Association for Information Systems

AIS Electronic Library (AISeL)

Aug 10th, 12:00 AM

Internet Privacy Concerns: A Replication and Parsimonious Extension

Oscar Lopez
University of Massachusetts, olopez@umass.edu

Traci J. Hess
UMass Amherst, traci_ej@yahoo.com

Follow this and additional works at: https://aisel.aisnet.org/amcis2020

Lopez, Oscar and Hess, Traci J., "Internet Privacy Concerns: A Replication and Parsimonious Extension" (2020). *AMCIS 2020 Proceedings*. 40.
https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/40

Internet Privacy Concerns: A Replication and Parsimonious Extension

Emergent Research Forum Paper

Oscar E. Lopez
University of Massachusetts Amherst
olopez@umass.edu

Traci J. Hess
University of Massachusetts Amherst
thess@isenberg.umass.edu

Abstract

Privacy concerns is a widely used construct in Information Systems research. Several different conceptualizations and taxonomies have been proposed but the Internet Privacy Concerns construct by Hong & Thong (2013) offers a more comprehensive approach to integrate previous research. The Internet Privacy Concerns construct is operationalized by an 18-item scale with six sub-dimensions. The present study aims to replicate and validate the best fitting model previously identified as a third-order construct with two second-order constructs, and six first-order dimensions. In addition, this research proposes a more parsimonious three-item criterion measure of internet privacy concerns which can offer researchers a more participant-friendly approach to measuring this relevant construct in IS research. Preliminary results are presented which confirm the original model and support the new criterion measures for internet privacy concerns, called hereafter Parsimonious Internet Privacy Concerns (PIPC) scale.

Keywords: Privacy concerns, internet privacy concerns, replication

Introduction

The age of the internet is pointedly characterized by the transmission of information at mind-shattering volume and speed. Amidst a torrent of problems, including data breaches, privacy violations, identity theft and others, protection of information has been a high priority for legislators, companies, individuals and researchers alike. The issue of information privacy is at the forefront of Information Systems (IS) academic research, yet there remain challenges with conceptualizing and measuring privacy, as described in a book chapter titled "Privacy: A Concept in Disarray" (Solove, 2008). Despite these challenges, there are similarities in the major conceptualizations of privacy. "There are many definitions for information privacy, but there is little variance in the elements of the definitions, which typically include some form of control over the potential secondary uses of one's personal information" (Belanger & Crossler, 2011).

For some time, IS research adopted the Smith, Milberg, & Burke (1996) *information privacy concerns* construct as the default privacy measure. The authors proposed a construct with four dimensions, including collection, errors, secondary use and unauthorized access (Smith et al., 1996). Interestingly, this de-facto standard IS conceptualization does not include a control dimension, describing the control that an individual feels they have over their personal information. Another important component missing from the Smith et al. (1996) conceptualization was awareness, which describes an individual's awareness of what a company may do with someone's personal information (Malhotra, Kim, & Agarwal, 2004), including the disclosures the company provides. A more comprehensive conceptualization of privacy concerns was proposed to address these gaps (Hong & Thong, 2013), and the addition of two dimensions (awareness and control), produced improved psychometric qualifications for the construct. The authors tested different model variations and proposed a third-order construct, with two second-order constructs, and six first-order dimensions, as the best fitting model for privacy concerns. The resulting scale required 18-items, with 3 items for each of the 6 first-order dimensions.
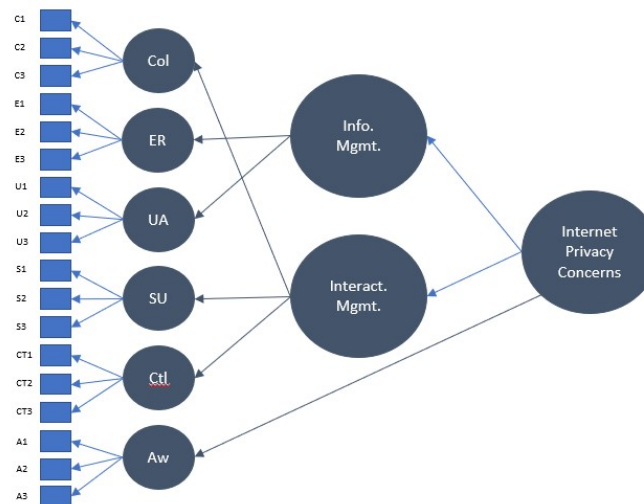
In this research, a replication of the Hong & Thong (2013) study on privacy concerns is first conducted. Next, 3 criterion items are developed to measure the privacy concerns construct in a more parsimonious manner, and are then validated using the 3rd order model of privacy concerns developed by Hong & Thong (2013). Contributions of this work include replication of a study which developed and validated the important privacy concerns scale, and development of a more parsimonious measure of privacy concerns.

