Transactions on Replication Research

Conceptual Replication

Empirical Examination of Information Privacy Concerns Instrument in the Social Media Context

Babajide Osatuyi
The University of Texas Rio Grande Valley
babajide.osatuyi@utrgv.edu

Abstract:

Concern for information privacy (CFIP) has been widely studied across several domains using Stewart and Segars' (2002) second-order model that includes four first-order constructs: errors, collection, unauthorized access, and secondary use. However, unlike the organizational context in which the model was developed, the social media context encourages self-disclosure of information among users and social media platform providers. Consequently, users' concern for social media information privacy (CFSMIP) is expected to manifest differently as compared to CFIP in other contexts. In an effort to advance science in the privacy domain in Information Systems, this study therefore argues that the existing privacy model needs to be replicated in this new context to assess its validity and explanation power. Based on a sample of avid social media users, this study explores the factor structure of the four dimensions of concern for information privacy instrument posited in prior research and validated across several contexts. Exploratory factor analysis and a consequent confirmatory factor analysis revealed three first-order factors structure in the social media context. Additional analysis revealed that the three-factor second order structure of CFSMIP outperforms the four-factor second order structure from prior research.

Keywords: Privacy Concerns, Social Media, Instrument Development, Information Privacy, Validity, Confirmatory Factor Analysis, Exploratory Factor Analysis

The manuscript was received 10/13/2014 and was with the author 1 months for 1 revision.

1 Introduction

The prevalence of social media avail individual users and organizations with unprecedented access to personal information that was once arduous to gather. Undoubtedly, privacy concerns on social media platforms become critically important as vendors can now potentially have access to a large collection of users' personal information. Unlike other online applications, users voluntarily contribute their personal information on social media platforms (Xu et al. 2013), thereby increasing the ease of gathering and using personally identifiable information.

A model for measuring users' concern for information privacy proposed by Stewart and Segars (2002) have been validated across several domains as a second-order construct with four first-order constructs including errors, collection, unauthorized access, and secondary use. However, the voluntary information self-disclosure allowance in the social media context is expected to shape the privacy concerns differently compared to other technologies.

Although a validated model exist for measuring users' concern for information privacy with the use of different technologies, the conduct of progressive science instructs the replication and validation of existing frameworks in a new context. Similarly, researchers call for "theoretical and operational assumptions underlying the structure of constructs such as concern for information privacy (CFIP) should be re-investigated in light of emerging technology, practice, and research (Stewart et al. 2002, p.37)." Replication of the existing CFIP model in the social media context will contribute to our understanding of information privacy as well as provide a foundation for future studies in that domain. In particular, the objective of this paper is to replicate and extend Stewart and Segars' (2002) CFIP model in the social media context. This article contributes to the information privacy literature by providing empirical evidence of the replication of CFIP model in the social media context as CFSMIP.

In this study, social media information privacy concern (CFSMIP) is defined as concerns about loss of privacy as a result of the disclosure of personal information to known and unknown external agents—including other social media users, social media platforms, and third parties.

2 Background

2.1 Current Information Privacy Concern Measurement Instruments

One of the major breakthroughs in information privacy research was a study conducted by Smith et al. (1996). In their work, they found that concern for information privacy was influenced by four fundamental factors based on individuals' concern in response to organizations' information practices, namely collection, unauthorized secondary use (internal and external), improper access to personal information, and errors in personal information storage. Smith et al., (1996) measured and validated the four factors as first-order constructs in a nomological network.

In a later validation of Smith et al.'s (1996) model, Stewart and Segars (2002) posited that CFIP is complex and should be measured as a second-order construct. Stewart and Segars (2002) then developed, tested, and validated their proposed hypothesis with CFIP as a multi-dimensional construct in a nomological network and found that it mediated the relationship between computer anxiety and behavioral intentions. Since then, researchers have validated the use of CFIP as a second-order construct, in nomological models across different contexts including the Internet (Malhotra et al. 2004) and instant messaging technologies (Lowry et al. 2011).

In response to Stewart and Segar's (2002) call to investigate the shifting dimensions of information privacy concerns in light of emerging technology, practice, and research, Xu et al., (2012, p.3) developed a 9-item instrument to measure mobile users' concerns for information privacy. The research program through which this study is conducted responds to the same call as it investigates measurement scales needed to understand individuals' concern for information privacy on social media platforms, which is increasingly becoming an important communication medium for users, organizations, and government entities.

