The Impact of Privacy Concerns and Perceived Vulnerability to Risks on Users Privacy Protection Behaviors on SNS: A Structural Equation Model

Noora Sami Al-Saqer and Mohamed E. Seliaman
Department of Information Systems, King Faisal University,
P.O. Box: 400, Al-Hufof, Al-Hasa, 31982,
Saudi Arabia

***Abstract*—This research paper investigates Saudi users' awareness levels about privacy policies in Social Networking Sites (SNSs), their privacy concerns and their privacy protection measures. For this purpose, a research model that consists of five main constructs namely information privacy concern, awareness level of privacy policies of social networking sites, perceived vulnerability to privacy risks, perceived response efficacy, and privacy protecting behavior was developed. An online survey questionnaire was used to collect responses from a sample of (108) Saudi SNSs users. The study found that Saudi users of social networking sites are concerned about their information privacy, but they do not have enough awareness of the importance of privacy protecting behaviors to safeguard their privacy online. The research results also showed that there is a lack of awareness of privacy policies of Social networking sites among Saudi users. Testing hypothesis results using the Structural Equation Modeling (SEM) showed that information privacy concern positively affects privacy protection behaviors in SNSs and perceived vulnerability to privacy risks positively affects information privacy concern.**

Keywords—Social networking sites (SNSs); information privacy concern; perceived vulnerability; SEM; protection behavior

I. INTRODUCTION

TODAY, the number of internet users in Saudi Arabia has reached 19.6 million [1]. With the continuous development in internet technologies over the years, smartphones revolution and the web mobile internet, social networking sites became a need for every internet user. SNSs are now the most preferred communication choice of users in today's context. The benefits that the SNSs provide are indeed remarkable on many dimensions, including reducing the financial cost especially with the reasonable prices of internet services in Saudi Arabia. These Social networking services also help the users to go beyond the geographic locations, and make it easier to connect and communicate with people all over the world.

Every new invention in technology field including the SNSs, is intended to simplify users' lives by helping them to follow the modern era of speed and technology. However on another side, using SNSs is associated with some privacy risks such as the misuse of users personal information with serious personal and social implications. The users' lack of awareness of privacy policies and the consequences associated with it, might make it easier to breach the personal privacy and increase cyber-crimes. Some SNSs are requesting users to provide sensitive information including some personal or private details. Some users are providing these information easily without even thinking about the consequences of providing such information, and without knowing that these information and details are being sold and shared to third parties for marketing reasons. Most SNSs are clearly publishing their privacy policies (PP) regarding information sharing but many users do not pay enough attention to figure out the details components of each SNSs' PP.

Only few research studies investigated the relationship between SNSs' PP awareness level and its effects on raising privacy concern and privacy protecting behaviors.

The main objectives of this research paper are : (1)Measure the level of awareness among Saudi SNSs users of PP, (2) measure the information privacy concern of Saudi SNSs users, (3) measure the effect of information privacy concern and awareness of privacy policies on privacy protecting behaviors.

II. RELATED RESEARCH

Privacy has been interpreted as the ''boundary control process in which individuals regulate when, how, and to what extent information about them is communicated to others'' [2]. Maintaining Internet users privacy is a legal and human right of person regarding information disclosing, storing, miss maintaining, miss using, and transmitting through internet based applications including SNSs, web sites, and search engines [3].

Privacy policy is about principles of actions adopted by an individual or an organization in protecting their personal information and serves as guideline for users who would like to share their information [4]. In today's context where technology is interfering in everything we do, millions of users are vulnerable to privacy threats. SNSs provide easy to use privacy settings to users. These settings provide visibility and privacy options for a user profile to limit the access to certain people like: family and friends, or set the profile as public. However, most people don't change the privacy settings and set their SNSs account as default[3]. The use of SNSs varies from shopping, communication, expressing personal ideas and feelings to organizational matter of use.

