the only way an individual would discover any reference to these practices is if he/she read through the 3,150-word (Slice) and 2,566-word (Ever) privacy policies.

Social media incidents accounted for over 56% of the 4.5 billion data records compromised worldwide in the first half of 2018 (Gilbert, 2018). With highly publicized data privacy scandals such as Facebook providing detailed personal information of millions of users to a voter-profiling company (Rosenberg, Confessore, & Cadwalladr, 2018), and Google shutting down their Google+ social network due to data from up to 500 000 users being exposed (Landwher, 2019), many are skeptical of the information privacy protections provided by social networking platforms. As the information becomes more sensitive, users may decide not to disclose their information in the SNS from concerns and beliefs related to the platform not the people.

Finally, the amount of variance explained in the model was significantly lower in the replication study than in the original study. In the original study, IUIPC explained 25% of the variance in trusting beliefs and 50% of the variance in risk beliefs. In the replication study, information privacy concerns explained 4% of the variance in trusting beliefs and 35% of the variance in risk beliefs. In turn, in the original study trusting beliefs, risk beliefs, and information sensitivity explained 66% of the variance in behavioral intention (i.e., willingness to give information) but in the replication study these variables only explained 13% of the variance in private disclosure. One explanation for this finding may be that within a social networking context, there are other factors that were not captured that more strongly influence individual private information disclosure (e.g., reciprocity, Liu, Cheung, & Lee, 2016; integrity, Chari, Christodoulides, Presi, Wenhold, & Casaletto, 2016; social presence, Gao, Liu, & Li, 2017).

Alternatively, the differences in the sample population (older adults vs young adults) or temporal factors (e.g., digital natives) may have influenced the findings (Vodanovich, Sundaram, & Myers, 2010). Even within young adults we see differences in these variables. For example, in a study of social commerce and trust,

Herrando, Jimenez-Martinez, and Martin-De Hoyos (2019) found that individuals in generations X (born roughly between 1965 and 1980) and Y (born roughly between 1981 and 1995) transfer trust to social commerce websites mainly from trust in information generated by companies, while Generation Z (born roughly between 1996 and the present) transfers trust mainly from information generated by users. Also, as Vodanovich et al. (2010, p. 712) state, "digital natives are not just using technology differently—their lives are being molded by technology differently" such that "they tend to be more comfortable with extensive peer-to-peer collaboration and the resultant disclosure of personal data." We speculate that generational effects may be in play within this dataset. We encourage future research targeted at exploring potential generational differences.

This study has multiple implications for social networking platform organizations. First, as our results suggest, privacy remains a concern in the online social networking context. SNS platform organizations may want to explore how to reduce users' information privacy concerns related to the collection, control, and awareness dimensions via SNS members views of each other, as well as SNS members views of the platform. For example, with the control dimension, individuals may feel comfortable with the amount of control they have over their information within their social network (i.e., among their 'friends'), but not feel comfortable with the amount of control they have in the platform.

Second, we found that users' perceptions of information sensitivity are negatively related to their intention to disclose private information in a social networking context, while trusting beliefs are positively related to their intention to disclose private information. Information disclosure is a major component of relationship building within SNS (Kim, Shin, & Chai, 2015), and increasing information disclosure is a goal of the SNS platform organizations. The typical SNS platform business model is based on advertising, either through targeted advertising that utilizes an individual's personal information, search habits, location or other such data, or by selling the personal information to third parties. Either way, the SNS platform organization needs information about users. On way to accomplish this might be through the optimization of devices connected via the Internet of things (IoT). The Internet of things (IoT) is a system of interactive objects/devices connected to the Internet that give people the ability to automatically transfer data to manage, monitor, and optimize various aspects of their daily activities (Porambage, Ylianttila, Schmitt, Kumar, Gurtov, & Vasilakos, 2016). Because of application interdependency in IoT devices and the amount of potentially sensitive data stored by these devices, a leakage of information could severely damage individual privacy. In order to encourage information disclosure in an IoT paradigm, social networking platform organizations might focus on incorporating privacy-enhancing technologies for IoT-related applications and privacy protection at the design level (e.g., privacy enhanced APIs). This extra level of protection may increase the individual's perceived trust of the SNS platform and thus information disclosure.

