Ashish Gupta

is Assistant Professor in the Department of Business Management at Dr. Harisingh Gour Central University, Madhya Pradesh, India. His research areas include relationship marketing, CRM, customer loyalty, e-services and consumer markets. He holds a degree in Management and has presented research papers at international and national conferences.

Anil Dhami

is studying for a Master of Technology (MTech) at the Department of Computer Science and Engineering, Motilal Nehru National Institute of Technology, Allahabad, India.

Keywords: social media, information sharing, Facebook, security, trust, privacy

Public and semi-public profiles

Ashish Gupta, Department of Business Management, Dr. Hari Singh Gour Central University, Near Nepal Palace, New Building, Sagar, Madhya Pradesh 470003, India

Papers

Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites

Ashish Gupta and Anil Dhami

Received (in revised form): 7th July 2015

Abstract

In the internet era, social networking websites have thrived. Computer-mediated communication has changed the rules of social interaction and communication. Most social networking sites, for example Orkut, Facebook, Google+ and Twitter, facilitate users with features such as online interaction, sharing of information and developing new relationships. Online interaction and sharing of personal information on social networking sites has raised new privacy concerns. This requires an exploratory study into users' behavioural intention to share information. *Journal of Direct, Data and Digital Marketing Practice* (2015) **17**, 43–53. doi:10.1057/dddmp.2015.32

Introduction

This paper discusses efforts to develop a research model with security and privacy concerns conceptualized as an antecedent of trust in social networking sites and a moderator of information sharing. The study aims to understand the impact of security, trust and privacy concerns on willingness to share information on social networking sites. Using an online questionnaire, empirical data was collected from 250 Facebook users of different age groups over the time period of 4 months. Reliability analysis, confirmatory factor analysis and structure equation modelling were used to validate the proposed research framework.

This empirical study, based on an established theoretical foundation, will help the research community to gain a deeper understanding of the impacts of privacy concerns in the context of Facebook. The proposed ideas and discussion are equally applicable to social networking site operators as useful strategies for enhancing users' acceptance. The privacy concerns of research respondents were found to be statistically significant, suggesting that these concerns, like security and trust, have a positive effect on information sharing.

In recent years, user participation in social networking sites has moved from a niche phenomenon to the highest level of mass adoption. The rapid growth of social networking sites in Web 2.0, such as Facebook, Orkut, Google+ and Twitter, facilitates millions of individuals to build a public or

semi-public profile within a bounded system. Facebook has become the most-accessed website in cyberspace today. Facebook statistics shows that it had 936 million daily active users for March 2015, with 1.44 billion monthly active users as of 31 March 2015.¹ Active participation in social networking sites has changed the way people build their online personal network for computer-mediated communication.^{2,3,4}

Victims of compromised privacy

The primary objective of social networking users is to make connections, communicate and maintain relationships. But latest trends show that social networking sites like Facebook are reshaping the way people communicate. Users share information and take collective action, playing an important role in, for example, the Arab Spring uprising, London riots and Assam riots.^{4,5} The issue of information privacy has been captivating, with 25 per cent of Americans considering themselves victims because their information privacy has been compromised.⁶ Programmes like Beacon, part of Facebook's advertisement system that sent data from external websites to Facebook, have triggered user protests over privacy issues. In addition, there are many other policies, for example advertisements, used by social networking sites where the privacy and trust of the user may be violated.

Pervasive and invisible technology

For users of social networking sites, there are many privacy and trust considerations that need to be addressed. First, the information revealed in users' profiles can lead to risks such as identity theft, online stalking and cyber harassment.⁴ Second, features such as newsfeeds make personal information more accessible and visible to others.⁷ Social network sites deeply penetrate their users' everyday lives and, as pervasive technology, tend to become invisible once they are widely adopted, ubiquitous and taken for granted.⁸ However, social networking site operators have provided many security features for preserving the privacy of users. Despite these features, however, the impact of security, privacy and trust on sharing of information needs to be addressed. Research by Johnston *et al.*⁹ investigated the role Facebook use plays in the creation or maintenance of social capital among university students in South Africa. This paper focuses on the impact of privacy, security and trust on users' willingness to share information within social networking sites in the context of Facebook. The primary research questions of this study are:

RQ1: What are the antecedents of trust in social networking sites?

RQ2: What is the impact of privacy, security, and trust on the willingness of sharing information?