Although there are large advantages offered by SNSs, there are also many challenges towards the information privacy from personal or organizational aspects. Moreover, most users don't know about the vulnerability of their information while using SNSs [4]. Some SNSs provide comprehensive, updated and detailed privacy policy, so the user can understand the potential risks when posting their information online. However, the more details and long comprehensive text make users ignore it, do not read it, and just clicking the agree button without understanding the implications of its content. People usually hate reading long texts especially when the PP includes technical jargons which are hard to understand for many users. Other reason to the lack of awareness of PP is the absence of engagements of users while developing the PP[4].

Privacy policies clearly mention about saving, sharing, and modifying the users' information and contents they post. Since many users do not read privacy policies, few people know about these details. The Saudi society in particular is conservative and religious society influencing its people attitudes and behaviors [5]. Hence, focusing on users' privacy and raising their awareness level of privacy threats is an important aspect. Information privacy is a critical issue in online environment as online companies depend on collecting large amounts of personal information about users [6].

Online users are concerned about information privacy when surfing the Web because the access to their personal information cannot be controlled meaning that information privacy is threatened [6, 7]. User concern about information privacy was found as an important factor which has a positive effect on his/her behavioral intention to practice privacy protection measures[8].

Previous studies of SNSs in Saudi Arabia focused on the reasons that motivate Saudi females to use Facebook. One study shows an existence of privacy concern among Saudi female users [5]. Studies [9, 10]found that Saudi women have higher levels of privacy concerns as compared to Saudi men. Regardless of gender differences for privacy behavior, gender does not predict worries about the ways third parties use personal information [11]. According to [11] users are aware of privacy protecting measures to protect themselves from threats and the users who are concerned about their information privacy are more likely to apply these privacy protecting measures.

While the research work in [11] used a simple binary variable (Yes, No) to measure the privacy protection measure use, this paper contributes to the SNS privacy research by developing and validating new measurement items operationalizing the construct of privacy protection behavior in SNS. In addition, this paper contributes to SNS research by developing new construct 'awareness level of privacy policies' and validating new self-developed measurement items operationalizing the construct. While research [11] was conducted in Malaysia, this paper validated the extended model with the new added construct of privacy protection behavior in the context of Saudi Arabia which is a different social context. Moreover, research [11] targeted a sample of only undergraduates at a public Malaysian university while this research targeted a more general sample of public respondents including different age groups and education levels.

III. Research Model and Hypothesis

This study followed the quantitative approach using a theoretical model as shown in Figure 1 to achieve the above-mentioned objectives. The research model developed for this study consists of the following five constructs:

1) Information privacy concern: It is the "extent to which an individual is concerned about organizational practices related to the collection and use of his or her personal information" [11].

2) Awareness level of privacy policies of SNSs: This construct is intended to understand the degree to which higher level of awareness of PP of SNSs affects the privacy protecting behavior in SNSs. It refers to SNSs users awareness and understanding of Privacy policies in SNSs.

3) Privacy protection behavior in SNSs: It is the adaption of protective behaviors to guard the privacy [12] .

4) Perceived vulnerability to privacy risks: is the degree to which a SNSs user believes a privacy threats will occur to him\her [11].

5) Perceived response efficacy: is the belief that a recommended protecting measure is effective in protecting the self and others from a threat [11].

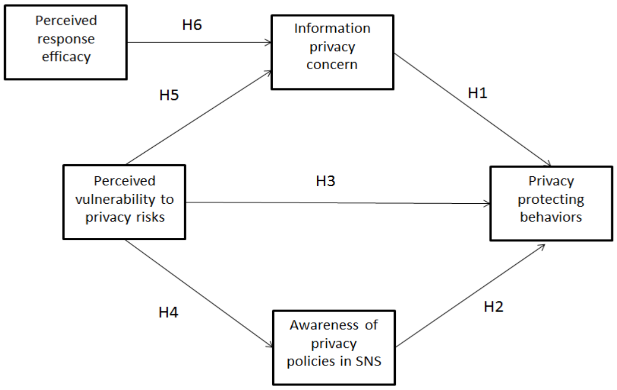
Perceived response efficacy
H6
Information privacy concern
H5
H1
Perceived vulnerability to privacy risks
H3
Privacy protecting behaviors
H4
H2
Awareness of privacy policies in SNS