5 Limitations and Future Research

Care must be taken when attempting to generalize these findings. Given the fact that there are several types of online communities, individuals participating in other types of online communities may have privacy perceptions that are different from those using SNSs. Much more research is needed in a variety of online contexts (e.g., sharing economy networks, online review sites) to determine the specific boundaries of the original IUIPC theory.

A characteristic of the sample to consider is the native language of the participants. Although efforts were made to include a range of participants representing different cultural groups, 90% of the participants were native English speakers. Therefore, the applicability of the findings to other cultural groups may be limited. In addition, the survey respondents in the replication study were college students (age 18-25) while the original study used household members. Although using student as participants in social networking context is appropriate, younger individuals tend to be less sensitive about privacy concerns and more inclined toward self-disclosure behavior (Li, Lin, & Wang, 2015). Future studies about information privacy concerns in a social networking context might examine whether age and/or generation influences the relationship between individuals' privacy concerns and their intention to disclose private information.

Our study focused on users' information privacy concerns and beliefs toward members of their online social network and found mixed results compared to the original study. Future research on information privacy concerns in a SNS context should consider a more finely grained view of information privacy concerns which can examine information privacy concerns toward SNS members and toward the social networking platform. By looking at these foci separately, researchers may be able to develop a more holistic nomological network for the construct.

6 Conclusion

This study replicated the research presented by Malhotra et al. (2004) on the relationship between Internet users' information privacy concerns and disclosure intention within an e-commerce setting. By a conceptual replication we have empirically validated that portions of the original model hold within the social networking context (e.g., the relationship between user's information privacy concerns and risks beliefs), and portions of the model are not generalizable to the online social networking context (e.g., the relationship between user's information privacy concerns and trusting beliefs). We encourage work in this area to further refine and enhance the Internet users' information privacy concerns (IUIPC) theory.

References

Armstrong, J. S., & Overton, T. S. (1977). Estimating nonresponse bias in mail surveys. *Journal of Marketing Research*, 14(3), 396-402.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74-94.

Biddle, S. (2017). Stop using Unroll.me, right now. It sold your data to Uber. *The Intercept*. Retrieved from https://theintercept.com/2017/04/24/stop-using-unroll-me-right-now-it-sold-your-data-to-uber/.

Chari, S., Christodoulides, G., Presi, C., Wenhold, J., & Casaletto, J. P. (2016). Consumer trust in user-generated brand recommendations on Facebook. *Psychology & Marketing*, 33(12), 1071-1081.

Child, J. T., Pearson, J. C., & Petronio, S. (2009). Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the American Society for Information Science and Technology,* 60(10), 2079-2094.

Chin, W. W. (1998a). Issues and opinion on structural equation modeling. *MIS Quarterly*, 22(1), 7-16.

Chin, W. W. (1998b). The partial least square approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern Methods for Business Research* (pp. 295-336). Mahwah, NJ: Erlbaum.

Chin, W. W. (2001). *PLS-Graph user's guide*. CT Bauer College of Business, University of Houston, USA, 15, 1-16.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295-316.

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

Gao, W., Liu, Z., & Li, J. (2017). How does social presence influence SNS addiction? A belongingness theory perspective. *Computers in Human Behavior*, 77, 347-355.

Garver, M. S., & Mentzer, J. T. (1999). Logistics research methods: Employing structural equation modeling to test for construct validity. *Journal of Business Logistics*, 20(1), 33-57.

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *The DATABASE for Advances in Information Systems*, 33(3), 38-53.

Gilbert, P. (2018). Social media becomes biggest data breach threat. *IT Web*. Retrieved from https://www.itweb.co.za/content/G98YdqLxZZNqX2PD.

Goldberg, R. (2018). Most Americans continue to have privacy and security concerns, NTIA survey finds. *National Telecommunications and Information Administration, United States Department of Commerce*. Retrieved from https://www.ntia.doc.gov/blog/2018/most-americans-continue-have-privacy-and-security-concerns-ntia-survey-finds.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Data Analysis*. Englewood Cliffs, NJ: Prentice Hall.

