Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume7, Issue 1, 2019

Social media privacy concerns and risk beliefs

Johnathan Yerby, Middle Georgia State University, USA, johnathan.yerby@mga.edu

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

Joanna Paliszkiewicz, Warsaw University of Life Sciences, Poland, joanna_paliszkiewicz@sggw.pl

Abstract

The purpose of this study was to investigate the link between users' risk beliefs and social media privacy concerns (concerns users express regarding social media sites' practices as to how they collect and use personal information). A Likert-type instrument with seven constructs, six of which described the social media privacy concerns and the seventh construct defined users' risk beliefs, was used to collect data from students who were studying at a university in the southeastern United States. All students (N = 138) used Facebook as their major social networking site. Collected data were analyzed via multiple regression analysis. The results indicated that subjects' risk beliefs are influenced by three social media privacy concerns (i.e., collection, error, and awareness). The Findings and their implications are discussed. Recommendations for future research are made.

Keywords: Risk beliefs, social media, privacy concerns, Facebook.

Introduction

A decade ago, people used social media to keep in touch with their friends. Today, social media is more pervasive in many people's lives and has transformed from merely a tool to share a comment or photo, a news source, a journal of lives, a means to conduct business, organize people for social causes, a marketing machine, and a distraction from reality. A Pew Research study found that 79% of adults in America use social media (Greenwood, Perrin, & Duggan 2016). Over the past two years, the active social media users worldwide increased 21%, to 2.789 billion users, with 599 million users coming from the Americas (Kemp, 2017).

Adoption and diffusion of social media show no signs of slowing down, at the same time, there are growing concerns about privacy and risk on these platforms where people are sharing intimate details about their lives (Madden, 2012). Madden (2012) reported that there is a major disconnect in peoples' attitudes and practices regarding privacy. People say that privacy is important, but when observed, their actions do not prioritize privacy (Madden, 2012).

The literature has documented that privacy concerns are restraining to the Internet users (e.g., Bansal & Gefen, 2010; Gerrard, Cunningham, & Devlin, 2006; Zhou, 2011) and various methods have been suggested to lessen privacy concerns (Bartsch & Dienlin, 2016; Dinev & Hart, 2004).

Online privacy concerns have been researched in many different topics, for example, consumer willingness to provide personal information (Phelps, Nowak, & Ferrell, 2000); shopper attitude (Inman & Nikolova, 2017); downloading mobile apps (Gu, Xu, Xu, Zhang, & Ling, 2017); location-based apps (Wang & Lin, 2017); privacy protection behaviors (Chen, Beaudoin, & Hong, 2017); self-disclosure across societies (Liang, Shen, & Fu, 2017); customer and firm performance (Martin, Borah, & Palmatier, 2017); individual characteristics (Taddicken, 2014); cultural and generational influences (Miltgen & Peyrat-Guillard, 2014); as well as photo sharing (Liang, Liu, Lu, & Wong, 2015).

Privacy concerns are “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). Social media is increasingly ubiquitous on people’s mobile phone, tablets, and computers. There is a debate among experts within the field of social media about privacy. Experts in the social media privacy question whether privacy is a relic of the past or if there are settings, tools, methods, and education that can allow privacy to coexist with social sharing (Madden, 2012). Social media users frequently lack the technical ability to understand how their information is collected, stored, and then repackaged to be sold (Rauhofer, 2008).

In their extensive research, Hong and Thong (2013) outlined six dimensions of the Internet privacy concerns based on previous research. These dimensions are collection, secondary usage, errors, improper access, control, and awareness. Koohang (2017) adapted the six dimensions of the Internet privacy concern to distinctly describe the users’ social media sites privacy concerns (SMPC) as listed below.

> “Collection - the amount of specific user data absorbed by the social media sites.
> Secondary usage – [users’] personal information collected by the social media sites for one purpose, but used, without authorization/permission from the user, for another secondary purpose.
> Errors - inadequate protections against deliberate and/or accidental errors in user personal data collected by the social media sites.
> Improper access - [users’] 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.
> Control - inadequate control over personal information held by the social media sites.
> Awareness - [users are] not being made aware of information privacy practices by the social media sites.” (Koohang, 2017, p. 17)

Literature has documented the role of users’ risk beliefs and their online privacy concerns (Dinev & Hart, 2006; Youn, 2009). Some studies have shown risk as a predictor of online privacy concerns (Dinev & Hart, 2006; Cocosila, Archer, & Yuan, 2009). Dinev and Hart (2006) stated that as perceived privacy risk increased, so did privacy concerns which in turn decreased users’ willingness to provide personal information. Metzger (2007) asserted that disclosing personal information online involves a degree of risk in such a way that if the user has a high privacy concern, he or she will find it risky to disclose his or her personal information. Culnan and Bies