Fig. 1. Research model

The model is derived from previous research models grounded in several theories such as: (1) information privacy concern was introduced by two theories: agency theory and social contract theory, both suggest that privacy concern exist in online transactions due to incomplete information about online behavior of customer information [11][17[11]] . In our study we focus on the information privacy concern among SNSs' users regarding their information to understand its effect on privacy protection behavior. However, neither the agency theory nor the social contract theory provided applicable framework for empirical research [17]. (2) Awareness level of privacy policies of SNSs was self-developed to study the impact of reading and understanding the content of SNSs privacy policy on raising the adoption of privacy protection behaviors. (3) Privacy protection behavior in SNSs: the human behavior was introduced in many information systems theories such as: Social Cognitive Theory, Theory of Reasoned Action (TRA), and theory of planned behavior (TPB), and Protection motivation Theory (PMT) in each theory behavior was interpreted in different perspectives [12] [11][17]. In our model we intended to understand the factors that influence actions and practices SNSs users do to protect their information privacy by studying the relationships between perceived vulnerability to privacy risk, information privacy concern, awareness level of PP in SNSs, and privacy protection behavior. (4) Perceived vulnerability to privacy risks was derived from the protection motivation theory (PMT), our focus here is to understand the relationship between this construct and information privacy concern, awareness level of SNSs PP, and privacy protection behaviors. (5) Perceived Response – efficacy was derived from protection motivation theory (PMT); it was added to understand its effect on information privacy concern.

Based on the research model described above, the following hypotheses were developed:

H 1: Information privacy concern positively affects privacy protection behaviors in SNS.

H2: Higher awareness of SNSs' PP positively affects privacy protection behaviors in SNSs.

H3: Perceived vulnerability to privacy risks positively affects privacy protecting behaviors.

H4: Perceived vulnerability to privacy risks increase awareness level of privacy policies in SNS.

H5: Perceived vulnerability to privacy risks positively affects information privacy concern.

H6: Perceived response efficacy positively affects information privacy concern.

IV. Research Methodology

A. Sampling and Data collection

An online survey questionnaire was developed to collect data required for assessing the SNSs users' awareness of PP. The survey questionnaire consisted of 22 questions and was divided into two sections. The first section contained questions about user's demographic information. The second section contained questions related to the research model five constructs. A sample of (108) respondents filled out the survey. Table 1 shows the survey items. Table 2 shows the basic demographic data of respondents. Majority of participants are young females and adults belong to the age group of 2 to 30 years. Most of them are educated holding bachelor degree.

TABLE I. Survey Items

Construct	Item
Information Privacy Concern	**IPC1:** I am concerned about submitting my personal information in social networking sites because of what others might do with it [11]. **IPC2:** I am concerned about submitting my personal information in social networking sites because it could be used in a way I did not foresee [11].
perceived vulnerability to privacy risks	**PVPR1:** I could be subjected to a malicious computer/ information security problems (e.g. virus, privacy, identity theft, hacking and etc.) in social networking sites [11]. **PVPR2**: I feel my personal information in social networking sites could be misused [11]. **PVPR3** I feel my personal information in social networking sites could be made available to unknown individuals or companies without my knowledge [11]. **PVPR4:** I feel my personal information in social networking sites could be made available to government agencies [11]. **PVPR5:** I feel my personal information in social networking sites could be inappropriately used [11].
Awareness level of Privacy Policies in SNSs	**APPS1**: I read privacy policies of SNSs before using them. **APPS2:** I understand carefully what is mentioned in the Privacy policies of SNSs. **APPS3:** I read the updated versions of SNSs PP.
Perceived Response - efficacy	**PRE1**: If I used privacy protection measures in social networking sites, I could probably protect myself from losing my information privacy [11]. **PRE2:** I can protect my information privacy better if I use privacy protection measures in social networking sites [11]. **PRE3:** Utilizing privacy protection measures in social networking sites works to ensure my information privacy [11]. **PRE4:** If I utilize privacy protection measures in social networking sites, I am less likely to lose my information privacy [11].
Privacy Protection behavior in SNSs	**PPBS 1:** I do not share my personal information (like: mobile number, personal photos, personal events) on SNSs. **PPBS 2:** I tend to be careful about sharing my personal information (like: mobile number, personal photos, etc.) while using SNSs.