Literature Review

Privacy Concerns

Information privacy has long been a subject of study in Information Systems (IS). The default scale for measuring privacy concerns comes from the information privacy concern construct developed in the Smith et al. (1996) study, and later defined as a second-order construct with 4 first-order dimensions: collection, errors, secondary use and unauthorized access (Stewart & Segars, 2002). The Smith et al. (1996) information privacy concerns scale is the most widely used privacy measure in IS (Dinev, Xu, Smith, & Hart, 2013; Miltgen & Peyrat-guillard, 2014). However, other conceptualizations and measures of privacy concerns have been advanced in the literature. A three-dimensional construct called internet user information privacy concerns (IUIPC) (Malhotra et al., 2004) was later proposed as a construct specifically developed for measuring individual's concerns in an online context. This construct included the dimensions of control, awareness and collection, overlapping the Smith et al. (1996) conceptualization with the collection dimension. Solove (2008) presented yet another taxonomy of privacy with four dimensions: information collection, information processing, information dissemination, and invasion. While highly comprehensive, no corresponding scale was developed for this conceptualization.

In an attempt to consolidate the different conceptualizations of privacy concerns, Hong & Thong (2013), developed and conducted four empirical studies aimed at finding the best possible model for a proposed, integrated construct that included 6 dimensions of privacy concerns: collection, errors, secondary use, unauthorized access, control and awareness. Thus, the 6 different dimensions of privacy were combined in one model, with each dimension measured by 3 items, for a total of 18 items. In testing for the best fitting model, 12 different configurations were assessed, and the best fitting model, shown in Figure 1, conceptualized internet privacy concerns (IPC) as a third-order, reflective construct determining two latent, second-order dimensions, labeled "interaction management" and "information management", and the awareness dimension. The collection, secondary use and control dimensions were modeled as reflective, sub-dimensions of the interaction management dimension, while errors and unauthorized access were modeled as reflective, sub-dimensions of the information management dimension.

Figure 1. Best-fitting model of internet privacy concerns per Hong & Thong (2013)

As noted previously, the conceptualization of privacy concerns continues to be a source of challenges and opportunities in IS research. In this study, a replication is conducted to confirm the findings of Hong & Thong (2013) and to validate a new, parsimonious three-item scale of internet privacy concerns.

Research Design

The original Hong & Thong (2013) study scales were used, as shown in Table 1. In addition, three criterion

items were developed to provide a more parsimonious measure of internet privacy concerns.

Item #	Description
	Internet Privacy Concerns (Hong & Thong, 2013) 7pt. Likert-type scale, anchored with Strongly disagree – Strong agree
COLL1	IPC: Collection. It usually bothers me when websites ask me for personal information.
COLL2	IPC: Collection. When websites ask me for personal information, I sometimes think twice before providing it.
COLL3	IPC: Collection. I am concerned that websites are collecting too much personal information about me.
ERR1	IPC: Errors. I am concerned that websites do not take enough steps to make sure that my personal information in their files is accurate.
ERR2	IPC: Errors. I am concerned that websites do not have adequate procedures to correct errors in my personal information.
ERR3	IPC: Errors. I am concerned that websites do not devote enough time and effort to verifying the accuracy of my personal information in their databases.
UNA1	IPC: Unauthorized Access. I am concerned that website databases that contain my personal information are not protected from unauthorized access.
UNA2	IPC: Unauthorized Access. I am concerned that websites do not devote enough time and effort to preventing unauthorized access to my personal information.
UNA3	IPC: Unauthorized Access. I am concerned that websites do not take enough steps to make sure that unauthorized people cannot access my personal information in their computers.
SEC1	IPC: Secondary Use. I am concerned that when I give personal information to a website for some reason, the website would use the information for other reasons.
SEC2	IPC: Secondary Use. I am concerned that websites would sell my personal information in their computer databases to other companies.
SEC3	IPC: Secondary Use. I am concerned that websites would share my personal information with other companies without my authorization.
CON1	IPC: Control. It usually bothers me when I do not have control of personal information that I provide online.
CON2	IPC: Control. It usually bothers me when I do not have control or autonomy over how my personal information is collected, used, and shared online.
CON3	IPC: Control. I am concerned when control is lost or unwillingly reduced as a result of making an online transaction.
AWA1	IPC Awareness. I am concerned when a clear and conspicuous disclosure is not included in online privacy policies.
AWA2	IPC Awareness. It usually bothers me when I am not aware or knowledgeable about how my personal information will be used on websites.
AWA3	IPC Awareness. It usually bothers me when websites do not disclose the way the data are collected, processed, and used.
Proposed Internet Privacy Concerns 3-Item Measure (7 point)	
OPC1	Overall, to what degree are you concerned about the privacy of the information you provide online? Extremely concerned - Not concerned at all
OPC2	In general, I am concerned about the online privacy of my personal information. Strongly disagree - Strongly agree
OPC3	How worried are you with the privacy of your personal information on the internet? Extremely worried- Not worried at all

