Issues in Information Systems
Volume 22, Issue 2, pp. 133-145, 2021

DOI: https://doi.org/10.48009/2_iis_2021_136-149

Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument

Alex Koohang, *Middle Georgia State University, USA, alex.koohang@mga.edu*
Kevin Floyd, *Middle Georgia State University, USA, kevin.floyd@mga.edu*
Johnathan Yerby, *Mercer University, USA, yerby_jm@mercer.edu*
Joanna Paliszkiewicz, *Warsaw University of Life Sciences, Poland, joanna_paliszkiewicz@sggw.edu.pl*

Abstract

This paper endeavors to empirically validate an instrument that measures users' privacy concerns, security concerns, trust, and risk awareness on social media. Four constructs (privacy concerns, security concerns, trust, and risk awareness) were used, each included specific items that explained the construct. Data were collected from 154 undergraduate students from a mid-sized university in the Southeast USA and analyzed via exploratory factor analysis. All subjects were using one or more social media platforms regularly. The results showed that all four constructs of the instrument were reliable to measure measures users' privacy concerns, security concerns, trust, and risk awareness on social media.

Keywords: Social media, privacy, security, awareness, trust

Introduction

Social media (i.e., Facebook, Instagram, Twitter, Snapchat, Pinterest, LinkedIn, Tumblr, Reddit, Vine, Flickr, etc.) is a platform for communicating, accessing news, sharing information, and making a decision. Social media is also being used to create, share, and disseminate information in all forms. It has now become a built-in and necessary tool in our social and business lives. Kemp (2020) reported that over 3.8 billion users are using social media around the world and by mid-2021, more than half of the world's total population will use social media.

Pew Research (2019) reported that the most widely used social media platforms by Americans are YouTube and Facebook, followed by Twitter, Pinterest, Instagram, and LinkedIn. Whilst eBizMBA (2020) reported that worldwide, the top-ranked social media platforms in 2020 based on usage, growth, and influence were Facebook, YouTube, Instagram, Twitter, and WhatsApp.

With its popularity and extensive usage worldwide, many challenges face users of social media. In the present study, we focus on four important challenges – privacy concerns, security concerns, trust, and awareness. We then attempt to develop an instrument with four constructs, each with its associated items, and empirically validate it via exploratory factor analysis.

This study is organized as follows. First, users' privacy concerns, security concerns, trust, and awareness related to social media are defined following a review of the literature. Second, methods that include the instrument, subjects, procedure, and data analysis are described. Third, the results are presented. Fourth, the findings are discussed. Fifth, conclusions and recommendations for future research complete the paper.

Definitions of Terms

Privacy Concerns - Our definition for privacy concerns on social media is based on Hong and Thong (2013, p. 276), where privacy concern was 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." This definition was adapted for social media privacy concerns by Koohang (2017). For the present study, we further refined Koohang's (2017) definition to include privacy concerns about the collection of personal information, secondary usage of personal information, improper access of personal information, and lack of control of personal information.

Security Concerns - Based on a study conducted by Zhang & Gupta (2016), we define security concerns on social media as users being concerns about how secure their personal information is against attacks on identity theft (attackers stealing personal information); impersonation/social phishing (attackers impersonating a real person through a fake website to steal data, login credentials, credit card numbers, etc.).; hijacking (attackers taking control over one's profile); image retrieval/analysis (attackers using face and image recognition software to find more information about users and their linked profiles); and malware attacks (attacker sending malware injected scripts or malicious software to perform activities on users' device without their knowledge).

Trust (Integrity, Benevolence, Competence) - Our definition of trust is based on Paliszkiewicz & Koohang (2016), where social media users have integrity trust (where social media platforms are trustworthy to protect users' privacy and security); benevolence trust (where social media platforms keep users' best interests and well-being in mind); and competence trust (where social media platforms are perceived to be competent in protecting and safeguarding users' personal information).