2.2 Concern for Social Media Information Privacy (CFSMIP)

The current CFIP model is a second-order construct that contains four first order scales—errors, collection, unauthorized access and secondary use—that relate to the use of users' personal information without their consent. These constructs are relevant in the social media context.

Smith et al. (1996, p.172) described error as individuals' "concern that protections against deliberate and accidental errors in personal data are inadequate." The authors noted that privacy-related concerns are initiated when errors are made in the representation of customers' information. In the offline context, such errors are not uncommon due to inevitable mistakes with the data entry process. However, in the context of social media where personal information is user-generated, improper update of personal information may also lead to erroneous personal data. Also, third party marketing entities that gain access to such erroneous user information are bound to offer target services that may be unwanted by the user. Hence, this study posits that errors characterize CFSMIP as it can affect the user, the platform provider, and third party vendors.

Collection is defined in the information privacy research stream as "concern that extensive amounts of personally identifiable data are being collected and stored in databases (Smith et al. 1996, p.172)." In today's data-driven society, aggressive data collection strategies are used by various organizations to build a better understanding of their customers as well as to maintain competitive advantage. However, as noted by several researchers (Malhotra et al. 2004; Smith et al. 1996), the practice of data collection, justifiable or not, raises privacy concerns for customers. With minimal integration into one's daily routine, social media applications may be used to track and gather an individual's behavioral pattern throughout each day e.g., choice of lunch locations, favorite online radio playlist, running/walking route information sharing with friends etc.

Users may not use social media for the fear that their personal information and private conversations may be collected and stored for future business or intelligence analysis. Studies report that when individuals are provided with a significant control over information disclosure, they create boundary structures that reduce the amount of information collection by others or they establish boundaries with low permeability (Child et al. 2009; Petronio 2010). Accordingly, this research posits that personal information collection is an important factor that characterizes CFSMIP.

Secondary use is the use of personal data collected by an organization for a legitimate reason (e.g., shipping information by an e-commerce company), but used for a secondary purpose without the consent of the user. Unauthorized access describes the interception of personal information captured from a legitimate transaction by a third party without the consent of either the user or the organization. In the context of social media, secondary use and unauthorized access both describe access and use of personal information without receiving permission from the information owner(s).

Based on the validated CFIP model posited by Stewart and Segars (2002), the constructs are adapted to the social media context and tested with data from avid social media users. Accordingly, the relationship between CFSMIP, social media anxiety, and behavioral intentions to use social media for sharing information is illustrated in the current CFSMIP model in Figure 1 below.

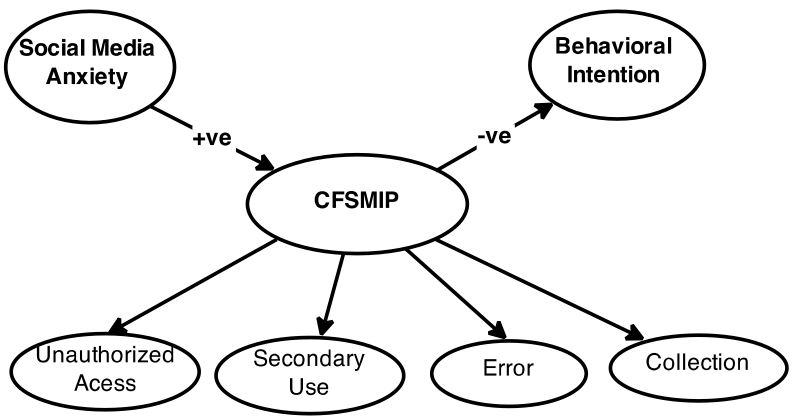

Figure 1. Current CFSMIP Model

In an attempt to replicate the measurements used in prior research by Stewart and Segars (2002), social media anxiety is proposed to replace computer anxiety. Drawing on prior definition of computer anxiety (Howard et al. 1986), social media anxiety describes an individual's tendency to experience a level of uneasiness over the impending use of social media sites to connect, share, and participate in conversations. Social media anxiety is expected to lead to greater concern for information privacy on social media sites. This relationship is expected since anxiety has been shown to influence concern for information privacy in other contexts (Korzaan et al. 2009; Korzaan et al. 2008; Stewart et al. 2002). Also, an individual that is anxious about the use of social media to share personal information is likely to be concerned about who will gain access to, misrepresent, or collect the information shared for other purposes.

Based on the test of CFIP in a nomological net, CFSMIP is expected to influence behavioral intention to use continue to use social media sites to share personal information or engage in activities that require the provision of personal information (e.g., purchasing celebratory gifts for friends on social media sites). In the social media context, it is expected that there will be a negative relationship between CFSMIP and behavioral intentions since users that are concerned about their personal information will be less inclined to share that information with others.