(2003) argued that people are readily willing to accept the loss of privacy if they perceive a positive outcome or benefit. This assertion may also be valid with social media privacy concerns (SMPC). The purpose of the present study is, therefore, to examine the link between social media privacy concerns and users' risk beliefs. Consistent with its purpose, the following research question is asked:

Which of the six predictor variables (SMPC: collection, SMPC: secondary usage, SMPC: error, SMPC: improper access, SMPC: control, SMPC: awareness) are most influential in predicting users' risk beliefs?

Risk beliefs on social media are referred to

> "the degree to which a user on a social media site risks disclosing his or her personal information. Risk on a social media site entails potential for loss of personal information, uncertainty about how personal information may be used, and unexpected problems associated with disclosing user's personal information." (Koohang, Paliszkiewicz, & Goluchowski, 2018a, p. 1210)

Methodology

Instrument

The seven-point Likert type instrument used for this study is comprised of seven constructs. Six of the seven constructs (i.e., collection, secondary usage, errors, improper access, control, & awareness) describe the social media privacy concerns. These constructs were developed and empirically validated by Koohang (2017), based on an extensive study researching the Internet privacy concerns by (Hong & Thong, 2013). The seventh construct describes risk beliefs (i.e., revealing personal information that may be subjected to possible loss; the doubt of how the information is used; and the probable unforeseen problems that may bring harm to users) taken from Hong and Thong (2013) and modified by Koohang et al. (2018a) to specifically reflect social media risk beliefs. The instrument's scale entails the following: 7 = completely agree, 6 = mostly agree, 5 = somewhat agree, 4 = neither agree nor disagree, 3 = somewhat disagree, 2 = mostly disagree, 1 = completely disagree (See Appendix A).

Sample and Data Collection

Upon approval from the university's Institutional Research Board (IRB) where this study took place, we administered the survey instrument electronically to approximately 600 undergraduate students. The students were majoring in the field of Information Technology at a university in the southeastern United States. Students were asked to complete the survey only if they used Facebook as their major social networking website. We received 142 completed surveys. Of the 142, four were eliminated because of incomplete data, yielding a final sample of 138. The participants were male (N = 79, 57%) and female (N = 59, 43%). Their age categories were 18 –

20 (N = 48, 35%), 21 – 29 (N = 60, 43%), 30 – 39 (N = 19, 14%), and 40 or older (N = 11, 8%). Participants were told that their participation was completely voluntary, and their responses would be kept confidential.

Data Analysis

SPSS™ version 25 was used to analyze the data. We used multiple regression analysis to answer the research question. The independent variables (IVs) were IV_1 = SMPC: collection, IV_2 = SMPC: secondary usage, IV_3 = SMPC: error, IV_4 = SMPC: improper access, IV_5 = SMPC: control, IV_6 = SMPC: awareness. The dependent variable (DV) was DV = risk beliefs. We applied the *Enter* method to include all independent variables into the model at the same time irrespective of significant contribution. The analysis shows which of the independent variables can best predict the dependent variable. The multiple regression includes a test of multicollinearity, model fit determination, a test of Analysis of Variance (ANOVA), and the path coefficients showing the beta weights, t and *p* values for the IVs (Mertler & Reinhart, 2016).

Results

The regression model's tolerance level and Variance Inflation Factor (VIF) for all IVs were SMPC: collection (.525, 1.906), SMPC: secondary usage (.377, 2.649), SMPC: errors (.496, 2.015), SMPC: improper access (.320, 3.125), SMPC: control (.368, 2.715), and SMPC: awareness (.481, 2.079). These results indicate that the tolerance level for each IV yielded a value below the threshold value of 0.1, and the VIF values for all IVs were below the threshold value of 10. These results indicated that multicollinearity among the IVs did not exist, and the analysis proceeded to interpret path coefficients.

The model fit was calculated to determine how well the IVs predicted the DV. The model fit includes the R, R^2, R^2_{adj} and the ANOVA (i.e., F statistics & *p* value). The results of multiple correlation (R = 0.62), squared multiple correlation ($R^2 = 0.38$), and the adjusted squared multiple correlation ($R^2_{adj} = 0.35$) were robust enough to indicate that the six IVs could reasonably predict the dependent variable (DV = risk beliefs). The F statistics ($F = 13.551$, $p < 0.001$) from the ANOVA indicated that the relationship between the DV and the IVs was linear and positive.