Theoretical background

Previous research into privacy concerns on social networking sites

Online social networking is emerging as the web's top application.¹⁰ Sites used primarily for social interaction have received significant research attention in recent years. Some prior studies examined users' acceptance of social networking sites with behavioural intention to use. Despite this, the

Privacy and technology adoption

growing importance of privacy concerns in the social networking context has not been previously studied as a moderator in the technology adoption model (TAM). In related social networking site research, some prior studies examined the impact of privacy concerns on usage behaviour and information revelation. Chai *et al.*¹¹ defined information privacy as ‘the claim of individuals, groups, or institutions to determine of themselves when, how, and to what extent information about them is communicated to others’.

Risks to online privacy

Trust and security have a direct effect on usage behaviour and information revelation, with trust the central component of social exchange theory.^{12,13,14} As trust and privacy play a crucial role in face-to-face communication and the development of a new relationship, several studies propose that a similar approach is used by users on social networking sites.^{15,16} Other studies have further established the privacy paradox on social networking sites. Furthermore, several risks to users of online social networks and groups have been highlighted,^{10,15} such as embarrassment, stalking and identity theft. Online social networking has been criticized because users lack trust in site security.¹⁶ Dwyer *et al.*¹⁶ and Goettke and Christiana¹⁷ have attempted to determine the implication of privacy concerns and awareness for users’ online practices and behaviour.

Defining trust, privacy and security

Concepts of privacy and trust in social networking sites

Privacy concerns are the primary focus of our study. Trust is defined as the ‘willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the truster irrespective of the ability to monitor or control that other party’.¹⁶ Privacy can be defined as ‘control over the flow of one’s personal information, including the transfer and exchange of that information’.¹² Security is defined as ‘the extent to which a user believes that using a social networking application will be risk-free’.¹² The major categories of trust and privacy in social networking sites can be defined by the following measures:

- Security
- Control over the flow of information in a user’s profile
- Notification

Constructing the framework

Research framework, hypothesis and constructs

Several theoretical models have been proposed and tested in the past to understand the privacy concerns in social networking sites. Drawing on social network theory, the TAM and previous frameworks, Shin,¹² Dwyer *et al.*¹⁶ and Gross *et al.*⁴ propose a framework for finding the willingness to share information on social networking sites, as represented in Figure 1. The proposed hypothesis in Figure 1 was empirically tested.

Proposed hypotheses

The proposed hypotheses aim to find the impact of privacy, security and trust on the willingness to share information on social networking sites. According to the proposed hypotheses, perceived security, perceived

Figure 1: Proposed research model

privacy and perceived trust are the factors that influence a user's willingness to share information on social networking sites.

- H1:** Perceived security is positively related to perceived trust within social networking sites.
- H2:** Perceived privacy is positively related to perceived trust within social networking sites.
- H3:** Perceived security is positively related to information sharing in social networking sites.
- H4:** Perceived privacy is positively related to information sharing in social networking sites.
- H5:** Perceived trust is positively related to information sharing in social networking sites.

Perceived privacy

The following research constructs were used in the proposed model.

Privacy is defined as a process of anonymity preservation and is strongly connected to control over information about the self. In online environments, people who perceive higher threats to privacy are less disposed to disclose information about the self because they perceive themselves as less able to control information and also protect themselves. In contrast, when people perceive lower privacy risks and higher control, such as when privacy policies are clearly exposed, they disclose more personal information.¹⁸ Research in information security and marketing has argued that information privacy and consumer concerns thereof are one of the most important issues in today's technology-based environment¹⁹ The concept of privacy is in itself not new and it has generally been defined as an individual's ability to control the terms by which their personal information is acquired and used.²⁰

Perceived trust

Trust is mandatory when risk is present.^{21,22,23} Trust is the foundation of any transaction that takes place between two parties. There are several facets to the concept of trust. For face-to-face, trust is a critical determinant of sharing information and developing new relationships.^{24,25} Trust is also important for successful online interactions.^{26, 27,28,29} Trust is believed to be used in the calculation of perceived cost. High trust would lead to a perception of low cost and vice versa. Studies of interpersonal exchange situations confirm that trust is a precondition for self-disclosure because it reduces perceived risks involved in revealing private information.³⁰