TABLE II. Demographic Data

Measure	Item	Frequency	Percent
Gender	Male	18	26.5%
	Female	50	73.5%
Age	Less than 20	13	12%
	From 21 to 30	63	58.3%
	From 31 to 40	24	22.2%
	From 41 to 50	7	6.5%
	More than 50	1	0.9%
Education	Pre high school	7	6.5%
	High school	14	13%
	College	52	48.1%
	Post graduate	35	32.4%

V. Results and Discussion

A. The measurement model

a) Reliability for the measurements: The sample consisted of 108 participants. WarpPls 5.0 was used to assess the reliability and validity of the the survey questionnaire as the main measurement instrument of this research study. The survey questionnaire measurement tool included 16 items forming 5 latent variables beside the moderators. Cronbach's Alpha (CA) was used to assess constructs reliability. CA estimates the inter-correlations of the indicators [18]. The acceptable score for CA is 0.7 and higher [18]. In addition, the constructs reliability was tested using Composite reliability (CR). CR or the internal consistency reliability readings unlike CA, takes into account the different loadings of the indicators. The acceptable score for CR should be 0.7 and higher [15]. As shown in table 3, all constructs reported Cronbach's Alpha values above the acceptable thresholds of 0.7. In addition, all CR values above the acceptable thresholds of 0.7.

TABLE III. MEASUREMENT RELIABILITY TESTING RESULTS

Construct	No of items	Cronbach's alpha	Composite reliability
Information privacy concern	2	0.791	0.905
Perceived vulnerability to privacy risks	5	0.832	0.882
Awareness level of privacy policies	3	0.851	0.910
Perceived response efficacy	4	0.868	0.911
Privacy protecting behaviors in SNS	2	0.761	0.893

b) Factor loadings: Factor loadings for the measured variables have to be at least 0.5 or the variable becomes a candidate for removal [15]. The factor loadings were calculated for the measured variables using confirmatory factor analysis as shown in table 4. All variables have statisified the loading value above 0.5 required for inclusion in the model.

TABLE IV. FACTOR LOADING FOR MEASURED VARIABLES

	IPC	PVPR	APPS	PRE	PPBS	SE	P value
IPC1	(0.909)					0.076	<0.001
IPC2	(0.909)					0.076	<0.001
PVPR1		(0.749)				0.079	<0.001
PVPR2		(0.846)				0.077	<0.001
PVPR3		(0.767)				0.079	<0.001
PVPR4		(0.757)				0.079	<0.001
PVPR5		(0.748)				0.079	<0.001
APPS1			(0.868)			0.077	<0.001
APPS2			(0.896)			0.076	<0.001
APPS3			(0.869)			0.077	<0.001
PRE1				(0.803)		0.078	<0.001
PRE2				(0.872)		0.077	<0.001
PRE3				(0.897)		0.076	<0.001
PRE4				(0.815)		0.078	<0.001
PPBS1					(0.898)	0.076	<0.001

c) The validity assessment:: Convergent validity was assessed by calculating composite reliability and the Average Variance Extracted (AVE) for each latent construct. Convergent validity is "the extent to which a measure is related to other measures which have been designed to assess the same construct" [14]. AVE is an indicator of convergence that is used to calculate the mean variance extracted for the construct items [15]. The composite reliability coefficients for all constructs are greater than the critical value of 0.7. In addition, all constructs reported an AVE score exceeding 0.5 as shown in Table 5.