Finally, we propose that information privacy concerns on social media sites will mediate the relationship between social media anxiety and behavioral intentions. The acknowledgment of privacy concerns (CFSMIP) associated with information shared on social media sites will reduce the anxiety of users tendency towards using social media sites for information sharing. Prior studies found support for the mediation effect of privacy concern on the relationship between anxiety and behavioral intentions in the organizational context (Smith et al. 1996; Stewart et al. 2002).

3 Methodology

3.1 Scale Development

A survey instrument was developed to test the hypothesized model in accordance to the practice in the information privacy domain (Smith et al. 1996; Son et al. 2008). Scales from the instruments for measuring concern for information privacy posited Smith et al., (1996) were adapted based on prior research. Information access was measured by a combination of items from unauthorized access and secondary use scales from Smith et al. (1996). Collection and error were adapted from Smith et al. (1996) and measured with multiple items on five-point Likert scales, anchored with strongly disagree to strongly agree. Behavioral intentions and social media anxiety were adapted from Stewart and Segar's (2002) and measured with three items on five-point Likert type scales, anchored with highly likely to not at all likely and strongly disagree to strongly agree respectively.

Experts in both social media and information privacy research fields reviewed the initial versions of the survey questions. Additional feedback was received from a sample of graduate and undergraduate students on the clarity of the questions and options before the final version was finally developed. All measurement items used in this research are included in the Appendix.

3.2 Survey Design

An online survey was developed and the link was sent to college students registered in an Introduction to Information Systems course in a southern region of United States. Students received extra-credits toward their final grade for participating in the study. To protect the privacy of participants and in compliance with the IRB regulations of the researcher's institution, no personally identifiable information was collected from participants. There were 310 participants in the study, but only 298 of the responses were complete and useful for analysis, yielding a 96.1% response rate. Respondents had a median age of 19, and 63.2% of them were female. 91% of the participants reported that they use social media on a daily basis. The study sample demographics reflect the user population on social media sites (Smith et al. 2011). Based on Pew research reports (Smith et al. 2011), college students are predominant social media users, hence, sampling from this population is ideal for this research.

4 Data Analysis and Results

Data analysis was conducted in two phases; Phase 1 sought to identify and validate the factor structure of CFSMIP and Phase 2 evaluated CFSMIP in a nomological network.

4.1 Step 1: Identification: Factor Structure of CFSMIP

Identifying a proper structure for the CFSMIP construct is necessary since it comprises scales from mature and validated instruments in addition to a newly developed item based on prior literature. As suggested by prior literature (e.g., Malhotra et al. 2004), exploratory factor analysis (EFA) of the various factors of CFSMIP was conducted followed by confirmatory factor analysis (CFA).

EFA was conducted with IBM SPSS software using Principal Components Analysis technique with VARIMAX rotation and Kaiser Normalization. The EFA included the four dimensions of CFIP posited by Smith et al., (1996). As shown in Table 1, three components were revealed and all the items loaded cleanly on their respective constructs with no cross loadings. As shown in Table 1, three components were revealed with two of the dimensions from prior research (unauthorized access and secondary use) converging on the same factor component.

Table 1. Principal Component Analysis using VARIMAX Rotation

Factor	Items	Component I			
		1	2	3	CA
Collection	COL1		**.783**		0.82
	COL2		**.747**		
	COL3		**.809**		
	COL4		**.740**		
Error	ERR1			**.852**	0.92
	ERR2			**.812**	
	ERR3			**.873**	
Unauthorized Access	UAC1	**.743**			0.93
	UAC2	**.766**			
	UAC3	**.819**			
	UAC4	**.660**			
Secondary Use	SUS1	**.805**			
	SUS2	**.765**			
	SUS3	**.805**			
Rotation Sums of Squared Loadings	Total	4.655	2.894	2.720	
	% Variance	33.251	20.671	19.426	
	Cumulative Variance	33.251	53.921	73.347	

CA-Cronbach's Alpha

Cronbach Alpha was used to assess the reliability of the factors revealed from the EFA (Bagozzi 1980). Cronbach Alpha for the three factors in EFA exceed the 0.70 threshold recommended by Nunnally (1978), indicating convergent validity. Since the unauthorized access construct loads on the same factor as the secondary use construct, it is plausible to propose an alternative factor structure for CFSMIP. The alternative CFSMIP structure can be divided into three dimensions (unauthorized access and secondary use, collection, and error) as described in Table 2.