Hart, K. (2019). Privacy policies are read by an aging few. Retrieved from https://www.axios.com/few-people-read-privacy-policies-survey-fec3a29e-2e3a-4767-a05c-2cacdcbaecc8.html.

Herrando, C., Jimenez-Martinez, J., & Martin-De Hoyos, M. J. (2019). Tell me your age and I tell you what you trust: The moderating effect of generations. *Internet Research*, 29(4), 799-817.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, 42(4), 80-85.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research*, 30(2), 199-218.

Jayachandran, S., Sharma, S., Kaufman, P., & Raman, P. (2005). The role of relational information processes and technology use in customer relationship management. *Journal of Marketing*, 69(4), 177-192.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research note—privacy concerns and privacy-protective behavior in synchronous online social interactions. *Information Systems Research*, 24(3), 579-595.

Johnson, R. E., Rosen, C. C., & Djurdjevic, E. (2011). Assessing the impact of common method variance on higher order multidimensional constructs. *Journal of Applied Psychology*, 96(4), 744-761.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems*, 44(2), 544-564.

Kim, B., Shin, K., & Chai, S. (2015). How people disclose themselves differently according to the strength of relationship in SNS? *Journal of Applied Business Research*, 31(6), 2139-2146.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25(2), 109-125.

Kumar, N., & Benbasat, I. (2006). Research note: The influence of recommendations and consumer reviews on evaluations of websites. *Information Systems Research*, 17(4), 425-439.

Kumparak, G. (2019). Capital One hacked, over 100 million customers affected. Retrieved from https://techcrunch.com/2019/07/29/capital-one-hacked-over-100-million-customers-affected/.

Landwher, C. (2019). Privacy and security 2018: A big year for privacy. *Communications of the ACM*, 62(2), 20-22.

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, T., & Unger, T. (2012). Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems*, 21(6), 621-642.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, 86(1), 114-121.

Liu, L., Cheung, C. M. K., & Lee, M. K. O. (2016). An empirical investigation of information sharing behavior on social commerce sites. *International Journal of Information Management,* 36(5), 686-699.

Lowry, P. B., Cao, J., & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, 27(4), 163-200.

MacKenzie, S. B., Podsakoff, P. M., & Jarvis, C. B. (2005). The problem of measurement model misspecification in behavioral and organizational research and some recommended solutions. *Journal of Applied Psychology*, 90(4), 710-730.

Madden, M., & Rainie, L. (2015). Americans' attitudes about privacy, security and surveillance. *Pew Research Center*.

Malheiros, M., Preibusch, S., & Sasse, M. A. (2013, June). "Fairly truthful": The impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure. In *International Conference on Trust and Trustworthy Computing* (pp. 250-266). Springer, Berlin, Heidelberg.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research,* 15(4), 336-355.

Milne, G. R., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing*, 25(2), 238-249.

Milne, G. R., Pettinico, G., Hajjat, F. M., & Markos, E. (2017). Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing. *Journal of Consumer Affairs*, 51(1), 133-161.

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity. *Pew Research Center*, 26. Retrieved from https://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf.

Oppenheimer, D. M., Meyvis, T., & Davidenko, N. (2009). Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology*, 45(4), 867-872.

Osatuyi, B. (2015). Empirical examination of information privacy concerns instrument in the social media context. *AIS Transactions on Replication Research*, 1, Article 3, 1-14.

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.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly,* 31(1), 105-136.

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, 1(4), 311-335.

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

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), 879-903.

Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., & Vasilakos, A. V. (2016). The quest for privacy in the internet of things. *IEEE Cloud Computing*, 3(2), 36-45.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. *European Journal of Information Systems*, 19(2), 181-195.

Quach, K. (2019). Photo 'memories' storage biz Ever uses family snaps to train facial recognition AI. *The Register*. Retrieved from https://www.theregister.com/2019/05/10/ever_facial_recognition/.