TABLE V. CONVERGENT VALIDITY STATISTICS FOR THE CONSTRUCTS

Construct	Composite reliability	AVE
information privacy concern	0.905	0.827
perceived vulnerability to privacy risks	0.882	0.600
Awareness level of privacy policies	0.910	0.771
Perceived response efficacy	0.911	0.718
Privacy protecting behaviors in SNS	0.893	0.807

Discriminant validity refers to "the extent in which a construct is truly distinctive from other constructs" [15].The square root of the Average Variance Extracted (AVE) for each latent construct was calculated to assess the discriminant validity and then comparing the values with the other latent constructs correlations. All constructs reported an AVE score exceeding 0.5. In addition, the square root of AVE for each construct is greater than all correlations of other constructs supporting the measurement discriminant validity as shown in **Table 6**.

TABLE VI. DISCRIMINANT VALIDITY FOR THE CONSTRUCTS

	IPC	PVPR	APPS	PRE	PPBS
IPC	(0.909)				
PVPR	0.645	(0.774)			
APPS	0.147	0.173	(0.878)		
PRE	0.151	0.224	0.087	(0.848)	
PPBS	0.435	0.404	0.102	0.177	(0.898)

d) The structural model: Structural Equation Modeling (SEM) is a multivariate statistical technique used to test the model hypotheses that describes relationships between variables [13]. SEM was used to test the hypothesis of the research model. structural equation modeling (SEM) belongs to the second generation data analysis method. SEM is a multivariate statistical technique used to test the model hypotheses that describes relationships between variables [13]. SEM is mainly used by researchers because it considers the measurements errors when analysing data statistically [13, 17]. SEM is preferred by researchers because it is not only used to assess the structural model – the assumed relationship between multiple independent and dependent constructs – but at the same time, it also asseses the measurement model – the loadings of observed measurement items on their latent constructs. SEM allows for examining reliability and validity of the measurements with the testing of the hypotheses [13].

e) Goodness of fit measures (GOF): Goodness of Fit measures indicates "how well the specified model reproduces the observed covariance matrix among the indicator items" [15]. In structural equation modeling (SEM) it is important to assess whether a specified model fits the data or not. Goodness of fit measures provide the most necessary indication of how well the proposed theory fits the data. Different indices as shown in Table 7 reflect a different aspect of model fit and present the acceptable value for each fit measure [19].

The confirmatory factor analysis calculated ten Goodness of Fit measures as shown in Table 7.

TABLE VII. GOODNESS OF FIT MEASURES

GOF of research model	Acceptable value
Average path coefficient (APC)=0.250, P=0.002	Good if p< 0.05 [16]
Average R-squared (ARS)=0.237, P=0.003	Good if p< 0.05 [16]
Average block VIF (AVIF)=1.374	acceptable if <= 5, ideally <= 3.3 [16]
Average full collinearity VIF (AFVIF)=1.389	acceptable if <= 5, ideally <= 3.3 [16]
Tenenhaus GoF (GoF)=0.420	small >= 0.1, medium >= 0.25, large >= 0.36 [16]
Sympson's paradox ratio (SPR)=1.000	acceptable if >= 0.7, ideally = 1 [16]
R-squared contribution ratio (RSCR)=1.000	acceptable if >= 0.9, ideally = 1 [16]
Statistical suppression ratio (SSR)=1.000	acceptable if >= 0.7 [16]
Nonlinear bivariate causality direction ratio (NLBCDR)=1.000	acceptable if >= 0.7 [16]

f) Hypotheses testing results: significant level chosen for testing hypothesis is at <=0.05. The results of testing the research model are presented in Figure 2, and summarized in Table 8.