Awareness - We define awareness as users being aware of potential threats and risks on social media platforms associated with their security and privacy that result in possible negative consequences, harm, and or loss.

Review of the Literature

Privacy Concerns

According to a report from RiskBasedSecurity (2020), the personal information of over 100,000 social media influencers was compromised and partially leaked following the breach of a social media marketing company. Moreover, the report indicates that because of this privacy breach, an additional 250,000 social media users have had their information fully exposed on the dark web. Pew Research Center (2018) reported that 80% of social media users were concerned about advertisers and businesses retrieving their personal information on social media sites. Moreover, 74% of users believe that it is very important for them to be in control of who can access their personal information.

Madden (2012) reported that privacy is a principal concern of users on social networking sites.   Benisch et al. (2011) stated that users of social networking sites believe that they do not have control of their privacy. The leading privacy concerns on social media were studies by Koohang (2017) and Yerby et al. (2019) and included collection, secondary usage, errors, improper access, control, and awareness. These concerns stemmed from a previous study by Hong and Thong (2013), where they studied Internet privacy. They described privacy concerns 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 and Thong (2013, p. 276)

Yerby, et al. (2019) stated that privacy concerns on social media sites are valid and that protecting personal information should be a high priority for social media sites. The authors stressed that measures should be taken by social media sites to ensure users' privacy protection.

Security concerns

A 2019 report by Forbes indicated that an unsecured Facebook database exposed the data of 419 million users (Winder, 2019). The growing number of people joining social media sites has led to increased security breaches as attackers seek to take advantage of vulnerabilities. Some of the prominent security concerns associated with the use of social media platforms include identity theft, spam attacks, malware attacks, social phishing, impersonation, hijacking, and fake requests (Zhang & Gupta, 2016). Fogues et al. (2015) explained that the benefits of using social media networks are now rapidly overshadowed due to growing concerns over user security threats.

Security concerns related to social media also pose a growing threat to businesses. As companies become increasingly connected with consumers via social media, another exchange occurs when consumers share their personal information within social media networks due to a lack of understanding privacy policies, making users vulnerable to security hacks when it comes to the information they share (Fox & Royne, 2018). Alba et al. (1997) noted that while social media provides consumers with access to a vast amount of company information to enable better, more efficient decision-making, consumers are vulnerable when it comes to the information they share. There is often uncertainty about how information is collected, stored, shared, and potentially misused by both public and private businesses (Buchannan et al., 2006).

To address security concerns associated with social media, Carminati et al. (2011) proposed that enhanced access control systems for social network sites are a recommended first step for addressing the security and privacy threats. Similarly, Zhang and Gupta (2016) argue that it is up to social media sites to establish security and trustworthiness within their platforms by studying user's actions and treat them as a means of establishing credible, safe, and lasting social platforms that provide secure infrastructure with regular security updates and notices to users.

Trust

Trust is the backbone for creating relationships on social media sites (Ayaburi & Treku, 2020; Paliszkiewicz & Koohang, 2016; Gibson & Trnka, 2020; Wang et al., 2021; Warner-Søderholm et al., 2018). Trust is essential to securing interactions on social media sites (Wang et al., 2021). Research has shown that trust is lost when breaches occur (Koohang et al., 2018; Roberts, 2018). Trust is a feeling that is built over time by demonstrating having the best interest of the users in mind and being competent in securing the environment (Ba & Pavlou, 2002). Cheng et al. (2017) concluded trust on social media could be broken into the following dimensions: privacy, shared preference, familiarity, convenience, time-saving, information quality, and chatting.

More specifically, trust on social media sites is divided into three dimensions – integrity trust, benevolence trust, and competence trust (Paliszkiewicz & Koohang 2016). Integrity trust refers to the social media sites' trustworthiness to protect users, benevolence trust refers to the social media sites' keeping users' best interests and well-being in mind, and competence trust refers to the social media sites being perceived to be competent in protecting and safeguarding users (Paliszkiewicz & Koohang 2016, Koohang, et al., 2018a, 2018b).