Table 2. Principal Component Analysis using VARIMAX Rotation

Factor	Items	Component I			
		1	2	3	CA
Collection	COL1		**.783**		0.82
	COL2		**.747**		
	COL3		**.809**		
	COL4		**.740**		
Error	ERR1			**.852**	0.92
	ERR2			**.812**	
	ERR3			**.873**	
Information Access	IAC1	**.743**			0.93
	IAC2	**.766**			
	IAC3	**.819**			
	IAC4	**.660**			
	IAC5	**.805**			
	IAC6	**.765**			
	IAC7	**.805**			
Rotation Sums of Squared Loadings	Total	4.655	2.894	2.720	
	% Variance	33.251	20.671	19.426	
	Cumulative Variance	33.251	53.921	73.347	

Consistent with prior study (Smith et al. 1996), CFA is used to assess the efficacy of the model structure suggested from the EFA, which contains 14 items. This research follows the procedures used by Stewart and Segars (2002) to conduct CFA, which compared covariance matrices based on observed data and the hypothesized models. According to Stewart and Segars (2002), CFA allows a researcher to specify, estimate, and re-specify multiple and interrelated dependence relationships as well as unobserved constructs. CFA assesses a hypothesized model by comparing its observed covariance matrix with the implied covariance matrix. The implied matrix is a set of covariances (14 × 14) generated through maximum likelihood estimation as a result of the specified model (Stewart et al. 2002). The closer the two models are, the better the model fit indicating that the specified model is indicative of the data collected. Goodness-of-fit indices are then used to report the result of the comparison between the observed and implied matrices. In accordance with prior studies (Bentler et al. 1980; Marsh et al. 1988), multiple fit indices were used for assessing the fit between the observed and implied models in this study. The

following section presents four hypothesized models to assess the factorial nature of CFSMIP and compares it with the existing CFIP structure from prior study (Stewart et al. 2002).

Model 1 hypothesizes that all items of CFSMIP form into one first-order factor accounting for all the common variance among the 14 items. Prior research (Smith et al. 1996) measured privacy concern as though it were a unidimensional construct indicating that one first-order factor can be used to explain the underlying data structure. If this model is accepted, then it is appropriate to consider CFSMIP as a single dimension that governs similarities in variation among all 14 items.

Model 2 hypothesizes that all 14 items of CFSMIP form into two first-order factors: secondary use and unauthorized access is loaded onto one factor and error and collection are loaded onto the second factor. This model proposes that individuals' concern for information privacy on social media sites is divided into two areas: 1) individuals' concern for privacy may be triggered by their perception of other people's access to their personal information and misuse of such information, and 2) users' concern as a result of erroneous collection of personal information on social media sites.

Model 3 hypothesizes that three first-order factors account for the covariance among the 14 items as unauthorized access and secondary use, collection, and error. This model suggests scaling CFSMIP as an average of the subscale scores to calculate an overall score. As noted by Stewart and Segars (2002), the assumption of this model is that all the items are equally important in computing each factor and each factor is equally vital to computing the overall score for the CFSMIP construct.

Model 4 hypothesizes that all items form into three first-order factors, which are then measured by a second-order factor CFSMIP. According to Stewart and Segars (2002), in such a model, "the inter-correlations among first-order factors form a system of interdependence (or covariation) that is itself important in measuring the construct. Conceptually, each factor and the second-order factor are necessary in capturing the nature of the construct domain (Stewart et al. 2002, p.39)." CFSMIP can therefore be defined as three distinct factors as well as the structure of interrelationships among these factors.

Model 5 is the existing second-order factor structure of CFSMIP proposed from prior research with four first-order factors. This model is developed to compare its performance with the hypothesized and emergent models in this study.

Table 3 presents the results of testing all five models for CFSMIP. As in prior research (Stewart et al. 2002; Xu et al. 2012), fit indices are examined in terms of NFI, GFI, AGFI, CFI, NNFI, Std. RMR, and RMSEA. As shown in the results, Model 1 and Model 2 have poor goodness of fit indices. Models 3, 4 and 5 have acceptable goodness fit indices, but Models 4 and 5 (2nd-order factors) indicate better fit to the data. This result supports Stewart and Segar's (2002) thesis that information privacy concern models are better structured as a higher order factor models rather than 1st-order factor models. Since Model 4 and Model 5 exhibit stronger measures of fit compared to other alternative models, the convergent and discriminant validity of both models are further examined.