Perceived security

From a consumer perspective, perceived security of an electronic commerce transaction may be defined as 'the subjective probability with which consumers believe that their personal information (private and monetary) will not be viewed, stored, and manipulated during transit and storage by inappropriate parties in a manner consistent with their confident expectations'. Security corresponds to concerns about the protection of personal information with three specific goals: integrity that ensures information is not altered during transit and storage; authentication that addresses the verification of a user's identity and eligibility for data access; and confidentiality that requires that data use be confined to authorized purposes by authorized people.^{31, 32,33} Prior research has found that security and privacy concerns were actually based on user perceptions, not objective measures, because the average internet user is not knowledgeable enough to distinguish between the various security features present on a particular website.³⁴

Information sharing

In line with previous research,^{4,35,36} the data shows high levels of information revelation on Facebook. Millions of people have joined social networking sites, adding profiles that reveal personal information. The reputations of social networking sites have been diminished by a number of incidents publicized by the news media.^{37, 38,39, 40} Is it possible to join a network of millions of people and be able to trust all of them? This does not seem realistic. Since people are obviously joining networks and revealing information, what role does trust play in the use of social networking sites?

Levelling online and offline privacy

Privacy within social networking sites is often not expected or is undefined.¹⁶ Social networking sites record all interactions and retain them for potential use in social data mining. Offline, most social transactions leave behind no trace. Therefore, these sites need explicit policies and data protection mechanisms in order to deliver the same level of social privacy found offline. Since online social privacy is harder to guarantee, does a higher level of concern for internet privacy affect the use of social networking sites?

Data analysis and interpretation**Pilot and reliability tests**

Data was collected by conducting an online customized questionnaire survey of Facebook users to test the proposed framework. The survey was conducted from May to August 2013. To maximize the response rate, we utilized search engines and emails. All items of the proposed research framework were measured on a 5-point Likert scale, ranging from 1

Table 1: Demographic profile of respondents

Profile	Items	Frequencies	Percentage
<i>Gender</i>	Male	189	77.1
	Female	56	22.9
<i>Age</i>	16–25 years	194	79.2
	26–35 years	40	16.3
	36–50 years	8	3.3
<i>Educational qualification</i>	Intermediate	23	9.4
	Graduate	119	48.6
	Postgraduate	100	40
<i>Occupation</i>	Student	165	67.3
	Government sector	43	17.6
	Private sector	14	5.7
	Professional	18	7.3

Table 2: Cronbach's α values for measurement model

Construct	Number of items	Cronbach's α
Perceived privacy	4	0.826
Perceived security	4	0.785
Perceived trust	4	0.725
Information sharing	5	0.736

(strongly disagree) to 5 (agree). A pilot survey was used for validating the proposed framework before the final analysis. Reliability analysis was performed using SPSS 19.0. Cronbach's alpha (α), which provides a measure of the internal consistency of a test or scale, was used to test the internal consistency of the questionnaire. SEM (structural equation modelling) was used to detect relationships among constructs. SEM was performed using AMOS 19.0.

Demographic profile of respondents

The online questionnaire was distributed through emails and search engines. A total of 265 questionnaires were collected over the time period of 4 months, out of which 246 were usable for the study. Table 1 shows the sample demographics of collected data.

Reliability and validity analysis

Before analysing the research framework, reliability analysis was used to test the internal consistency of the questionnaire. Cronbach's α is a widely used measurement for internal consistency. To ensure the reliability of the study, items were adapted based on an acceptable Cronbach's α score above 0.60, based on standard values.^{41,42} Table 2 represents the Cronbach's α of the measured construct of the research framework — it suggests that the internal consistency of the measured constructs is acceptable for the study. The overall reliability assessment of the entire scale was observed well with a Cronbach's α of 0.825.

Model fit summary

Confirmatory factor analysis is used for the model fit of the proposed framework. For structural equation model fit, various fit indices and tests have been developed. These indices and tests, however, can point to conclusions about the extent to which a model actually matches the

Table 3: Fit indices for the measurement models

Fit indices	Recommended value	Measurement model
χ^2		361.239
df		113
χ^2/df	≤ 3	3.1
Goodness of fit index (GFI)	≥ 0.90	0.942
Adjusted for degrees of freedom (AGFI)	≥ 0.90	0.889
Comparative fit index (CFI)	≥ 0.90	0.91
Root mean square error of approximation (RMSEA)	≤ 0.08	0.076