Awareness

User awareness is a vital issue in protecting users against risks and threats on social media. Bulgurcu, Cavusoglu, and Benbasat (2010) defined security awareness as "… an employee's overall knowledge and understanding of potential issues related to information security and their ramifications" (p. 532). D'Arcy et al. (2009) asserted that awareness promotes openness among employees, and openness creates trust (Golembiewski & McConkie, 1975). Furthermore, McKnight and Webster (2001) stated that a relationship between awareness and trust exists to support a trusting environment.

Shaw et al. (2009, p. 92) described security awareness as "… the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control." Yerby, et al. (2019) found that Social media awareness was a significant predictor of risk and that users must be trained on how to avoid identity theft and to secure their personal information. Awareness must include educating users about the threats, risks, and methods to be safer (Carillo et al., 2019; Van der Walt et al., 2018). Users that perceive themselves to be aware of the threats and policies do modify their behaviors when interacting with the social media platforms (Yerby et al., 2019).

The purpose of this study is to empirically validate an instrument with 4 constructs/components (privacy concerns, security concerns, trust, and awareness) identified to be challenges for users of social media platforms. The following research question will be answered. Are the four constructs/components (privacy concerns, security concerns, trust, and awareness) reliable and interpretable among their associated variables?

Methodology

Instrument

The instrument for this study was designed to include 4 constructs/components with their associated items/variables. The constructs are privacy concerns, security concerns, trust, and awareness. The constructs/components with their associated variables are as follows.

Privacy Concerns Construct (Defines collection, secondary usage, improper access, and control)

1. I am concerned that social media sites are collecting my personal information.
2. I am concerned that social media sites share/sell my stored personal information in their databases to other companies.
3. I am concerned that social media sites do not devote enough time and effort to preventing unauthorized access to my personal information.
4. It 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.

Security Concerns Construct (Defines identity theft, impersonation / social phishing, hijacking, image retrieval and analysis, and malware attacks**)**

When I am on social media sites, I am concerned about

1. Identity theft (attacker stealing my personal information).
2. Impersonation/Social phishing (attacker impersonating a real person through a fake website to steal my data, including login credentials and credit card numbers, etc.).

3. Hijacking (attacker taking control over my profile).
4. Image retrieval and analysis (attacker using face and image recognition software to find more information about me and my linked profiles).
5. Malware attacks (attacker sending malware injected scripts or malicious software to perform activities on my device without my knowledge).

Trust Construct (Defines integrity trust, benevolence trust, and competence trust)

When it comes to privacy and security, the social media sites I belong to:

1. are trustworthy.
2. keep my best interests and well-being in mind.
3. are competent in protecting and safeguarding my personal information.

Awareness Construct (Defines security threats/risks, privacy threats/risks, and harm/loss)

When using social media sites

1. I am aware of the potential security threats and risks and their negative consequences.
2. I am aware of potential privacy threats and risks and their negative consequences
3. I am aware that there is potential for harm/loss associated with my security and privacy.

The instrument used a Likert-type scale 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.

Procedure and Sample

After securing approval from the institution's Institutional Research Board (IRB) where this study took place, we administered the instrument electronically via SurveyMonkey™, an Internet survey software to approximately 800 undergraduate students who were majoring in one of the seven information technology major concentrations (e.g.., cybersecurity, forensics, software engineering, etc.) studying at a medium-sized university in the Southeast, USA. At the time of this study, we collected 161 surveys from the subjects. Of the 161 surveys, we eliminated 7 because of incomplete data. This yielded a total of 154 completed surveys to be used for data analysis. The subjects were 18 years and older. They were assured confidentiality and anonymity.