Table 3. Measures of Model Fit: Confirmatory Factor Analysis Results for Alternative Factor Structures

Fit Indices	Recommended Indices	Alternative CFSMIP Factor Structures				
		Model 1: One 1st-Order Factor	Model 2: Two 1st-Order Factors	Model 3: Three 1st-Order Factors	Model 4: 2nd-Order Factor	Model 5: 2nd-Order Factor
χ2		387.70*	306.58*	114.35*	82.12	82.65
df		64	63	69	64	111
χ2/(df)	< 3.00	6.06	4.87	1.66	0.74	1.29
NFI	> 0.90	0.87	0.90	0.98	0.98	0.97
GFI	> 0.90	0.84	0.85	0.95	0.97	0.96
AGFI	> 0.80	0.73	0.75	0.92	0.95	0.94
CFI	> 0.90	0.89	0.92	0.98	0.99	0.99
NNFI	> 0.90	0.84	0.88	0.98	0.99	0.99
Std.RMR	< 0.05	0.08	0.07	0.03	0.02	0.03
RMSEA	< 0.06	0.13	0.11	0.05	0.00	0.03

*p<0.05; Std. RMR-Standardized RMR

As shown in Table 4 the t-values for all the construct items indicate significant factor loadings and provide evidence to support the convergent validity of the items measured (Anderson et al. 1988). The composite reliability results shown in Table 4 measure internal consistency of the scales, each exceeding the recommended 0.70 threshold (Fornell et al. 1981), indicating satisfactory reliability for all the factors. The average variance extracted (AVE) for each scale exceeds the recommended 0.50 threshold (Fornell et al. 1981). Put together, both models demonstrate strong properties of convergent validity.

Table 4. Convergent Validity for Model 4 and Model 5									
Construct	Item	Model 4				Model 5			
		Std. Loading	t	AVE	CR	Std. Loading	t	AVE	CR
Collection	COL1	0.97	7.79	0.95	0.99	0.92	7.26	0.85	0.94
	COL2	0.95	7.74			0.85	7.43		
	COL3	0.99	9.44			0.93	10.77		
	COL4	0.99	8.37			0.89	7.43		
Error	ERR1	0.89	15.89	0.90	0.96	0.84	16.24	0.86	0.95
	ERR2	0.99	16.14			0.91	15.92		
	ERR3	0.95	16.66			0.89	16.67		
Information Access = Unauthorized Access + Secondary Use of Personal Information	UAC1/IAC1	0.88	16.66	0.93	0.99	0.85	19.64	0.88	0.98
	UAC2/IAC2	0.99	20.48			0.94	19.23		
	UAC3/IAC3	0.98	18.87			0.92	18.87		
	UAC4/IAC4	0.94	16.99			0.94	16.89		
	SUS1/IAC5	0.90	16.65			0.88	14.98		
	SUS2/IAC6	0.90	15.89			0.89	12.67		
	SUS3/IAC7	0.92	17.53			0.90	15.23		

AVE—Average Variance Extracted; CR—Composite Reliability; t—t-value

Although the psychometric properties of Model 4 and Model 5 are strong and satisfactorily fit the data, Model 4 represents the structure of CFSMIP more parsimoniously than Model 5.

To assess the discriminant validity of the new CFSMIP model, correlations among the latent variables are examined as shown in Table 5. Discriminant validity is assessed if the square root of the AVE is larger than correlation coefficients (Fornell et al. 1981). The result shows that correlations among the latent variables are less than the square root of the AVEs along the diagonals of Table 5. Hence, the measurement model is shown to exhibit strong discriminant validity.

Table 5. Correlations among Latent Variables			
	IAC	COL	ERR
Information Access (IAC)	**0.93**		
Collection (COL)	0.56	**0.87**	
Error (ERR)	0.65	0.44	**0.93**

4.2 Step 2: Validation: CFSMIP within a Nomological Network

Consistent with prior work (Stewart et al. 2002), the construct for CFSMIP is tested for nomological validity. In accordance with the approach recommended by Chin (1998), establishing the efficacy of a second-order model involves its assessment with other constructs within a nomological network. In accordance to the procedure established by Stewart and Segars (2002), a second-order factor is expected to act as a significant mediator when embedded within a network of predictor and consequent variables. Accordingly, CFSMIP is placed between a predictor variable (social media anxiety) and a

consequent variable (behavioral intention). Stewart and Segars (2002) validated CFIP as a mediator between individuals' frustration with the use of computers (i.e., computer anxiety) and their behavioral intention to use it in future. Individuals that are apprehensive or fearful about current or future use of computers are found to have stronger levels of privacy concerns (Smith et al. 1996; Stewart et al. 2002). As such, this article argues that CFSMIP will act as a consequent of social media anxiety. Individuals that are anxious about the use of social media are highly likely to be concerned about how their personal information is collected and used on social media platforms.