Rice, M. D., & Bogdanov, E. (2019). Privacy in doubt: An empirical investigation of Canadians' knowledge of corporate data collection and usage practices. C*anadian Journal of Administrative Sciences/Revue Canadienne des Sciences de l'Administration,* 36(2), 163-176.

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organizational Research Methods*, 12(4), 762-800.

Ridings, C. M., Gefen, D., & Arinze, B. (2002). Some antecedents and effects of trust in virtual communities. *Journal of Strategic Information Systems*, 11(3-4), 271-295.

Ringle, C. M., Wende, S., Will, A. (2005). *SmartPLS 2.0.M3*. Hamburg, Germany: SmartPLS. Retrieved from https://www.smartpls.com/.

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018). How Trump consultants exploited the Facebook data of millions. *The New York Times*, 17(3), 2018. Retrieved from https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

Schomakers, E. M., Lidynia, C., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity–insights from Germany. *International Journal of Information Management*, 46, 142-150.

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly*, 37(4), 1141-1164.

Terlizzi, M. A., Brandimarte, L., & Sanchez, O. (2019). Replication of internet privacy concerns in the mobile banking context. *AIS Transactions on Replication Research*, 5(8), 1-18.

Tifferet, S. (2019). Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior*, 93, 1-12.

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

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, 7(6), 1-16.

Vodanovich, S., Sundaram, D., & Myers, M. (2010). Research commentary: Digital natives and ubiquitous information systems. *Information Systems Research,* 21(4), 711-723.

Wakefield, R. (2013). The influence of user affect in online information disclosure. *Journal of Strategic Information Systems*, 22(2), 157-174.

Westin, A. F. (1967). Special report: Legal safeguards to insure privacy in a computer society. *Communications of the ACM*, 10(9), 533-537.

Wheeless, L. R., & Grotz, J. (1976). Conceptualization and measurement of reported self-disclosure. *Human Communication Research*, 2(4), 338-346.

Widaman, K. F. (1985). Hierarchically nested covariance structure models for multitrait-multimethod data. *Applied Psychological Measurement*, 9(1), 1-26.

Williams, L. J., Cote, J. A., & Buckley, M. R. (1989). Lack of method variance in self-reported affect and perceptions at work: Reality or artifact? *Journal of Applied Psychology*, 74(3), 462-468.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2009). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, 26(3), 135-174.

Yu, Y., Au, M. H., Mu, Y., Tang, S., Ren, J., Susilo, W., & Dong, L. (2015). Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage. *International Journal of Information Security*, 14(4), 307-318.

Appendix A: Measures

Table A1. Replication Study Measures

Construct Dimension	Question	Item #
Information privacy concerns (IPC): Collection	It bothers me when I need to disclose private information about myself to social networking site members.	IPC1
	I sometimes think twice before disclosing private information about me on my social networking site.	IPC2
	It bothers me to disclose private information about me to so many social networking site members.	IPC3
	It bothers me to disclose too much private information about me on my social networking site.	IPC4
	I'm concerned that I disclose too much private information about me on my social networking site.*	IPC5
Information privacy concerns (IPC): Control	Privacy in the social networking site is really a matter of my right to exercise control over decisions about how my private information is shared on my social networking site.	IPC6
	Control of my private information lies at the heart of privacy in the social networking site.	IPC7
	I believe that privacy in the social networking site is invaded when control over private information about me is lost or unwillingly reduced.	IPC8
	It is very important to me that I am knowledgeable about how social networking site members view my private information.*	IPC9
Information privacy concerns (IPC): Awareness	Social networking site members who want to further share my private information should inform me how they will discuss it.	IPC10
	Social networking site members should make it clear and conspicuous to me about the way my private information is discussed.	IPC11
	It is very important to me that I am knowledgeable about how social networking site members treat my private information.*	IPC12
	Social networking site members who want to further share my private information should inform me how they will share it.	IPC13
	Social networking site members should make it clear and obvious to me how my private information is shared.	IPC14
Risk beliefs	It is risky to give my private information to online social network members.	IPRB1
	There is a high potential for loss associated with giving my private information to online social network members.	IPRB2
	There is too much uncertainty associated with giving my private information to online social network members.	IPRB3
Trusting beliefs	I trust that social networking site members would keep my best interests in mind when dealing with my private information.	ITB1
	Social networking site members are in general honest with me regarding how they will discuss my private information.	ITB2
	Social networking site members are in general honest with me regarding how they will share my private information.	ITB3
	Social networking site members are in general predictable regarding how they will discuss my private information.	ITB4
	Social networking site members are in general predictable with me regarding how they will share my private information.	ITB5
	Social networking site members are in general consistent with me regarding how they will discuss my private information.	ITB6