Table 1: Demographics (N = 154)

	N		N
# of SM Platforms use		**Age**	
Facebook	139/154	18 - 20	52
Instagram	121/154	21 - 29	61
LinkedIn	119/154	30 - 39	19
Snapchat	91/154	40 or older	22
Twitter	88/154	**Gender**	
Pinterest	78/154	Female	78
Tumblr	43/154	Male	76
Reddit	29/154		
Vine	17/154		
Flickr	9/154		

Data Analysis

We used exploratory factor analysis to analyze the collected data via SPSS™ version 26,. Exploratory factor analysis determines the underlying constructs for a set of measured variables. According to Mertler and Vannatta (2010), exploratory factor analysis entails four procedures/tests to be conducted and deemed favorable before conducting the final procedure, principal component analysis with Varimax rotation, to answer the research question. These procedures/tests are 1) Kaiser-Meyer-Olkin measure of sampling adequacy and Bartlett's test of sphericity, 2) Eigenvalues (Kaiser Criterion) test, 3) test of variance explained, and 4) the Scree plot test. The index for Kaiser-Meyer-Olkin measure of sampling adequacy should be greater than 0.6, and Bartlett's test of sphericity should be less than .05. The Eigenvalues (Kaiser Criterion) test which retains factors with eigenvalues greater than 1 as common factors and is reliable if the number of subjects is equal or greater than 150, there are less than 30 variables, or the values of communalities are high - normally close .70 and higher. The test of variance explained (showing variance-retain components) for all components retained should account for at least 70% of the total variability. The Scree Plot test that detects all components within the breakpoint before eigenvalues level off is reliable when the subjects are less than 250 and the communalities for each variable are greater than .30 (Mertler and Vannatta, 2010).

With obtaining favorable results for the four procedures/tests, principal component analysis with Varimax rotation is conducted to answer the research question. The principal component analysis with the Varimax rotation procedure forces the number of components with their associated factors/items to be retained. The internal consistency among the factors/items for each component will be determined by the Cronbach's alpha reliability test. An acceptable reliability coefficient should be .70 or higher (Mertler and Vannatta, 2010).

Results

KMO and Bartlett's test of sphericity

Kaiser-Meyer-Olkin measure of sampling adequacy was performed to determine the sampling adequacy. Kaiser-Meyer-Olkin's accepted index must be greater than 0.6. The Bartlett's Test of Sphericity was performed to determine the significance of the study related to the validity and suitability of the responses collected. The p-value of Bartlett's Test of Sphericity must be less than .05.

The result for Kaiser-Meyer-Olkin was .826, indicating that the sampling adequacy was met. The results for Bartlett's test of sphericity (Chi-Squared = 1411.592, df = 105, and p = .000) indicated the existence of the validity and suitability of the collected data. (See Table 2)

Table 2: KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.826
Bartlett's Test of Sphericity	Approx. Chi-Square	1411.592
	df	105
	Sig.	.000

Establishing the number of factors/components that can be retained

The Kaiser Criterion procedure is used to establish the number of factors/components that can be retained. This test retains only components with eigenvalues greater than 1. The procedure eliminates factors with eigenvalues less than 1.

Eigenvalue (Kaiser Criterion)

The Kaiser Criterion procedure is used to establish the number of factors/components that can be retained. This test retains only components with eigenvalues greater than 1. The conditions for the reliability of Kaiser Criterion are as follows. The subjects should be at least equal or greater than 150, the total number of items must be than 30, and or the communalities for all items must be moderate to high.

In the present study, there were 154 subjects, the total number of variables was 15, and communalities values were all moderate to high. These results established the reliability of the Kaiser Criterion. Table 3 shows the results of communalities.