As for the predictor variable of CFSMIP, individuals with higher levels of privacy concerns are more likely in the future to refuse to disclose their personal information, and refuse to use a technology that demands data collection with online merchants. Prior research provides evidence for a negative relationship between privacy concern and behavioral intention (Xu et al. 2004). Therefore, a negative relationship is expected between CFSMIP and users' behavioral intentions.

Adapting previously defined scales in the social media context, the analysis of CFSMIP is expanded using a 20 × 20 covariance matrix consisting of a 14-item CFSMIP scale, a 3-item social media anxiety scale, and a 3-item behavioral intentions scale. Table 6 presents the structural model for Model 6 (3-factor structure model) and Model 7 (4-factor structure model).

Table 6. Measures of Model Fit: CFSMIP within a Nomological Network

Fit Indices	Recommended Indices	Model 6: 2nd-Order Factor	Model 7: 2nd-Order Factor
χ2		105.17	111.11
df		101	145
χ2/(df)	< 3.00	1.04	1.10
NFI	> 0.90	0.97	0.95
GFI	> 0.90	0.96	0.95
AGFI	> 0.80	0.94	0.93
CFI	> 0.90	0.99	0.99
NNFI	> 0.90	0.99	0.99
Std.RMR	< 0.05	0.04	0.04
RMSEA	<0.06	0.01	0.02

Following recommendations from prior research, fit indices in terms of Normed χ2, NFI, GFI, AGFI, CFI, NNFI, and RMSEA indicate good model fit for Model 6 and Model 7. Based on the NFI, GFI, AGFI, and RMSEA indices, Model 6[1] demonstrates stronger fit compared to Model 7. Figure 2 demonstrates the revised 3-factor structure model (Model 6) and associated estimate of CFSMIP mediating the relationship between social media anxiety and behavioral intentions. The paths are all significant and consistent with the theoretical prediction. When compared to Model 7, Model 6 appears to have a better fit to the data.

[1] Discriminant validity was also verified using nested model method recommended by Bagozzi et al. (1991), which showed significant differences among all the models, showing that the constructs are distinct from one another. Common method bias analysis was conducted to rule out the variance attributable to the measurement method rather than to the constructs, and none was observed in the data.

Based on the final model (Model 6), the hypothesized relationships between social media anxiety, CFSMIP, and behavioral intention are all supported. Using bootstrapping procedures recommended for mediation test (Preacher et al. 2008) indicate that the 95% confidence interval ranged from .03 to .18, thus showing that CFSMIP mediates the relationship between social media anxiety and behavioral intentions.

5 Discussion and Conclusions

The research program through which this study was conducted sought to begin the investigation of information privacy in the social media context by replicating prior studies. Replication provides validity of information privacy measurement items proposed from prior studies in the social media context and contributes to the advancement of science in the field of Information Systems. It is plausible to expect that privacy issues in social media will become important, as consumers' personal information is more readily accessible by other users, vendors, and social media platforms. Although research in the area of information privacy is matured and extensive, the social media context of information privacy research is in its infancy, and requires further exploration.

This study empirically present CFSMIP as a three dimensional second-order construct including, information access to users' personal information, collection of personal information, and errors with the storage and representation of personal information. The three-factor structure of CFSMIP was revealed in an exploratory factor analysis (EFA), which was further confirmed through confirmatory factor analysis. Three factors emerged from the EFA with secondary use and unauthorized access loading on one factor, errors loaded on the second factor, and collection loaded on the third factor. Further analysis revealed that the 2nd-order factor model of CFSMIP outperformed the four-factor 2nd-order factor model of CFSMIP from prior studies (2002) based on better model fit indices. The better fit indices for the three-factor model of CFSMIP does not simply imply that social media users are concerned about these issues, but it also suggest that interdependencies among these issues are vital to measuring individuals' information privacy concerns on social media platforms (CFSMIP).

More importantly, the three-factor structure observed in the social media context suggests that users view unauthorized access and secondary use of information as the same phenomenon. The voluntary disclosure of personal information on social media differentiates it significantly from other contexts where access to one's information is restricted only to authorized personnel. However in the social media context, unauthorized access and use of one's personal information is, by default, privy to social media users, social media providers and third parties. Facebook's unauthorized access and secondary use of users' information to post the recent "Year in Review" collage on users' profile is an example of information access on social media. While the "Year in Review" algorithm is meant to aggregate the most popular posts in the year, users have demonstrated their concern with those posts, as some of the most engaging posts during the year may have be associated with horrid memories (Peterson 2014).