The path coefficients were interpreted to determine the predictor variables (the six independent variables) that are most influential in predicting the dependent variable. Table 1 shows the coefficients table of the multiple regression model. From the six IVs, as shown in Table 1, the significant SMPC variables that are most influential in predicting the users' risk beliefs are SMPC: collection, SMPC: error, and SMPC: awareness. Tables 2 and 3 show correlations and descriptive statistics.

Table 1. Coefficients Table of the Multiple Regression Model (N=138)

Model	***Unstandardized Coefficients***		***Standardized Coefficients***	**t**	**Sig.**
	B	***Standard Error***	**Beta**		
(Constant)	.303	.586		.517	.606
COL	.394	.123	.302	3.190	***.002*** **
SEC	-.116	.101	-.128	-1.143	.255
ERR	.208	.087	.233	2.388	***.018*** *
ACC	.126	.118	.129	1.067	.288
CON	-.007	.123	-.007	-.060	.952
AWE	.231	.107	.213	2.156	***.033*** *

*** $p<0.001$, ** $p<0.01$, * $p<0.05$

Note: COL = SMPC: collection, SEC = SMPC: secondary usage, ERR = SMPC: errors, ACC = SMPC: improper access, CON = SMPC: control, AWE = SMPC: awareness

Table 2. Correlations (N=138)

	RISK	**COL**	**SEC**	**ERR**	**ACC**	**CON**	**AWE**
RISK	1.000	.483	.336	.471	.509	.388	.502
COL	.483	1.000	.588	.365	.574	.630	.471
SEC	.336	.588	1.000	.519	.656	.691	.399
ERR	.471	.365	.519	1.000	.678	.386	.511
ACC	.509	.574	.656	.678	1.000	.609	.638
CON	.388	.630	.691	.386	.609	1.000	.580
AWE	.502	.471	.399	.511	.638	.580	1.000

Note: RISK = risk beliefs, COL = SMPC: collection, SEC = SMPC: secondary usage, ERR = SMPC: errors, ACC = SMPC: improper access, CON = SMPC: control, AWE = SMPC: awareness

Table 3. Descriptive Statistics (N=138)

	Mean	**Std. Deviation**
RISK	5.0761	1.21638
COL	5.8889	0.93446
SEC	5.6763	1.34118
ERR	5.1377	1.36027
ACC	5.6908	1.25347
CON	5.9710	1.11502
AWE	5.9469	1.12355

Note: RISK = risk beliefs, COL = SMPC: collection, SEC = SMPC: secondary usage, ERR = SMPC: errors, ACC = SMPC: improper access, CON = SMPC: control, AWE = SMPC: awareness

Discussion

This study was carried out to examine which of the six social media privacy concerns (SMPCs) were most influential in predicting users' risk beliefs. An instrument consisting of seven constructs (six SMPCs & one risk beliefs) was administered electronically to subjects from a university in the southeast region of the USA. All subjects used Facebook as their main social media platform to communicate and share information. Collected data were analyzed using multiple regression analysis.

The findings showed the absence of multicollinearity among the independent variables (COL = SMPC: collection, SEC = SMPC: secondary usage, ERR = SMPC: errors, ACC = SMPC: improper access, CON = SMPC: control, AWE = SMPC: awareness) signifying the strength of the regression analysis model. Next, the model fit was established, and it showed that the independent variables adequately predict the dependent variable (risk beliefs). Furthermore, the test of ANOVA indicated a linear relationship between all the independent variables and the dependent variable. Finally, the path coefficients were interpreted to establish the predictor variables (the six SMPCs) that were most influential in predicting the dependent variable of risk beliefs. The findings showed that SMPC: collection, SMPC: error, and SMPC: awareness were significant variables and that they are most influential in predicting users' risk beliefs.

Users, in general, find it risky to disclose their personal information because 1) the amount of personal information collected by the social media; 2) the offering of inadequate protection of their personal information by the social media against deliberate and/or accidental errors; and 3) lack of awareness of information privacy practices by the social media sites. The SMPC: collection focuses on the amount of specific user data collected. Zheleva (2011) described the idea of differential privacy in an experiment where he created an open network and monitored people's risk beliefs. Differential privacy essentially found that some users were willing to give up a little privacy alongside with several other users. In the case of the present research, perhaps participants are willing to share some information if everyone else is doing the same. Therefore, they would be averse to simply revealing information that may cause their privacy to be easily violated.