Table 3: Communalities

Constructs	Items	Initial	Extraction
Social Media Privacy Concerns	PRIV1	1.000	.849
	PRIV2	1.000	.841
	PRIV3	1.000	.611
	PRIV4	1.000	.659
Social Media Security Concerns	SEC1	1.000	.635
	SEC2	1.000	.787
	SEC3	1.000	.828
	SEC4	1.000	.722
	SEC5	1.000	.599
Social Media Trusting Beliefs	TRUST1	1.000	.831
	TRUST2	1.000	.857
	TRUST3	1.000	.797
Social Media Threat & Risk Awareness	AWAR1	1.000	.655
	AWAR2	1.000	.712
	AWAR3	1.000	.702

Variance explained

The test of variance explained (showing variance-retain components) for all four retained components, including the initial eigenvalues and the rotation sums of squared loadings components, is shown in Table 4. The total variance-retain accounted for 73.890%. This value is above the acceptable threshold value of 70% of the variability.

Table 4: Total Variance Explained

	Initial Eigenvalues		
Component	Total	% of Variance	Cumulative %
1	5.767	38.447	38.447
2	2.655	17.697	56.144
3	1.597	10.647	66.791
4	1.065	7.099	73.890
	Rotation Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %
1	3.661	24.406	24.406
2	2.811	18.741	43.146
3	2.549	16.992	60.138
4	2.063	13.752	73.890
Note: Total % of Variance explained for all 4 Components = 73.891			

Extraction Method: Principal Component Analysis

Scree Plot Test

Figure 1 shows the Scree Plot. It is a graphical representation of the eigenvalues that uses Principal Component Analysis. It further confirms data points that were above the breakpoint where the number of factors is retained. This test also detected four components within the breakpoint before eigenvalues level off.