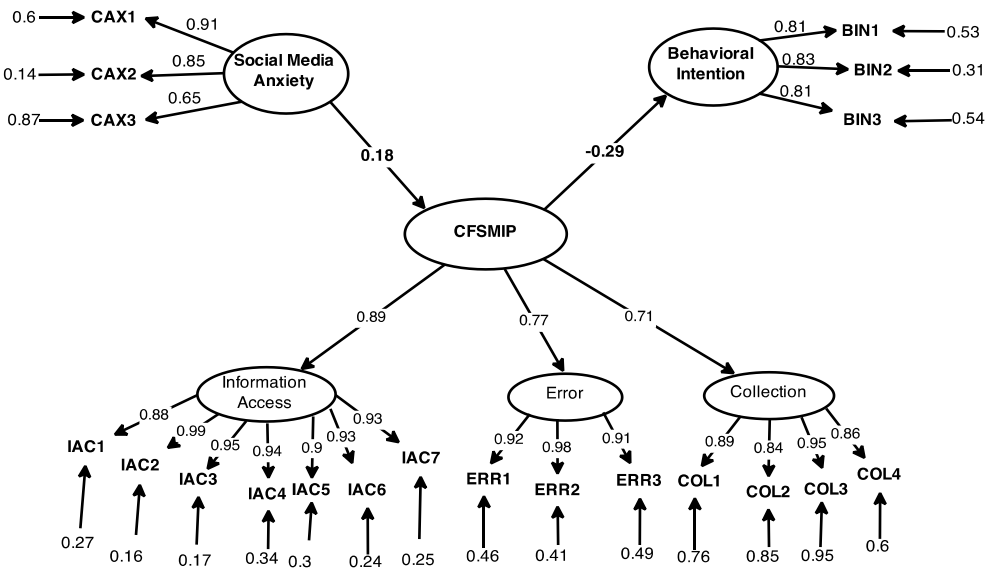

Figure 2: Revised CFSMIP as a 2nd-Order Model in a Nomological Network

The results of this study provide interesting insights into the dimensionality of CFSMIP construct in the context of social interactions. This study therefore contributes to the literature by replicating and extending the instrument for measuring individuals' privacy concern on social media platforms. As noted by Stewart and Segars (2002), with this validated instrument, further research can now be conducted into the relationships among antecedents and consequences of information privacy concerns on social media platforms. Additionally, researchers are invited to use the instrument developed in this study with confidence due to the strong reliability and validity of the constructs indicated in the results. The CFSMIP instrument can now be used as a standardized measure of individuals' concern for information privacy on social media platforms.

Although the results presented are insightful, there are limitations associated with the conduct of this study. As noted in prior research (Stewart et al. 2002, p.45), results of confirmatory factor analysis must be interpreted cautiously, since the "criteria for comparing [competing] models and assessing goodness-of-fit indices are relative and not absolute." This suggests that a model is a good representation of reality when it can be replicated in subsequent studies. As such, the authors call on researchers to further confirm the validity of CFSMIP in across social media contexts. For instance, research may validate the efficacy of this instrument on different social media platforms such as assessing the mediating effect of CFSMIP on social networking sites such as Facebook and Bebo. Studies can also be conducted to compare the mediating effect of CFSMIP across different types of social media platforms including comparison between social networking sites (e.g., Facebook) and microblogging sites (e.g., Twitter).

Acknowledgements

The author acknowledges the review team for the constructive comments provided. Many thanks to members of Social Media Research Lab currently located at the University of Texas Rio Grande Valley and NFG Research Lab for their help with proofreading, designing and funding this research.

References

Anderson, J. C., & Gerbing, D. W. (1988). Structural equation modeling in practice: A review & recommendation two-step approach. *Psychological Bulletin*, 103(3), 411-423.

Bagozzi, R. P. (1980). *Casual methods in marketing*. New York: John Wiley & Sons.

Bentler, P. M., & Bonett, D. G. (1980). Significance tests & goodness of fit in the analysis of covariance structures. *Psychological Bulletin*, 88(3), 588.

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

Chin, W. W. (1998). Issues & opinion on structural equation modeling. *MIS Quarterly*, 22(1), VII-XVI.

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

Howard, G. S., & Smith, R. D. (1986). Computer anxiety in management: myth or reality? *Communications of the ACM*, 29(7), 611-615.