The findings for the SMPC: improper access indicated that this variable was not a significant predictor of risk beliefs. However, the SMPC: errors and the SMPC: awareness were significant predictors of risk beliefs. One way to interpret these results is that the respondents may have felt comfortable in being able to configure access to the information that they share. However, they were concerned about exploits or accidents. Social media sites have proven to be penetrable to override access controls, for example, Li et al., (2015) found seven exploits that worked on multiple social networks. The attacks included errors made by social media platforms, errors made by shared connections among users, and errors made when setting, tagging or sharing information. Interestingly, a survey of 1,520 people in the United States showed that only 5.2% of people using social media think that their accounts are safe from hackers (Newton, 2017). An important issue to highlight regarding SMPC: improper access not being a significant predictor of risk beliefs may be the timing of this study. The present study on users' social media privacy concerns was conducted a few months before the New York Times reported that Cambridge Analytica, a data mining/analytics company, was harvesting and misusing data from millions of Facebook users (Granville, 2018). Following the breaking into the Cambridge Analytica story, the Federal Trade Commission opened an investigation on Facebook and Cambridge Analytica. Since March 2018, people have learned that the data collection was not a data breach, rather a data collection and permissions issue. Cambridge Analytica was collecting data with consent on an estimated 87 million people (Meyer, 2018). A #DeleteFacebook campaign followed where millions of users vowed to get rid of their Facebook accounts, however, according to CEO Mark Zuckerberg, the follow-through on leaving the social lifeline was not a meaningful number (Leswing, 2018). In a survey of 1000 Americans, 76% were aware of the Cambridge Analytica scandal; 17% deleted the Facebook application from their phone, and 9% reported that they had deleted their account completely (Leswing, 2018). If this study were conducted at the time of the Cambridge Analytica/Facebook story, the results of SMPC: improper access might likely be a significant predictor of risk beliefs.

Shore and Steinman (2015) stated that the privacy policy is less transparent, harder to understand, and contains fewer options to control data and third-party access. Social media sites such as Facebook change privacy settings frequently, contradict policies in short time frames, and generally seesaw between keeping users informed about privacy and changing the settings without consent or knowledge (Fox, 2016). These frequent changes in privacy policy may be translated into users' risk behavior that is predicted by their awareness of the conditions that their information is subjected to.

Because technology moves quickly, and people's attention is drawn in many directions, there may be limitations on how intensely or how long people focus on most things. Because of the recent privacy issues with Facebook (Granville, 2018), Facebook users may attempt to be more aware of their privacy, which may change some of their behaviors on the social media platform. However, it is not clear how lasting or meaningful the changes will be for each individual. Perhaps, differential privacy as described by Zheleva (2011) and time have a way of slowly bringing users' guards down, and they return to sharing personal and intimate details of their lives on social media sites.

The findings of this study have implication for practice. First, Koohang, Paliszkiewicz, and Nord (2018b) suggested that social media sites should adopt the concept of *privacy by design* advanced by Cavoukian (2010) to protect user privacy. The concept of privacy by design includes seven principles. They are "1) proactive not reactive - preventative not remedial 2) privacy as the default, 3) privacy embedded into design, 4) full functionality – positive-sum, not zero-sum, 5) end-to-end lifecycle protection, 6) visibility and transparency, and 7) respect for user privacy" (Cavoukian, 2010, para. 18). We assert that to protect user privacy, social media sites should go beyond merely adopting these privacy principles. They must embed the *privacy by design* principles into their platforms to protect users' privacy and pledge to use various sound strategies that include users' safety and well-being. Implementing the concept of *privacy by design* into the social media sites may lessen users' risk beliefs, therefore, decreasing their privacy concerns.

Second, Trepte et al. (2015) suggested that users' privacy skills are important in protecting personal information. Other studies have asserted that privacy skills must be considered as an important part of any online activities (Bartsch & Dienlin, 2016; Dinev & Hart, 2004; Park & Jang, 2014). Therefore, we assert that that privacy skills can be provided by social media sites through privacy awareness training. The privacy awareness training should include the awareness of:

- necessary skills, knowledge, and competencies about privacy issues (i.e., issues such as identity theft, hacking, web-based information brokers, and tracking apps) and their negative consequences;
- users' responsibilities to ensure privacy protection of their personal information on social media sites;
- privacy compliance strategies to constantly protect, secure, safeguard, and enhance user privacy on social media;
- how personal information is collected, used, and shared with others; and
- how privacy settings on a social media site are controlled.