Table A1. Replication Study Measures		
	Social networking site members are in general consistent with me regarding how they will share my private information.	ITB7
Private disclosure	I would reveal personal thoughts about the photos in my virtual territory.	PD1
	I would reveal personal feelings about the photos in my virtual territory.	PD2
	I would reveal personal experiences about the photos in my virtual territory.	PD3
	I would reveal sensitive information about the photos in my virtual territory.	PD4
	I would reveal a lot of information about the photos in my virtual territory.	PD5
* item dropped		

Table A2. Replication Items for Control Variables
Age: number of years from birthdate.
Gender: male; female; other.
Native language: Native language? Arabic; Chinese; English; French; Hindi; Korean; Malay; Portuguese; Spanish; Other, please specify _____.
Education: Highest level of education attained? Some school, no degree; high school diploma; associates degree; bachelor's degree; graduate degree.
Tenure in SNS: Years you have participated in your focal online social network? Less than 1 year; 1-2 years; 2-3 years; 3-4 years; 4-5 years; 5-6 years; 6-7 years; 7 or more.
Connections: Number of connections (e.g., friends, followers, etc.) in the focal online social network? Less than 100; 101-200; 201-300; 301-400; 401-500; 501-600; 601-700; 701-800; 801-1,000; More than 1,000.
Weekly hours in SNS: Hours per week, on average, in the focal online social network? < 1 hour per week; 1-2 hours per week; 3-4 hours per week; 5-6 hours per week; 7-8 hours per week; 9-10 hours per week; 11-14 hours per week; 15-18 hours per week; 19-24 hours per week; 25-30 hours per week; 30-40 hours per week; > 40 hours per week.

Appendix B: Factor Analysis

Table B1. Factor Analysis – First Order

	Component						
	Awareness	Collection	Control	Info Sensitivity	Private Disclosure	Risk Beliefs	Trusting Beliefs
IPC10	**0.93**	0.45	0.38	0.09	-0.20	0.42	0.01
IPC11	**0.94**	0.43	0.47	0.11	-0.22	0.48	0.03
IPC13	**0.96**	0.48	0.40	0.05	-0.19	0.45	0.00
IPC14	**0.95**	0.44	0.47	0.10	-0.22	0.48	0.00
IPC1	0.38	0.39	**0.91**	-0.02	-0.15	0.41	-0.03
IPC2	0.47	0.40	**0.88**	0.00	-0.17	0.40	-0.05
IPC3	0.39	0.42	**0.94**	-0.03	-0.18	0.44	0.02
IPC4	0.43	0.43	**0.94**	0.02	-0.14	0.48	0.01
IPC6	0.34	**0.78**	0.46	-0.01	-0.07	0.34	0.11
IPC7	0.43	**0.82**	0.26	0.00	-0.09	0.36	-0.03
IPC8	0.43	**0.88**	0.46	-0.01	-0.13	0.38	0.01
IPRB1	0.43	0.39	0.42	0.06	-0.08	**0.83**	-0.04
IPRB2	0.44	0.42	0.38	-0.02	-0.16	**0.92**	-0.09
IPRB3	0.47	0.41	0.48	0.04	-0.18	**0.90**	-0.10
IPRB4	0.33	0.29	0.36	0.00	-0.11	**0.86**	-0.12
ITB1	0.03	0.01	-0.11	0.01	0.24	-0.09	**0.72**
ITB2	-0.01	0.04	-0.05	0.06	0.19	-0.15	**0.88**
ITB3	0.00	0.04	0.00	0.03	0.21	-0.13	**0.93**
ITB4	0.08	0.02	0.05	0.06	0.15	-0.03	**0.86**
ITB5	-0.01	0.02	0.06	0.01	0.16	-0.07	**0.88**
ITB6	-0.03	0.06	0.03	-0.03	0.13	-0.07	**0.81**
ITB7	0.01	0.03	0.02	-0.03	0.13	0.01	**0.84**
InfoSens	0.09	-0.01	0.00	**1.00**	-0.24	0.03	0.02
PD1	-0.03	-0.02	-0.05	-0.19	**0.82**	-0.02	0.18
PD2	-0.03	0.02	-0.04	-0.15	**0.82**	-0.08	0.19
PD3	-0.10	0.00	-0.02	-0.20	**0.78**	-0.09	0.11
PD4	-0.34	-0.23	-0.27	-0.21	**0.84**	-0.20	0.19
PD5	-0.29	-0.17	-0.24	-0.23	**0.85**	-0.18	0.21