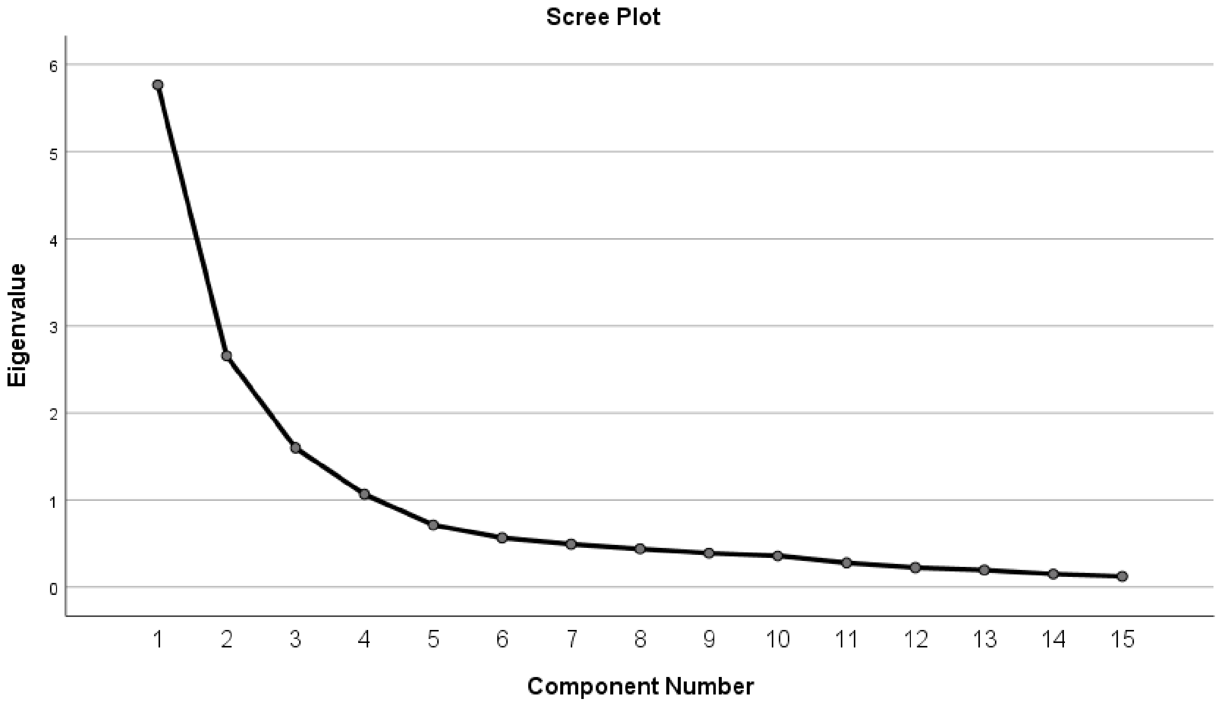

Figure 1: Scree Plot Test

Principal component analysis with Varimax rotation

The results of the principal component analysis with Varimax rotation are shown in Table 5. Component 1 (Privacy Concerns) retained four items, i.e., PRIV1: Collection, PRIV2: Secondary Usage, PRIV3: Improper Access, and PRIV4: Control with the loading values of 0.859, 0.856, 0.627, and 0.713, respectively. There were no cross-loadings for this component on any of the other three components.

Component 2 (Security Concerns Construct) retained 5 items, i.e., SEC1: Identity theft, SEC2: Impersonation / Social phishing, SEC3: Hijacking, SEC4: Image retrieval and analysis, and SEC5: Malware attacks with the loading values of 0.851, 0.893, 0.810, and 0.744 respectively. There were no cross-loadings for this component on any of the other three components.

Component 3 (Trust Construct) retained 3 items, i.e., TRUST1: Integrity, TRUST2: Benevolence, and TRUST3: Competence, with loading values of 0.905, 0.901, and 0.868, respectively. There were no cross-loadings for this component on any of the other three components.

Component 4 (Awareness Construct) retained 3 items, i.e., AWAR1: Security threats & risks, AWAR2: Privacy threats & risks, and AWAR3: Harm/Loss with loading values of 0.808, 0.800, and 0.760, respectively. There were no cross-loadings for this component on any of the other three components.

The reliability tests for the components suggested existence of internal consistency for the items of each component, Privacy Concerns = .87, Security Concerns = .89, Trust = .90, and Awareness = .75.

Table 5: Rotated Component Matrix

		Component			
Constructs	Items	1	2	3	4
Social Media Privacy Concerns	PRIV1	**0.859**	0.252	-0.203	0.076
	PRIV2	**0.856**	0.273	-0.175	0.051
	PRIV3	**0.627**	0.369	-0.094	0.271
	PRIV4	**0.713**	0.278	-0.144	0.229
Social Media Security Concerns	SEC1	0.340	**0.713**	0.022	0.099
	SEC2	0.235	**0.851**	0.029	0.084
	SEC3	0.158	**0.893**	0.006	0.078
	SEC4	0.247	**0.810**	0.045	0.054
	SEC5	0.152	**0.744**	-0.107	0.103
Social Media Trusting Beliefs	TRUST1	-0.087	0.009	**0.905**	-0.066
	TRUST2	-0.203	0.056	**0.901**	-0.041
	TRUST3	-0.156	-0.065	**0.868**	-0.125
Social Media Threat & Risk Awareness	AWAR1	0.011	0.030	0.043	**0.808**
	AWAR2	0.185	0.053	-0.187	**0.800**
	AWAR3	0.228	0.242	-0.115	**0.760**

Extraction Method: Principal Component Analysis | Rotation Method: Varimax with Kaiser Normalization | Rotation converged in 5 iterations

Discussion

The primary goal of this study was to empirically validate an instrument that measures users' privacy concerns, security concerns, trust, and risk awareness on social media. The instrument's constructs were privacy concerns, security concerns, trust, and risk awareness. Collected data from 154 subjects were analyzed through exploratory factor analysis. The discussion of findings is as follows.

The *Privacy Concerns Construct/Component* retained all its four designated items/factors indicating that the component was empirically validated to be reliable and interpretable among all its four items/factors. The four items retained were privacy concerns regarding 1) social media sites collecting users' personal information, 2) social media sites sharing users' stored personal information in their databases and/or sell the information to other companies, 3) social media sites not devoting enough time and effort in preventing unauthorized access to users' personal information, and 4) users not having control or autonomy over decisions about how their personal information is collected, used, and shared by social media sites.

