
Social media sites privacy concerns: Empirical validation of an instrument

Alex Koohang, Middle Georgia State University, USA, alex.koohang@mga.edu

Abstract

This study attempts to empirically validate a social media sites privacy concerns instrument with six constructs (collection, secondary usage, errors, improper access, control, & awareness). Each construct includes three designated items/variables. Data were collected from 157 participants and analyzed using exploratory factor analysis. The results indicated that all six constructs of the instrument were reliable to measure social media sites privacy concerns of users. Recommendations for future research are provided.

Keywords: Social media privacy concerns, collection, secondary usage, errors, improper access, control, awareness, exploratory factor analysis

Introduction

Social media sites (i.e., social networking sites, media sharing, blogs, micro-blogs, wiki, virtual worlds, location based services, social bookmarking, group buying, writing communities, review sites, & Internet forums) have become increasingly a part of social, professional, and business settings. Social media is being used as a platform for daily communication to share information (Hsu, Park, & Park, 2013) and create user-generated content of many forms (Steenkamp & Hyde-Clarke, 2014). The popularity of social media use is, without a doubt, soaring at an exponential rate. As of January 1, 2017, the top five popular social media sites in terms of estimated unique monthly visitors reported by eBizMBA (2017) were Facebook (1,100,000,000), YouTube (1,000,000,000), Twitter (310,000,000), LinkedIn (255,000,000), and Pinterest (250,000,000).

With the increasing popularity of social media usage, user privacy becomes a vital issue. Literature has documented that users on social media sites, such as the social networking sites, have difficulties in managing their privacy options (Madden, 2012; Madejski, Johnson, & Bellovin, 2012). These difficulties may be due to users' lack of motivation and/or reluctance to control their privacy (Compañó & Lusoli, 2010), users' lack of understanding of social media sites' privacy settings (Liu, Gummadi, Krishnamurthy, & Mislove, 2011) or users' own disclosure of information on social media sites regardless of the privacy settings (Madejski et al., 2012). Nevertheless, many studies have shown that social networking sites users call for complete control of their privacy (e.g., Tang Lin, Hong, Siewiorek, & Sadeh, 2010; Benisch, Kelley, Sadeh, & Cranor, 2011). In addition, Madden (2012) stated that privacy is a primary concern of users on social networking sites. As users become increasingly concerned about their privacy, social media sites have begun to implement various privacy procedures for users to control their information privacy (Karr-Wisniewski, Wilson, & Richter-Lipford, 2011).

Online privacy concerns, particularly, the Internet privacy concerns, have been the focus of many research studies (e.g., Alge, Ballinger, Tangirala, & Oakley, 2006; Chen & Rea, 2004; Harris,

Hoye, & Lievens, 2003; Liu, Marchewka, Lu, & Yu, 2005; Malhotra, Kim, & Agarwal, 2004; Sheehan & Hoy, 2000; Son & Kim, 2008). It is described as "... the degree to which an Internet user is concerned about website practices related to the collection and use of his or her personal information" (Hong & Thong, 2013, p. 276).

The motivation to undertake the present study emerged from a prior research on the Internet privacy concerns by Hong and Thong (2013) where they developed and validated an integrated conceptualization of Internet privacy concerns with six adapted dimensions from prior literature. These privacy dimensions are: 1) collection, 2) secondary usage, 3) errors, 4) improper access, 5) control, and 6) awareness. The definitions for the secondary usage, errors, and improper access dimensions are taken from Malhotra et al. (2004). The definitions for collection, control, and awareness are taken from Smith, Milberg, and Burke (1996) as cited in Hong and Thong (2013). These definitions for each privacy dimension are as follows:

"Collection is the degree to which a person is concerned about the amount of individual-specific data possessed by websites. Secondary usage is the degree to which a person is concerned that personal information is collected by websites for one purpose but is used for another, secondary purpose without authorization from the individual. Errors is the degree to which a person is concerned that protections against deliberate and accidental errors in personal data collected by websites are inadequate. Improper access is the degree to which a person is concerned that personal information held by websites is readily available to people not properly authorized to view or work with the data. Control is the degree to which a person is concerned that he/she does not have adequate control over his/her personal information held by websites. Awareness is the degree to which a person is concerned about his/her awareness of information privacy practices by websites." (Hong & Thong, 2013, pp. 278-279)

In the present study, the above six Internet privacy concern dimensions (collection, secondary usage, errors, improper access, control, & awareness) were adapted to specifically describe the users' privacy concerns on social media sites. Each privacy concern dimension is referred to a construct and defined as follows:

Collection - the amount of specific user data absorbed by the social media sites. The privacy concerns for the *collection* construct are then translated into the following three items/variables:

1. Social media sites asking users to provide information
2. Users thinking twice about providing information
3. Social media sites collecting user information by and large

Secondary usage - personal information collected by the social media sites for one purpose, but used, without authorization/permission from the user, for another secondary purpose. The privacy concerns for the *secondary usage* construct are then translated into the following three items/variables:

1. Social media sites storing user information for their purpose
2. Social media sites storing user information to sell to other companies
3. Social media sites sharing user information without user authorization

Errors - inadequate protections against deliberate and/or accidental errors in user personal data collected by the social media sites. The privacy concerns for the *errors* construct are then translated into the following three items/variables:

1. Social media sites making sure of user information accuracy
2. Social media sites having adequacy of procedures to correct inaccurate user information
3. Social media sites spending time and effort to verify user information accuracy

Improper access - personal information held by the social media sites that is readily available to others and/or not properly authorized to be viewed or accessed by others. The privacy concerns for the *improper access* construct are then translated into the following three items/variables:

1. Social media sites protect users from unauthorized access
2. Social media sites devote time and effort to prevent unauthorized access to user accounts
3. Social media sites take steps to prevent unauthorized access to user accounts

Control - inadequate control over personal information held by the social media sites. The privacy concerns for the *control* construct are then translated into the following three items/variables:

1. Users having control over what information they provide to social media sites
2. Users having control over decision of how their information will be used by social media sites
3. Lost or reduced control by users because information is used by social media sites for marketing transaction with others

Awareness - not being made aware of information privacy practices by the social media site. The privacy concerns for the *awareness* construct are then translated into the following three items/variables:

1. Users not being aware of policies set forward by social media sites
2. Users not being aware of how their information is used by social media sites
3. Users not being aware of how their information is collected, processed, and used by social media sites

Purpose of the Study

The purpose of this study was to empirically validate an instrument with six constructs/components (collection, secondary usage, errors, improper access, control, & awareness) that measures users' privacy concerns on social media sites. Each construct/component has three designated items describing the construct/component. The following research question, therefore, emerged from the study's purpose:

RQ1: Are the six social media privacy construct/components (collection, secondary usage, errors, improper access, control, & awareness) of the instrument empirically validated to be reliable and interpretable among their designated items?

Methodology

Instrument

The instrument used for the present study is adapted from Hong and Thong (2013), where they investigated the different conceptualizations of Internet privacy concerns (collection, secondary usage, errors, improper access, control, & awareness) using four online surveys focusing on user's concerns for website behavior rather than user's expectation of website behavior and adopted uniform view in the wording of the items for enhancing the validity of the instrument.

The adapted instrument for the present study focuses specifically on social media privacy concerns with six constructs: collection, secondary usage, errors, improper access, control, and awareness. The adapted instrument only reflects social media privacy concerns, specifically replacing "commercial/government websites" with "social media sites" and minor tweaking of some items. The instrument consists of 18 items (three items per construct). The instrument items were stated as follows:

Social media privacy concerns (Collection) Construct

1. It bothers me when social media sites ask me to provide personal information.
2. When social media sites ask me for personal information, I sometimes think twice before providing it.
3. I am concerned that social media sites are collecting personal information about me.

Social media privacy concerns (Secondary Usage) Construct

4. I am concerned that social media sites would use my stored personal information for their own advantage/profit.
5. I am concerned that social media sites would sell my stored personal information in their databases to other companies.
6. I am concerned that social media sites would share my stored personal information in their databases with other companies without my authorization.

Social media privacy concerns (Errors) Construct

7. I am concerned that social media sites do not take enough steps to make sure that my personal information in their files is accurate.
8. I am concerned that social media sites do not have adequate procedures to correct errors in my personal information.
9. I am concerned that social media sites do not devote enough time and effort to verifying the accuracy of my personal information in their databases.

Social media privacy concerns (Improper Access) Construct

10. I am concerned that social media site databases that contain my personal information are not protected from unauthorized access.
11. I am concerned that social media sites do not devote enough time and effort to preventing unauthorized access to my personal information.
12. I am concerned that social media sites do not take enough steps to make sure that unauthorized people cannot access my personal information on their computers.