In addition, the privacy awareness training must include users' awareness of best practices to keep safe on social media sites. Some examples of these best practices are regular managing of privacy settings, limiting the amount of personal information users disclose, limiting details about work history, verifying who users connect to, and using a strong password and changing passwords routinely.

Conclusion

The social media privacy concerns are real and the outcomes of failing to protect personal information can be critical and risky. Therefore, measures must be taken by social media sites to ensure users' privacy protection. Social media sites should develop and include tools that assist their users to understand privacy and its importance to their daily lives. The seriousness of the privacy breach must be communicated with users. Furthermore, a privacy awareness education must be adopted and embedded as a required part of joining a social media site. This study has limitations that may influence the generalizability of the results. These limitations include a self-reported survey, a sample of convenience, an uneven age category and limited geographical location for collection of data. The population sample was from students majoring in the information technology field, which may not be generalizable to other population samples. Another limitation of this study is the unevenness of the age category among subjects in which 78% were between 18 – 29 years old. Future studies should be mindful of these limitations. Future research should also consider studying the role of other social media platforms as they relate to privacy concerns and users' risk beliefs.

References

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

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147–154.

Cavoukian, A. (2010). Privacy by design: The definitive workshop. *Identity in the Information Society*, *3*(2), 247-251.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291-302.

Cocosila, M., Archer, N., & Yuan, Y. (2009). Early investigation of new information technology acceptance: A perceived risk–motivation model. *Communications of the Association for Information Systems*, *25*(1), 339–358.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*, *59*(2), 323-342.

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

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

Fox-Brewster, T. (2016, June 29). *Facebook is playing games with your privacy and there's nothing you can do about it.* Retrieved from: https://www.forbes.com/sites/thomasbrewster/2016/06/29/facebook-location-tracking-friend-games/#35c2e55c35f9 .

Gerrard, P., Cunningham, J. B., & Devlin, J. F. (2006). Why consumers are not using Internet banking: A qualitative study. *Journal of Services Marketing*, *20*, 160–168.

Granville, K. (2018). Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. *The New York Times*. Retrieved from: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Greenwood, S., Perrin, A., & Duggan, M. (2016). Social media update 2016. *Pew Research Center*, 11.

Gu, J., Xu, Y. C., Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19-28.

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

Inman, J. J., & Nikolova, H. (2017). Shopper-facing retail technology: A retailer adoption decision framework incorporating shopper attitudes and privacy concerns. *Journal of Retailing*, *93*(1), 7-28.

Kemp, S. (2017). *Digital in 2017: Global overview.* We are social. Retrieved from: https://wearesocial.com/special-reports/digital-in-2017-global-overview

Koohang, A., Paliszkiewicz, J. & Goluchowski, J. (2018a). Social media privacy concerns: Trusting beliefs and risk beliefs. *Industrial Management & Data Systems, 118*(6), 1209-1228.

Koohang, A., Paliszkiewicz, J. & Nord, J. (2018b). Social media privacy concerns among college students. *Issues in Information systems, 19*(1), 11-19.

Koohang, A. (2017). Social media sites privacy concerns: Empirical validation of an instrument. *Online Journal of Applied Knowledge Management*, *5*(1), 14-26.

Leswing, K. (April 12, 2018). Nearly one in 10 Americans surveyed say they deleted their Facebook account over privacy concerns. *Business Insider.* Retrieved from: http://www.businessinsider.com/delete-facebook-statistics-nearly-10-percent-americans-deleted-facebook-account-study-2018-4

Li, Y., Li, Y., Yan, Q., & Deng, R. H. (2015). Privacy leakage analysis in online social networks. *Computers & Security*, *49*, 239-254.

Liang, H., Shen, F., & Fu, K. W. (2017). Privacy protection and self-disclosure across societies: A study of global Twitter users. *New Media & Society*, *19*(9), 1476-1497.

Liang, K., Liu, J. K., Lu, R., & Wong, D. S. (2015). Privacy concerns for photo sharing in online social networks. *IEEE Internet Computing*, *19*(2), 58-63.

Madden, M. (2012). Privacy management on social media sites. *Pew Internet Report*, 1-20.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58.

Mertler, C. A., & Reinhart, R. V. (2016). *Advanced and multivariate statistical methods: Practical application and interpretation*. New York, NY: Routledge.

Metzger, M. J. (2007). Communication privacy management in electronic commerce. *Journal of Computer Mediated Communication*, *12*(2), 335-361.