The *Security Concerns Construct/Component* retained all its five designated items/factors, indicating that the component was empirically validated to be reliable and interpretable among all its five items/factors. The five items retained were security concerns about regarding 1) identity theft - attacker stealing users' personal information, 2) impersonation/social phishing - attacker impersonating a real person through a fake website to steal users' data, including login credentials and credit card numbers, etc., 3) hijacking - attacker taking control over users' profile, 4) image retrieval and analysis - attacker using face and image recognition software to find more information about users and their linked profiles, and 5) malware attacks - attacker sending malware injected scripts or malicious software to perform activities on users' device without their knowledge.

The *Trust Construct/Components* retained all its three designated items/factors, indicating that the component was empirically validated to be reliable and interpretable among all its three items/factors. The three items retained were 1) users' integrity trust – social media sites being trustworthy, 2) users' benevolence trust – social media sites keeping users' best interests and well-being in mind, and 3) competence trust – social media sites being competent in protecting and safeguarding users' personal information.

The *Awareness Construct/Component* retained all its three designated items/factors, indicating that the component was empirically validated to be reliable and interpretable among all its three items/factors. The three items retained were 1) users' awareness of potential security threats and risks and their negative consequences, 2) users' awareness of potential privacy threats and risks and their negative consequences, and 3) users' awareness of the potential for harm/loss associated with their security and privacy.

Conclusions

In summary, the instrument was found to be reliable to measure users' privacy concerns, security concerns, trust, and awareness on social media sites. We defined users' privacy concerns on social media sites to include the collection of personal information, secondary usage of personal information, improper access of personal information, and lack of user's control of personal information. Users' security concerns on social media included users being concerns about how secure their personal information is against attacks on identity theft, impersonation/social phishing; hijacking, image retrieval/analysis, and malware attacks. Trust on social media was defined as integrity, benevolence, and competence. Integrity trust describes social media platforms as trustworthy to protect users' privacy and security, benevolence trust describes social media platforms keeping users' best interests and well-being in mind, and competence trust describes social media platforms being perceived as competent in protecting and safeguarding user's personal information. Awareness describes users of social media being aware of risks and threats associated with their security and privacy on social media platforms that result in possible negative consequences, harm, and or loss.

We recommend that this instrument be used for future research. It could also be modified to include new items in each of the constructs, i.e., privacy concerns, security concerns, trust, and awareness on social media sites. Also, new constructs that are deemed critical to users of social media sites may be added to the instrument for testing. This study took place in a university setting using undergraduate students. Future studies may want to consider using a different population sample from other universities or non-university entities/companies.

References

Alba J., Lynch, J., Weitz, B., Janiszewski, C., Lutz, R., Sawyer, A., & Wood, S. (1997). Interactive home shopping: Consumer, retailer, and manufacturer incentives to participate in electronic marketplaces, *Journal of Marketing*, *61*(3), 38–53. https://doi.org/10.1177%2F002224299706100303

Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. International Journal of Information Management, 50, 171-181.

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly*, 243-268.

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.

Buchanan, T., Paine, C., Joinson, A.B., & Reips, U. (2006). Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157–65. https://doi.org/10.1002/asi.20459

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M., & Thuraisingham, B. (2011). Semantic web-based social network access control. *Computers & Security*, *30*. 108-115. https://doi.org/10.1016/j.cose.2010.08.003

Cheng, X., Fu, S., & de Vreede, G. J. (2017). Understanding trust influencing factors in social media communication: A qualitative study. *International Journal of Information Management*, *37*(2), 25-35.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information systems research*, *20*(1), 79-98.

eBizMBA (2020). Top 15 most popular social networking sites. Retrieved January 23, 2021 from http://www.ebizmba.com/articles/social-networking-websites