Korzaan, M., Brooks, N., & Greer, T. (2009). Demystifying personality & privacy: An empirical investigation into antecedents of concerns for information privacy. *Journal of Behavioral Studies in Business*, 1(1) 1-17.

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

Lipford, R. H., Wisniewski, J. P., Lampe, C., Kisselburgh, L., & Caine, K. (2012). Workshop on reconciling privacy with social media at The ACM Conference on Computer Supported Cooperative Work. Washington, USA.

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.

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

Marsh, H. W., & Hocevar, D. (1988). A new, more powerful approach to multitrait-multimethod analyses: Application of second-order confirmatory factor analysis. *Journal of Applied Psychology*, 73(1), 107-117.

Nunnally, J. (1978). *Psychometric Theory.* New York: McGraw-Hill.

Peterson, A. (2014, December 26). Facebook's 'Year in Review' app swings from merely annoying to tragic. *The Washington Post*. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/26/facebooks-year-in-review-app-swings-from-merely-annoying-to-tragic/

Petronio, S. (2010). Communication privacy management theory: What do we know about family privacy regulation? *Journal of Family Theory & Review*, 2(3), 175-196.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic & resampling strategies for assessing & comparing indirect effects in multiple mediator models. *Behavior research methods*, 40(3), 879-891.

Smith, A., Raine, L., & Zickuhr, K. (2011). College students & technology. *Pew Research Center*. Retrieved from http://www.pewinternet.org/2011/07/19/college-students-and-technology/

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

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy & a nomological model. *MIS Quarterly*, 32(3), 503-529.

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, 13(1), 36-49.

Xu, H., & Bélanger, F. (2013). Information Systems Journal Special issue on: Reframing privacy in a networked world. *Information Systems Journal*, 23(4), 371-375.

Xu, H., Gupta, S., Rosson, M. B., & Carroll, J. M. (2012). Measuring mobile users' concerns for information privacy. *Proceedings of 33rd Annual International Conference on Information Systems*. Orlando, FL.

Xu, H., & Teo, H.-H. (2004). Alleviating consumers' privacy concerns in location-based services: A psychological control perspective. *Proceedings of the Twenty-Fifth Annual International Conference on Information Systems* (pp. 793-806). Washington, D.C.

Appendix A: Concern for Information Privacy Measurement Scales

Social Media Anxiety (SMA) [Based on: (Stewart et al. 2002)]

1. I am sometimes frustrated by increasing social media use in the society.
2. I am sometimes afraid that I will delete important messages/pictures on social media sites.
3. I am sometimes afraid that I will mistakenly send personal information to the wrong recipients on social media sites.

Concern for Information Privacy [Source: (Smith et al. 1996)]
Collection (COL)

1. It usually bothers me when social media sites ask me for personal information.
2. It usually bothers me when social media sites ask me for my current location information.
3. It bothers me to give personal information to so many people on the social media sites I am registered with.
4. I am concerned that social media sites are collecting too much personal information about me.

Unauthorized Access (UAC)/Information Access (IAC1-4)

1. Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.
2. Social media sites should take more steps to make sure that unauthorized people cannot access personal information in their computers.
3. Databases that contain personal information should be stored in a highly secured location.
4. Social media sites should delete a user's account for illegally accessing other users' personal information.

Errors (ERR)

1. Social media sites should take more steps to make sure that personal information in their files is accurate.
2. Social media sites should have better procedures to correct errors in personal information.
3. Social media sites should devote more time and effort to verifying the accuracy of the personal information in their databases before using it for recommendations.

Secondary Use (SUS)/Information Access (IAC5-7)

1. Social media sites and companies should not use personal information for any purpose unless it has been authorized by the individuals who provide the information.
2. When people give personal information to a social media site for some reason, the social media site should never use the information for any other purpose.
3. Social media sites should never share personal information with other third-party entities unless it has been authorized but the individual who provided the information.

Behavioral Intentions (BIN) [Based on: (Stewart et al. 2002)]

How likely are you, within the next three years to…

1. Provide personal information on social media sites?
2. Make your social media account public for others to find easily?
3. Share information on social media sites with your friends?

About the Author

Babajide Osatuyi is an Assistant Professor of Information Systems at the University of Texas Rio Grande Valley. His research interests revolve around the use of technology for information exchange in areas such as decision support systems, knowledge management systems, social networks, and information and communication technologies. He serves on the review board for Information Systems Journals and Conferences. His research has appeared in journals such as Journal of Computer Information Systems, Computers in Human Behavior, Information Processing and Management, and International Journal of Data Engineering.