Meyer, R. (March 20, 2018). The Cambridge Analytica scandal, in 3 paragraphs. *The Atlantic.* Retrieved from: https://www.theatlantic.com/technology/ archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), 103-125.

Newton, C. (2017, October 27). America doesn't trust Facebook. *The Verge.* Retrieved from: http://www.theverge.com/2017/10/27/16552620/facebook-trust-survey-usage-popularity-fake-news

Park, Y. J., & Jang, S. M. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, *38*, 296–303.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1), 27-41.

Rauhofer, J. (2008). Privacy is dead, get over it! Information privacy and the dream of a risk-free society. *Information & Communications Technology Law*, *17*(3), 185-197.

Shore, J., & Steinman, J. (2015). Did you really agree to that? The evolution of Facebooks privacy policy. *Technology Science*, *2015081102.*

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248-273.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., et al. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reforming European data protection law* (pp. 333–365). Dordrecht, Netherlands: Springer.

Wang, E. S. T., & Lin, R. L. (2017). Perceived quality factors of location-based apps on trust, perceived privacy risk, and continuous usage intention. *Behaviour & Information Technology*, *36*(1), 2-10.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418.

Zheleva, E., & Getoor, L. (2011). Privacy in social networks: A survey. In *Social network data analytics* (pp. 277-306). Springer, Boston, MA.

Zhou, T. (2011). The impact of privacy concern on user adoption of location-based services. *Industrial Management & Data Systems*, *111*, 212–226.

Authors' Biographies

Johnathan Yerby, Ph.D. is the Director of the Center for Cybersecurity Education and Applied Research and an Assistant Professor in the School of Information Technology at Middle Georgia State University. He serves as associate editor-in-chief for JCISSE, editor-in-chief for JITDIS, technical editor for JSAIS, and on the editorial board for Knighted, which is a university-hosted student journal. His teaching, service, and research center around cybersecurity, forensics, awareness, and privacy. He has been involved with several United States national initiatives and governmental agencies to direct and develop security-related education.

Alex Koohang, Ph.D. is Payton Anderson Eminent Scholar, Endowed Chair of Information Technology, Professor, and Dean of the School of Information Technology at Middle Georgia State University. He is the author/co-author of numerous scholarly papers and has written/edited several books. 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. He is a Fellow at the Informing Science Institute. Dr. Koohang is the recipient of many awards, including IACIS Computer Educator of the Year and Lifetime Academic Achievement Award from IIAKM.

Joanna Paliszkiewicz, Ph.D. is a specialist in management issues connected with knowledge management, intellectual capital and trust management. She holds the rank of University Professor of Warsaw University of Life Sciences and Polish-Japanese Academy of Information Technology. Prof. J. Paliszkiewicz is well recognized in Poland and abroad with her expertise in management issues. She has published over 170 original papers and eight books. She serves on the editorial board of several international journals. She is the editor of *Issues in Information Systems* and deputy editor-in-chief of *Management and Production Engineering Review Journal*. Dr. Paliszkiewicz was named the 2013 Computer Educator of the Year by IACIS.

Appendix A. Instrument

SMPC: Collection

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

SMPC: Secondary usage

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

SMPC: Errors

- I am concerned that social media sites do not take enough steps to make sure that my personal information in their files is accurate.
- I am concerned that social media sites do not have adequate procedures to correct errors in my personal information.

- 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.

SMPC: Improper Access

- I am concerned that social media site databases that contain my personal information are not protected from unauthorized access.
- I am concerned that social media sites do not devote enough time and effort to preventing unauthorized access to my personal information.
- 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.

SMPC: Control

- It usually bothers me when I do not have control of personal information that I provide to social media sites.
- 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.
- 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.

SMPC: Awareness

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

Risk beliefs

- In general, it would be risky to give my personal information to social media sites.
- There would be a high potential for loss associated with giving my personal information to social media sites.
- There would be too much uncertainty associated with giving my personal information to social media sites.
- Providing social media sites with my personal information would involve many unexpected problems.

Note: The six SMPC constructs (SMPC: collection, SMPC: secondary usage, SMPC: errors, SMPC: improper access, SMPC: control, and SMPC: awareness) are adapted from Hong and Thong (2013) to specifically describe social media privacy concerns and empirically validated by Koohang (2017). The Risk Beliefs construct is taken from Hong and Thong (2013), and was modified by Koohang et al. (2018a) to reflect social media sites risk beliefs.