Fogues, R., Such, J.M., Espinosa, A., & Garcia-Fornes, A. (2015). Open challenges in relationship based privacy mechanisms for social media services. *International Journal of Human Computer Interaction, 31*(5), 350-370. https://doi.org/10.1080/10447318.2014.1001300

Fox, A.K., & Royne, M.B. (2018). Private information in a social media world: Assessing consumers' fear and understanding of social media privacy. *Journal of Marketing Theory & Practice*, *26*, 72-89. https://doi.org/10.1080/10696679.2017.1389242

Gibson, K., & Trnka, S. (2020). Young people's priorities for support on social media: "It takes trust to talk about these issues." Computers in Human Behavior, 102, 238-247.

Golembiewski, R. T. & McConkie, M. (1975). The centrality of interpersonal trust in group processes. In G. L Cooper (Ed.), *Theories of group processes* (pp. 131-185). London: John Wiley & Sons.

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

Kemp, S. (2020). "Digital 2020 report." Retrieved February 20, 2021 from https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media

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

Koohang, A., Floyd, K., Rigole, N., & Paliszkiewicz, J. (2018a). Security policy and data protection awareness of mobile devices in relation to employees' trusting beliefs. *Online Journal of Applied Knowledge Management (OJAKM)*, *6*(2), 7-22

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

Mertler, C. & Vannatta, R. (2010). *Advanced and Multivariate Statistical Methods: Practical Application and Interpretation, (4th Edition).* Glendale, CA: Pyrczak Publishing

Paliszkiewicz, J., & Koohang, A. (2016). Social media and trust: A multinational study of university students. Informing Science, Santa Rosa, CA, USA: Informing Science Press.

Pew Research (2019), Social media fact sheet. Retrieved January 23, 2021 from https://www.pewresearch.org/internet/fact-sheet/social-media/

Pew Research Center (2018). "Americans' complicated feelings about social media in an era of privacy concerns." Retrieved March 15, 2021 from https://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

RiskBasedSecurity (2020). "Personal Data of 350,000+ Social Media Influencers and Users Compromised." Retrieved March 15, 2021 from https://www.riskbasedsecurity.com/2020/06/24/personal-data-of-350000-social-media-influencers-and-users-compromised-following-preen-me-hack/

Roberts, S. (2018). Learning lessons from data breaches. *Network Security*, *2018*(11), 8-11.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100.

Van der Walt, E., Eloff, J. H., & Grobler, J. (2018). Cyber-security: Identity deception detection on social media platforms. *Computers & Security*, *78*, 76-89.

Wang, X., Wang, Y., Lin, X., & Abdullat, A. (2021). The dual concept of consumer value in social media brand community: A trust transfer perspective. International Journal of Information Management, 59, 102319.

Warner-Søderholm, G., Bertsch, A., Sawe, E., Lee, D., Wolfe, T., Meyer, J., ... & Fatilua, U. N. (2018). Who trusts social media? Computers in human behavior, 81, 303-315.

Winder, D. (2019, September 5). *Unsecured facebook databases leak data of 419 million users*. Forbes. https://www.forbes.com/sites/daveywinder/2019/09/05/facebook-security-snafu-exposes-419-million-user-phone-numbers/?sh=7e7a5a161ab7

Yerby, J., & Floyd, K. (2018, August). Faculty and staff information security awareness and behaviors. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 6, No. 1, pp. 23-23).

Yerby, J., Koohang, A., & Paliszkiewicz, J. (2019). Social media privacy concerns and risk beliefs. *Online Journal of Applied Knowledge Management (OJAKM)*, *7*(1), 1-13.

Yerby, J., Koohang, A., & Paliszkiewicz, J. (2019). Social media privacy concerns and risk beliefs. *Online Journal of Applied Knowledge Management*, 7(1), 1-13.

Zhang, Z., & Gupta, B.B. (2016). Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems*, *86*, 914-925. https://doi.org/10.1016/j.future.2016.10.007