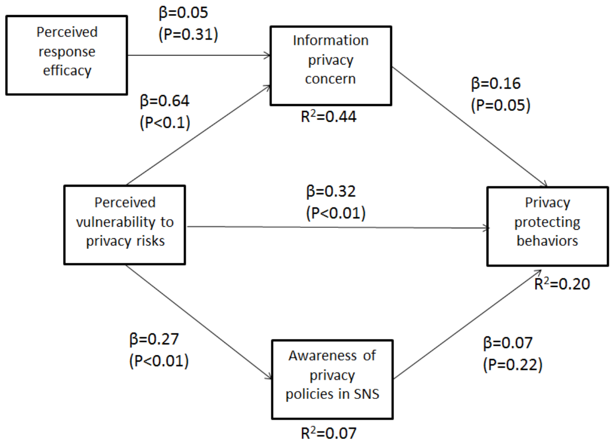
Perceived response efficacy
β=0.05
(P=0.31)
Information privacy concern
R^2=0.44
β=0.64
(P<0.1)
β=0.16
(P=0.05)
Perceived vulnerability to privacy risks
β=0.32
(P<0.01)
Privacy protecting behaviors
R^2=0.20
β=0.27
(P<0.01)
Awareness of privacy policies in SNS
R^2=0.07
β=0.07
(P=0.22)

Fig. 2. Structural Equation Model Results

TABLE VIII. MODEL RESULTS

Hypothesis	Test result	Conclusion
H 1: Information privacy concern positively affects privacy protection behaviors in SNS.	(beta=0.16, p=0.05)	Supported
H2: Higher awareness of SNSs' PP positively affects privacy protection behaviors in SNSs.	(beta=0.07, p=0.22)	Not Supported
H3: perceived vulnerability to privacy risks positively effects privacy protecting behaviors.	(beta=0.32, p<0.01)	Supported
H4: perceived vulnerability to privacy risks increase awareness level of privacy policies in SNS.	(beta=0.27, p<0.01)	Supported
H5: perceived vulnerability to privacy risks positively effects information privacy concern.	(beta=0.64, p<0.01)	Supported
H6: perceived response efficacy positively effects information privacy concern.	(beta=0.05, p=0.31)	Not supported

Hypothesis 1 suggests a positive relationship between information privacy concern and privacy protection behavior. This Hypothesis was supported and it was found that information privacy concern positively influences privacy protecting behavior (beta=0.16, p=0.05). Hypothesis 2 proposes a positive relationship between awareness levels of privacy policies of social networking sites and privacy protection behaviors. It was found that awareness level of PP does not affect privacy protecting behaviors (beta=0.07, p=0.22) which does not support hypothesis 2. Hypothesis 3 suggests that perceived vulnerability to privacy risks positively affects privacy protecting behaviors. It was found that perceived vulnerability to privacy risks positively contributes to the adaption of privacy protecting behaviors (beta=0.32, p<0.01) supporting hypothesis 3. Hypothesis 4 proposes that perceived vulnerability to privacy risks increases awareness level of privacy policies in SNS. The perceived vulnerability to privacy risks positively contributes to awareness level of PP of SNSs (beta=0.27, p<0.01). Hence, hypothesis 4 is supported. Hypothesis 5 proposes that perceived vulnerability to privacy risks positively affects information privacy concern. Results showed that perceived vulnerability to privacy risks positively contributes to information privacy concern (beta=0.64, p<0.01) and that supports hypothesis 5. Hypothesis 6 suggests that perceived response efficacy positively affects information privacy concern. It was found that this hypothesis 6 is not supported.

VI. CONCLUSIONS

This study aimed to investigate Saudi users' awareness levels about privacy policies of Social Networking Services (SNSs) and the factors affect privacy protecting behaviors. A research model that consists of five constructs was developed for this purpose. The study sample consists of (108) participants who were surveyed to collect the data. The research model was assessed using WarpPLS 5.0 software.

Testing the hypotheses results supported all proposed hypotheses except for hypothesis two and hypothesis six. The study found that Saudi users' privacy concerns and perceived vulnerability to privacy risks in social networking sites are significant antecedents of their privacy protection behaviors. In addition, users' perceived vulnerability to privacy risks in social networking sites positively influences their awareness levels of the content of privacy policies of SNS. In contrast with our expectation, it was found that awareness level of privacy policies does not necessarily influence privacy protection behavior in social networking sites. Also, it was found that perceived response efficacy does not influence the information privacy concern which is consistent with previous studies in the literature.