Table 4: Summary of hypothesis tests

Hypotheses	Path coefficient	p-value	Support
H1: Perceived Security→Perceived Trust	0.25**	0.000	Yes
H2: Perceived Privacy→Perceived Trust	0.51**	0.000	Yes
H3: Perceived Security→Information Sharing	0.22**	0.000	Yes
H4: Perceived Privacy→Information Sharing	0.04	0.005	No
H5: Perceived Trust→Information Sharing	0.25**	0.000	Yes

** $p < 0.001$

observed data, known as good model fit involving non-experimental research. The following model fit indices are used to validate the model fit:

1. χ^2/df
2. Goodness of fit indices (GFI)
3. Adjusted goodness of fit indices (AGFI)
4. Comparative fit indices (CFI)
5. Root mean square error of approximation (RMSEA)

Table 3 represents the model fit indices that satisfy their respective criteria suggested in the prior literature review. Therefore, we can conclude that the proposed framework has a good fit with the collected sample data. The comparison of fit indices with recommended values^{43, 44,45} represent a good model fit.

The hypothesized causal paths (β) were estimated for hypothesis testing. Table 4 represents the results of hypothesis testing.

- H1:** proposes that there is a positive relationship between perceived privacy and perceived trust ($\beta = 0.51$; $p < 0.000$), thus supporting:
- H1:** suggests that if users have control over their information flow and protection of their profile privacy, then it increases their trust level in Facebook.
- H2:** proposes that there is a positive relationship between perceived security and perceived trust ($\beta = 0.25$; $p < 0.000$), thus supporting hypothesis H2. This suggests that if users are provided with greater

Structural paths and hypothesis test

Figure 2: Result of hypothesis testing

security while accessing their profile, then it increases their trust level.

H3: proposes that there is a positive relationship between perceived security and information sharing ($\beta = 0.22$; $p < 0.000$), thus supporting:

H3: suggests that if users are provided with greater security levels over the internet, then it increases the user's interest in sharing information in Facebook.

H4: proposes that there is a positive relationship between perceived privacy and information sharing ($\beta = 0.04$; $p < 0.500$), thus rejecting hypothesis H4.

H5: proposes that there is a positive relationship between perceived trust and information sharing ($\beta = 0.25$; $p < 0.000$), thus supporting hypothesis H5.

This suggests that users' trust in the ability of Facebook will increase their willingness to share information. Thus, we can conclude that perceived security and perceived privacy have a positive relationship with perceived trust in Facebook and are antecedents of perceived trust. Figure 2 and Table 4 summarize the result of hypothesis testing.

Discussion and conclusion

Control increases trust

The primary objective of the study is to investigate the effect of users' privacy concerns on usage behaviour and information sharing on social networking sites with reference to Facebook. Human behaviour issues have a crucial role in the deployment of social networking sites. Using the extended TAM and social exchange theory, the proposed research framework was empirically tested. Our research findings suggest that users

having control over their information flow and protection of their profile is more likely to lead to trust in Facebook. Another factor that affected trust in Facebook was the security features provided by Facebook and individual belief that accessing Facebook over the internet is secure.

Privacy and sharing

Further results suggest that perceived privacy and perceived security are antecedents of perceived trust, whereas there is a strong correlation between perceived privacy and perceived trust. In terms of information sharing, when trust is exerted through privacy and trust, this leads to user willingness to share information. In contrast, privacy has no direct effect on sharing of information — an interesting result of the study. This shows that trust in the ability of Facebook will lead to a tendency for users to share more information.

Practical implications for site operators

Aside from theoretical values, the results have significant practical implications. The findings may provide social network operators with a better understanding of how privacy concerns may affect user acceptance and information revelation. This study gives an insight to site operators into users' sense of belonging as a motive for sharing information and users' privacy concerns, which may lead operators to develop and promote corresponding applications. There are certain limitations to this study, however. First, most of the research respondents belonged to the age group of 16–35 years, which may not cover the general population of social networking sites users. Second, social network users lived in different countries, were from different cultures and had different perceptions of privacy concerns, which potentially influenced their usage behaviour.