Table B2. Factor Analysis – Second Order					
	Component				
	Private Disclosure	Privacy Concerns	Info Sensitivity	Risk Beliefs	Trusting Beliefs
Collection	-0.12	**0.81**	-0.01	0.44	0.04
Awareness	-0.22	**0.82**	0.09	0.48	0.01
Control	-0.18	**0.80**	0.00	0.47	-0.01
IPRB1	-0.08	0.41	0.06	**0.83**	-0.04
IPRB2	-0.16	0.41	-0.02	**0.92**	-0.09
IPRB3	-0.18	0.46	0.04	**0.90**	-0.10
IPRB4	-0.11	0.40	0.00	**0.86**	-0.12
ITB1	0.24	-0.03	0.01	-0.09	**0.72**
ITB2	0.19	-0.01	0.06	-0.15	**0.88**
ITB3	0.21	0.02	0.03	-0.13	**0.93**
ITB4	0.15	0.07	0.06	-0.03	**0.87**
ITB5	0.16	0.03	0.01	-0.07	**0.88**
ITB6	0.13	0.02	-0.03	-0.07	**0.81**
ITB7	0.13	0.02	-0.03	0.01	**0.84**
InfoSens	-0.24	0.03	**1.00**	0.03	0.02
PD1	**0.82**	-0.04	-0.19	-0.02	0.18
PD2	**0.82**	-0.02	-0.15	-0.08	0.18
PD3	**0.78**	-0.05	-0.20	-0.09	0.11
PD4	**0.84**	-0.35	-0.21	-0.20	0.18
PD5	**0.85**	-0.29	-0.23	-0.18	0.21

About the Authors

Miaoyi Zeng. Miaoyi Zeng is a Ph.D. student of Management Information Systems in the College of Business at Florida State University. Her research interests lie at the human behavior side of Information systems (IS), focusing on issues involving users' perceptions, intentions, and behaviors in social media platforms, also the usage of emerging information analysis tools.

Shuaifu Lin. Shuai-fu Lin is an assistant professor of Management Information Systems in the Marilyn Davies College of Business at the University of Houston - Downtown. Shuaifu Lin has developed research interests around individual cognition and behavior, and usage of emerging information technologies. Among his projects, Shuaifu's main research interest focuses on privacy issues in the online environment. His research has been published in, among others, the *Journal of the Association for Information Systems* and *Computers in Human Behavior*.

Deborah J. Armstrong. Deb Armstrong is a Professor of Management Information Systems in the College of Business at Florida State University. Her research is programmatic in its focus at the nexus of information systems (IS) - where people, process, and technology coalesce. Specifically, her research interests cover issues at the intersection of IS personnel and cognition, involving the human aspects of technology, change, and learning. Many of the research problems that Deb finds interesting involve gender-related IS workforce issues. She has published articles in such journals as *Management Information Systems Quarterly,* the *Journal of Management Information Systems,* the *Journal of the Association for Information Systems, the European Journal of Information Systems* and *The Database for Advances in Information Systems*. Joshua 1:9, Be strong and courageous. Do not be afraid; do not be discouraged, for the LORD your God will be with you wherever you go.