Similar to any other study, this research has some limitations. Contrasting the expectations, the research results did not report any correlation between awareness level of privacy policies and user privacy protecting behaviors. This issue can be investigated further considering more sophisticated measurement items for some constructs in the current research model. The sample size can also be increased in future research and the quantitative methodology can be assisted by a qualitative inquiry for more in depth analysis.

Future studies may enhance the research model by adding more constructs, expand the sample size, and apply mixed methodology that includes qualitative approach to interpret the results.

Acknowledgment

The authors would like to acknowledge the support for this research provided by King Faisal University.

References

[1] Anonymous "Communication and information technology commesion annual report 2014," communication and information technology commesion, KSA, 2014.

[2] E. Van De Garde-Perik, P. Markopoulos, B. De Ruyter, B. Eggen and W. Ijsselsteijn, "Investigating privacy attitudes and behavior in relation to personalization," *Soc. Sci. Comput. Rev.,* vol. 26, pp. 20-43, 2008.

[3] S. Talib, N. A. Ismail, A. Olowolayemo, S. Naser, S. Aina, S. Z. Haron, M. Yusof and A. Hanisah, "Social networks privacy policy awareness among undergraduate students: The case of twitter," in *Information and Communication Technology for the Muslim World (ICT4M), 2014 the 5th International Conference on,* 2014, pp. 1-5.

[4] S. Talib, A. Razak, S. Munirah, A. Olowolayemo, M. Salependi, N. F. Ahmad, S. Kunhamoo and S. K. Bani, "Perception analysis of social networks' privacy policy: Instagram as a case study," in *Information andCommunication Technology for the Muslim World (ICT4M), 2014 the 5th International Conference on,* 2014, pp. 1-5.

[5] Y. Al-Saggaf, "Saudi females on Facebook: An ethnographic study," *International Journal of Emerging Technologies and Society,* vol. 9, pp. 1-19, 2011.

[6] M. Zviran, "User's Perspectives on Privacy In Web-Based Applications." *Journal of Computer Information Systems,* vol. 48, 2008.

[7] E. Aimeur, S. Gambs and A. Ho, "UPP: User privacy policy for social networking sites," in *Internet and Web Applications and Services, 2009. ICIW'09. Fourth International Conference on,* 2009, pp. 267-272.

[8] M. L. Korzaan and K. T. Boswell, "The influence of personality traits and information privacy concerns on behavioral intentions," *Journal of Computer Information Systems,* vol. 48, pp. 15-24, 2008.

[9] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," *Comput. Hum. Behav.,* vol. 25, pp. 153-160, 2009.

[10] M. G. Hoy and G. Milne, "Gender differences in privacy-related measures for young adult Facebook users," *Journal of Interactive Advertising,* vol. 10, pp. 28-45, 2010.

[11] N. Mohamed and I. H. Ahmad, "Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia," *Comput. Hum. Behav.,* vol. 28, pp. 2366-2375, 2012.

[12] Y. Feng and W. Xie, "Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors," *Comput. Hum. Behav.,* vol. 33, pp. 153-162, 2014.

[13] J. Recker, *Scientific Research in Information Systems: A Beginner's Guide.* Springer Science & Business Media, 2012.

[14] D. Cramer and D. L. Howitt, *The Sage Dictionary of Statistics: A Practical Resource for Students in the Social Sciences.* Sage, 2004.

[15] J. Hair, W. Black, B. Babin and R. Anderson, "Multivariate Data Analysis Seventh Edition Prentice Hall," 2010.

[16] N. Kock, "WarpPLS 5.0 user manual," *Laredo, TX: ScriptWarp Systems,* 2015.

[17] Y. Li, "Theories in online information privacy research: A critical review and an integrated framework," *Decis. Support Syst.,* vol. 54, pp. 471-481, 2012.

[18] M. Moqbel, *The Effect of the use of Social Networking Sites in the Workplace on Job Performance,* 2012.

[19] D. Hooper, J. Coughlan and M. Mullen, "Structural equation modelling: Guidelines for determining model fit," *Articles,* pp. 2, 2008.