Social media privacy concerns (Control) Construct

- 13. It usually bothers me when I do not have control of personal information that I provide to social media sites.
- 14. It usually bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by social media sites.
- 15. I am concerned when control of my personal information on a social media site is lost or unwillingly reduced because of marketing transactions with other companies.

Social media privacy concerns (Awareness) Construct

- 16. I am concerned when a clear and visible disclosure is missing in online privacy policies of social media sites.
- 17. It usually bothers me when I am not aware or knowledgeable about how my personal information will be used by social media sites.
- 18. It usually bothers me when social media sites seeking my information online do not disclose the way the data are collected, processed, and used.

A Likert-type scale was used with the following scoring strategy: 7 = completely agree, 6 = mostly agree, 5 = somewhat agree, 4 = neither agree nor disagree, 3 = somewhat disagree, 2 = mostly disagree, 1 = completely disagree.

Sample and Data Collection

The participants for this study (N = 157) were undergraduate students who were studying at a medium-sized university in the Southeast, USA. The participants were female and male students who were enrolled in various general studies and information technology courses. Data were collected electronically via SurveyMonkey™, an Internet survey site. At the time of this study, 165 surveys were collected. Of the 165, six surveys were eliminated because of incomplete data, two were eliminated after the outlier test performed by SPSS™ version 24. This yielded a total of 157 usable records for this study. See demographics of the participants in Table 1.

Table 1: Demographics (N = 157)

	N	%		N	%
# of SNS sites use			Age		
Facebook	145	92	18 - 20	56	36
Instagram	114	73	21 - 29	66	42
Snapchat	107	68	30 - 39	21	13
Pinterest	101	64	40 or older	14	9
Twitter	78	50	Gender		
LinkedIn	53	22	Female	86	55
Google Plus+	53	34	Male	71	45
Tumblr	35	22			
Vine	31	20			
Reddit	11	7			
Flickr	5	3			

Data Analyses

Collected data were analyzed through conducting exploratory factor analysis using Principal Component Analysis (PCA) via SPSS™ version 24. Exploratory factor analysis describes the underlying structure that explains a set of variables with shared variability (Mertler & Vannatta, 2010). The analysis includes the following:

- 1) Kaiser-Meyer-Olkin (KMO) and Bartlett's test of sphericity to test for multivariate normality and sampling adequacy. The accepted index for KMO should be greater than 0.6. The Bartlett's test of sphericity should be less than .05 (Cerny & Kaiser, 1977).
- 2) Eigenvalues (Kaiser Criterion) test retains factors with eigenvalues greater than 1 as common factors showing the initial eigenvalues, extraction sums of squared loadings, and rotation sums of squared loadings. According to Mertler and Vannatta (2010), the Kaiser criterion is reliable when a) the number of records is equal or greater than 150, b) there are less than 30 variables, and c) the values of communalities are high - normally close to .70.
- 3) Test of variance explained that shows variance-retain components. All components retained should collectively account for at least 70% of total variability.
- 4) The Scree Plot test, a graphical representation of the eigenvalues that uses Principal Component Analysis. It detects all components within the breakpoint where the curve flattens (before eigenvalues level off). According to Mertler and Vannatta (2010), this test is reliable when the number of subjects is less than 250 and communalities are greater than .30.

Once the results of the tests from 1 to 4 above are shown to be favorable, analysis moves to include PCA with Varimax rotation to answer the research question. This procedure forces the number of components, with their designated items, to be retained. Varimax rotation is a preferred and most commonly used method. Mertler and Vannatta (2010) stated that this method "... minimizes factor complexity by maximizing variance for each factor" (p. 253). Finally, the reliability test (Cronbach's Alpha) is conducted to determine the internal consistency among the factors for each component. A reliability coefficient of .70 or higher is considered acceptable.

Results

Before conducting the exploratory factor analysis, multivariate outlier analysis on data was conducted to eliminate (if any) unusual or extreme values at one or both ends of the data distribution. Two cases were found to have unusual or extreme multivariate outlier. These cases were removed before conducting the exploratory factor analysis. This yielded a final sample of 157 usable records for inclusion in the analyses.

KMO and Bartlett's Test of Sphericity

KMO measure of sampling adequacy and Bartlett's test of sphericity tests were conducted to determine multivariate normality and sampling adequacy. The results for KMO was .868 that is well above the .6 acceptance level. The Bartlett's test of sphericity results (Chi-Squared = 2213.672, df = 153, & $p < .0001$) indicated an acceptable multivariate normality and sampling adequacy (See Table 2).