Table 1. Measurement Items

Data collection was conducted using a Qualtrics survey on Amazon's Mechanical Turk. Participants were compensated with payments ranging from 1 to 2 USD and were requested to be in the United States. The total number of respondents is 300. Ten responses were discarded for having an unacceptably low response time. All remaining responses successfully answered an attention check item, bringing the total valid participant count to 290. The Hong & Thong (2013) study in which the 3rd order model was tested as having the best fit, included 887 participants.

Participants were approximately gender balanced with 152 identifying as males, 137 as females and 1 as

'other'. The average age of the participants was 41, with a range of 24 to 73. The standard deviation on the participant age was 10.98. Finally, participants took an average of 8 minutes to complete the survey.

Data Analysis

Reliability analysis was performed with IBM SPSS 26. The lowest Cronbach's alpha score for a single dimension was .857 for the collection dimension of the internet privacy concerns construct. All the remaining dimensions scored above .90 (see table 2). These scores were acceptable measures of construct reliability and are equal or better than those reported in the original study (Hong & Thong, 2013).

	Alpha	CR	Collection	Errors	Unauth-Access	Secondary Use	Control	Aware-ness
Collection	0.857	0.668						
Errors	0.914	0.906	.422**					
Unauthorized Access	0.953	0.858	.654**	.437**				
Secondary Use	0.929	0.732	.738**	.442**	0.771**			
Control	0.929	0.766	.759**	.434**	0.656**	.700**		
Awareness	0.924	0.817	.679**	.492**	0.628**	.650**	.814**	
PIPC	0.927	0.893	.804**	.370**	0.604**	.689**	.710**	.658**

Table 2. Cronbach's Alpha, Correlations

A confirmatory factor analysis was run using several different model configurations, based on Hong & Thong (2013). The best model fit was found using the third-order model with two second-order constructs and six first-order constructs as previously depicted in Figure 1, and shown below in Figure 2 with the current study results. These results largely confirm the findings of the original study. Fit statistics were .948 for CFI, .048 for RMSR and .091 for RMSEA. These fit statistics are close to, or less than, recommended thresholds. While not as high as the fit statistics obtained in the original study, the sample size of 290 was also much smaller than the 887 participants in the original study. There are two discrepancies noted in the results below. The factor loading for the errors dimension was only .501, and the factor loading for the second-order construct interaction management was greater than 1, at 1.02. Additional data collection is being planned to better assess these results.
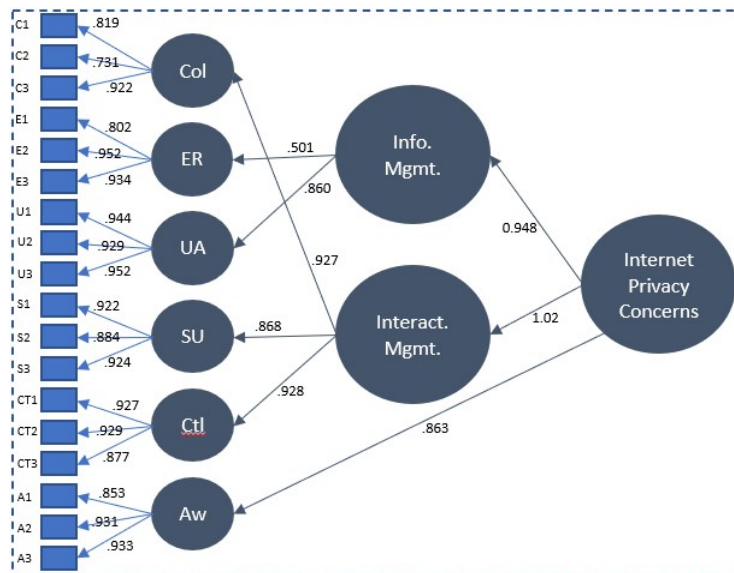