Table 2: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.868
Bartlett's Test of Sphericity	Approx. Chi-Square	2213.672
	df	153
	Sig.	.000

Eigenvalues (Kaiser Criterion)

Kaiser criterion is reliable when 1) the number of records is equal or greater than 150, 2) there are less than 30 variables or factors, and 3) the values of communalities are high. All the three criteria were met. The number of records was above 150. There were 18 items overall. The results of communalities as shown in Table 3 revealed high values for all 18 items.

Table 3: Communalities

Social Media Privacy Concerns	Items / Variables	Initial	Extraction
Collection	CL1	1.000	.794
	CL2	1.000	.750
	CL3	1.000	.688
Secondary Usage	SU1	1.000	.831
	SU2	1.000	.884
	SU3	1.000	.851
Errors	ER1	1.000	.865
	ER2	1.000	.932
	ER3	1.000	.892
Improper Access	IA1	1.000	.801
	IA2	1.000	.861
	IA3	1.000	.832
Control	CO1	1.000	.829
	CO2	1.000	.875
	CO3	1.000	.840
Awareness	AW1	1.000	.804
	AW2	1.000	.840
	AW3	1.000	.874

Variance Explained

Table 4 shows the variance explained for the six retained components including the initial eigenvalues, the extraction sums of squared loadings, and the rotation sums of squared loadings. The total variance-retained accounted for 83.58%, which is well above the acceptable 70% of total variability.

Table 4: Total Variance Explained

Component	Initial Eigenvalues		
	Total	% of Variance	Cumulative %
1	8.052	44.736	44.736
2	2.306	12.813	57.549
3	1.490	8.279	65.828
4	1.261	7.003	72.832
5	1.141	6.339	79.170
6	.793	4.406	83.577
Component	Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %
1	2.761	15.338	15.338
2	2.655	14.751	30.089
3	2.603	14.461	44.550
4	2.598	14.435	58.985
5	2.258	12.546	71.531
6	2.168	12.046	83.577
<i>Note: Total % of Variance explained for all 6 Components = 83.577</i>			

Extraction Method: Principal Component Analysis (PCA)

Testing the Scree Plot

Figure 1 shows the Scree Plot, a graphical representation of the eigenvalues that uses PCA. It detects six components within the breakpoint where the curve flattens or before eigenvalues level off.

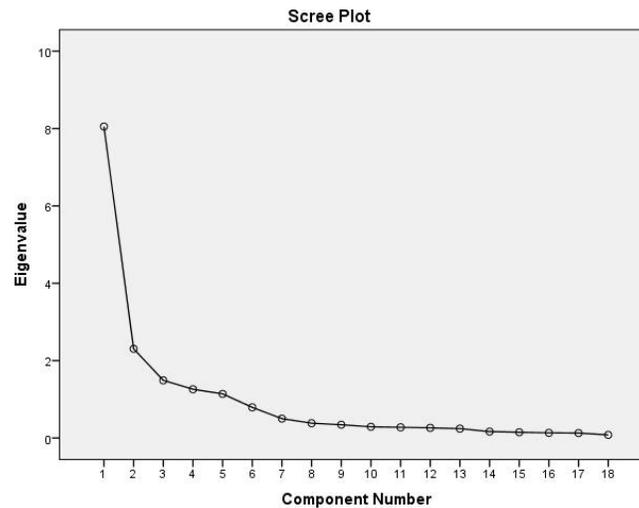


Figure 1: Scree Plot Test

Principal Component Analysis with Varimax Rotation

Table 5 shows the principal component analysis with Varimax rotation. As can be seen, component 6 retained items 1, 2, and 3 with high loading and no high cross loading on any of the other five components. This component represented *social media privacy concerns (collection)*. Component 1 retained items 4, 5, and 6 with high loading and no high cross loading on any of the other five components. This component represented *social media privacy concerns (secondary usage)*. Component 5 retained items 7, 8, and 9 with high loading and no high cross loading on any of the other five components. This component represented *social media privacy concerns (errors)*. Component 2 retained items 10, 11, and 12 with high loading and no high cross loading on any of the other five components. This component represented *social media privacy concerns (improper access)*. Component 3 retained items 13, 14, and 15 with high loading and no high cross loading on any of the other five components. This component represented *social media privacy concerns (control)*. Component 4 retained items 16, 17, and 18 with high loading and no high cross loading on any of the other five components. This component represented *social media privacy concerns (awareness)*.

Reliability Test (Cronbach's Alpha)

The alpha coefficient for the three items of the collection component was .80, suggesting that the items have relatively high internal consistency. The alpha coefficient for the three items of the secondary usage component was .91, suggesting that the items have relatively high internal consistency. The alpha coefficient for the three items of the errors component was .94, suggesting that the items have relatively high internal consistency. The alpha coefficient for the three items of the improper access component was .90, suggesting that the items have relatively high internal consistency. The alpha coefficient for the three items of the control component was .90, suggesting that the items have relatively high internal consistency. The alpha coefficient for the three items of the awareness component was .90, suggesting that the items have relatively high internal consistency. Table 5 shows the Cronbach's alpha, and % variance explained for all six components.

Table 5: Rotated Component Matrix

Social Media Privacy Concerns	Items / Variables	Component					
		1	2	3	4	5	6
Collection	CL1	.168	.157	-.125	.173	.142	.822
	CL2	.001	.080	-.047	.109	.154	.840
	CL3	.213	.366	-.133	.264	.123	.637
Secondary Usage	SU1	.842	.212	-.017	.065	.236	.129
	SU2	.884	.178	-.015	.209	.145	.076
	SU3	.848	.097	.005	.227	.245	.102
Errors	ER1	.336	.272	-.163	.124	.750	.273
	ER2	.314	.310	-.187	.237	.787	.162
	ER3	.257	.279	-.167	.281	.783	.168
Improper Access	IA1	.176	.826	-.111	.120	.218	.120
	IA2	.166	.819	-.136	.233	.212	.212
	IA3	.174	.799	-.124	.256	.228	.174
Control	CO1	.079	-.121	.864	-.190	-.127	-.101
	CO2	.015	-.089	.912	-.048	-.123	-.133
	CO3	-.126	-.103	.895	-.077	-.081	-.021
Awareness	AW1	.150	.266	-.182	.766	.212	.212
	AW2	.172	.132	-.084	.869	.138	.111
	AW3	.194	.207	-.110	.846	.149	.207
<i>Cronbach's alpha</i>		0.91	0.90	0.90	0.90	0.94	0.80
<i>% Variance Explained</i>		14.75	14.44	12.55	12.05	14.46	15.34

Extraction Method: Principal Component Analysis | Rotation Method: Varimax with Kaiser Normalization | Rotation converged in six iterations

Conclusion

This study was undertaken to empirically validate a social media privacy concerns instrument with six constructs/components (collection, secondary usage, errors, improper access, control, & awareness). The instrument is based on a previous study on the Internet privacy concerns (Hong & Thong, 2013) and adapted specifically to measure users' social media sites privacy concerns. Each construct/component included three designated items describing the construct/component. The research question asked whether the six social media sites privacy concerns construct (each separately) can be empirically validated to be reliable and interpretable among their designated items. The findings indicated the following:

The *social media privacy concerns (collection)* component retained all its three designated items indicating that the component was empirically validated to be reliable and interpretable among all its three items. The items retained are concerns about 1) social media sites asking users to

provide information, 2) users thinking twice about providing information, and 3) social media sites collecting user information by and large.

The *social media privacy concerns (secondary usage)* component retained all its three designated items indicating that the component was empirically validated to be reliable and interpretable among all its three items. The items retained are concerns about 1) social media sites storing user information for their purpose, 2) social media sites storing user information to sell to other companies, 3) social media sites sharing user information without user authorization.

The *social media privacy concerns (errors)* component retained all its three designated items indicating that the component was empirically validated to be reliable and interpretable among all its three items. The items retained are concerns about 1) social media sites making sure of user information accuracy, 2) social media sites having adequacy of procedures to correct inaccurate user information, and 3) social media sites spending time and effort to verify user information accuracy.

The *social media privacy concerns (improper access)* component retained all its three designated items indicating that the component was empirically validated to be reliable and interpretable among all its three items. The items retained are concerns about 1) social media sites protect users from unauthorized access, 2) social media sites devote time and effort to prevent unauthorized access to user accounts, and 3) social media sites take steps to prevent unauthorized access to user accounts.

The *social media privacy concerns (control)* component retained all its three designated items indicating that the component was empirically validated to be reliable and interpretable among all its three items. The items retained are concerns about 1) users having control over what information they provide to social media sites, 2) users having control over the decision of how their info will be used by social media sites, and 3) lost or reduced control by users because of social media sites marketing transaction with others.

The *social media privacy concerns (awareness)* component retained all its three designated items indicating that the component was empirically validated to be reliable and interpretable among all its three items. The items retained are concerns about 1) users not being aware of policies set forward by social media sites, 2) users not being aware of how their information is used by social media sites, and 3) users not being aware of how their data are collected, processed, and used by social media sites.