Figure 2. Replication results

Next, the new criterion items were validated using the model shown below in Figure 3. The path between the third-order model of internet privacy concerns and the newly developed three-item scale, was high, at .839. These findings suggest that the parsimonious 3-item scale of internet privacy concerns (PIPC) is a good surrogate for the third-order model with 18 measurement items, when privacy concerns are being used more for control purposes. In research where the 6 dimensions of privacy concerns can provide

insight on relevant antecedents and outcomes, the 18-item measurement scale should be used.

Conclusion

This paper confirmed the best-fitting model from Hong & Thong (2013), and provided preliminary evidence that the 3 item criterion measure of PIPC works well as a more parsimonious scale. Additional data collection is planned to bring the sample size closer to that of the original study, and run confirmatory factor analysis again with more rigorous assessments of validity, to confirm the findings and provide further insight on some unexpected findings (i.e., problematic loadings, as discussed above).
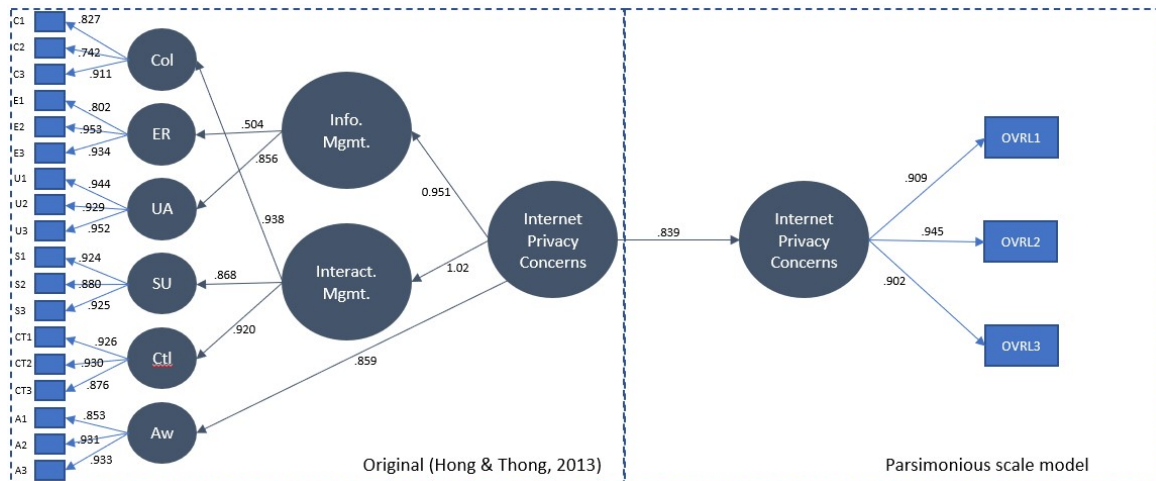
Figure 3. Validation of new, parsimonious internet privacy concerns

REFERENCES

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

Belanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1041.

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

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80.

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*(1561), 295–316.

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

Korzaan, M. L., & Boswell, K. T. (2008). The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information*, *48*(4), 15–24. Retrieved from

Li, H., Luo, X., Zhang, J., & Xu, H. (2016). Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information and Management*, (2016).

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.

Miltgen, C. L., & Peyrat-guillard, D. (2014). Cultural and generational influences on privacy concerns. *European Journal of Information Systems*, *23*(2), 103–125.

Smith, J. ., Milberg, S. ., & Burke, S. . (1996). Information privacy: measuring individuals concerns about organizational practices. *MIS Quaterly*, *20*(2), 167–196.

Solove, D. J. (2008). *Understanding Privacy* (1st ed.). Cambridge, MA: Harvard University Press.

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