In summary, all six constructs of the instrument (collection, secondary usage, errors, improper access, control, and awareness) were found to be reliable to measure social media privacy concerns of users. The findings of this research contribute to improved knowledge about measuring users' perception toward privacy concerns on social media sites. Furthermore, this research corroborates previous research by Hong and Thong (2013) documenting that the enhanced validity of an instrument depends upon the focus that is given to user's concern for website behavior rather than user's expectation of website behavior; and the use of uniform view in the wording of the items of the instrument. This study was limited to a sample of convenience from one higher education institution in the southeast, USA. To enhance the generalizability of the findings, future studies should focus on larger sample population from diverse institutions

and/or organizations. Further research should also consider inclusion of possible emerging users' privacy concerns dimensions/constructs on the social media sites.

References

- Alge, B. J., Ballinger, G. A., Tangirala, S., & Oakley, J. L. (2006). Information privacy in organizations: empowering creative and extra-role performance. *Journal of applied psychology, 91*(1), 221.
- Benisch, M., Kelley, P. G., Sadeh, N., & Cranor, L. F. (2011). Capturing location-privacy preferences: quantifying accuracy and user-burden tradeoffs. *Personal and Ubiquitous Computing, 15*(7), 679-694.
- Cerny, C. A., & Kaiser, H. F. (1977). A study of a measure of sampling adequacy for factor-analytic correlation matrices. *Multivariate Behavioral Research, 12*(1), 43-47.
- Chen, K., & Rea Jr, A. I. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information Systems, 44*(4), 85-92.
- Compañó, R., & Lusoli, W. (2010). The policy maker's anguish: Regulating personal data behavior between paradoxes and dilemmas. In *Economics of information security and privacy*, 169-185.
- eBizMBA (2017). Top 15 most popular social networking sites. Retrieved January 05, 2017 from <http://www.ebizmba.com/articles/social-networking-websites>
- Harris, M. M., Hoye, G. V., & Lievens, F. (2003). Privacy and attitudes towards internet-based selection systems: A cross-cultural comparison. *International Journal of Selection and Assessment, 11*(2-3), 230-236.
- Hong, W., & Thong, J. Y. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly, 37*(1), 275-298.
- Hsu, C. L., Park, S. J., & Park, H. W. (2013). Political discourse among key Twitter users: the case of Sejong city in South Korea. *Journal of Contemporary Eastern Asia, 12*(1), 65-79.
- Karr-Wisniewski, P., Wilson, D., & Richter-Lipford, H. (2011). A new social order: Mechanisms for social network site boundary regulation. In *Proceedings of the Americas Conference on Information Systems*, (p. 9).
- Liu, C., Marchewka, J. T., Lu, J., & Yu, C. S. (2005). Beyond concern - a privacy-trust-behavioral intention model of electronic commerce. *Information & Management, 42*(2), 289-304.
- Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011, November). Analyzing facebook privacy settings: user expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, 61-70.
- Madden, M. (2012). Privacy management on social media sites. *Pew Internet Report*, 1-20.

- Madejski, M., Johnson, M., & Bellovin, S. M. (2012). A study of privacy settings errors in an online social network. In *Proceedings of Pervasive Computing and Communications Workshops*, 340-345.
- 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.
- Mertler, C. & Vannatta, R. (2010). *Advanced and multivariate statistical methods: Practical application and interpretation, (4th Edition)*. Glendale, CA: Pyrczak Publishing
- Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of public policy & marketing*, 19(1), 62-73.
- 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 and a nomological model. *MIS Quarterly*, 32(3), 503-529.
- SteenKamp, M., & Hyde-Clarke, N. (2014). The use of Facebook for political commentary in South Africa. *Telematics and Informatics*, 31(1), 91-97.
- Tang, K. P., Lin, J., Hong, J. I., Siewiorek, D. P., & Sadeh, N. (2010). Rethinking location sharing: exploring the implications of social-driven vs. purpose-driven location sharing. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*, 85-94.

Author's Biography

Alex Koohang is Professor and Dean in the School of Information Technology at Middle Georgia University. He has published and presented numerous papers. Currently, he is the editor-in-chief of the *Journal of Computer Information Systems* and serves on the editorial review board of several IS/MIS publications. Dr. Koohang is the Peyton Anderson Eminent Scholar and Endowed Chair in Information Technology.