References

1. <http://newsroom.fb.com/company-info/>, accessed 1 July 2015.
2. Correa, T., Hinsley, A. W. and de Zúñiga, H. G. (2010) 'Who interacts on the web? The intersection of users' personality and social media use', *Computers in Human Behavior*, Vol. 26, No. 2, pp. 247–253.
3. Lin, K. Y. and Lu, H.-P. (2011) 'Why people use social networking sites: An empirical study integrating network externalities and motivation theory', *Computers in Human Behavior*, Vol. 27, No. 3, pp. 1152–1161.
4. Gross, R. and Acquiti, A. (2005) 'Information revelation and privacy in online social networks', Proceedings of the Association for Computing Machinery workshop on privacy in the electronic society (Alexandria, VA, 7 November). ACM Press, New York.
5. Doerr, B., Fouz, M. and Friedrich, T. (2012) 'Why rumors spread so quickly in social networks communication', *Association for Computing Machinery*, Vol. 55, No. 6, pp. 70–75.
6. Mohamed, N. and Ahmad, I. H. (2012) 'Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia', *Computers in Human Behavior*, Vol. 28, No. 6, pp. 2366–2375.
7. Boyd, D. (2008) 'Facebook's privacy trainwreck — Exposure, invasion, and social convergence', *The International Journal of Research into New Media Technologies*, Vol. 14, No. 1, pp. 13–20.
8. Luedtke, J. (2003) 'Toward pervasive computing — RFID tags: Pervasive computing in your pocket, on your key chain and in your car', 17 July, *DMReview.com*.
9. Johnston, K., Tanner, K., Lalla, N. and Kawalski, D. (2013) 'Social capital: The benefit of Facebook "friends"', *Behaviour & Information Technology*, Vol. 32, No. 1, pp. 24–36.
10. Cheung, C. M. K., Chiu, P. Y. and Lee, M. K. O. (2011) 'Online social networks: Why do students use Facebook?', *Computers in Human Behavior*, Vol. 27, No. 4, pp. 1337–1343.

11. Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R. and Upadhyaya, A. J. (2009) 'Internet and online information privacy: An exploratory study of preteens and early teens', *IEEE Transactions on Professional Communication*, Vol. 52, No. 2, pp. 167–182.
12. Shin, D. (2010) 'The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption', *Interacting with Computers*, Vol. 22, No. 5, pp. 428–438.
13. Ajzen, I. (1991) 'The theory of planned behavior', *Organizational Behavior and Human Decision Processes*, Vol. 50, No. 2, pp. 179–211.
14. Lin, K.-Y. and Lu, H.-P. (2011) 'Why people use social networking sites: An empirical study integrating network externalities and motivation theory', *Computers in Human Behavior*, Vol. 27, No. 3, pp. 1152–1161.
15. Almadhoun, N. M., Dominic, P. D. D. and Woon, L. F. (2011) 'Perceived security, privacy, and trust concerns within social networking sites: The role of information sharing and relationships development in the Malaysian higher education institutions marketing', *International Conference on Control System, Computing and Engineering*, IEEE, Malaysia, pp. 426–431.
16. Dwyer, C., Hiltz, S. R. and Passerini, K. (2007) 'Trust and privacy concerns within social networking sites: A comparison of Facebook and MySpace', *Americas Conference on Information Systems*, Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, 9–12 August, Colorado, USA, p. 339.
17. Goettke, R. and Christiana, J. (2007) 'Privacy and online social networking websites', *Computer Science 199r: Special Topics in Computer Science Computation and Society: Privacy and Technology*, 14 May.
18. Weber, R. H. (2009) 'Internet of things — Need for a new legal environment?', *Computer Law & Security Review*, Vol. 25, No. 6, pp. 522–527.
19. Miyazaki, A. D. and Fernandez, A. (2001) 'Consumer perceptions of privacy and security risks for online shopping', *Journal of Consumer Affairs*, Vol. 35, No. 1, pp. 27–44.
20. Westin, A. F. (1967) *Privacy and Freedom*, Atheneum, New York.
21. Corritore, C. L., Kracher, B. and Wiedenbeck, S. (2003) 'On-line trust: concepts, evolving themes, a model', *International Journal of Human Computer Studies*, Vol. 58, No. 6, pp. 737–758.
22. Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995) 'An integrative model of organizational trust', *Academic Management Review*, Vol. 20, No. 3, pp. 709–734.
23. Pavlou, P. A. (2003) 'Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model', *International Journal of Electronic Commerce*, Vol. 7, No. 3, pp. 69–103.
24. Fukuyama, F. (1995) *Trust: The Social Virtues and the Creation of Prosperity*, Simon & Schuster, New York.
25. Lewis, J. D. and Weigert, A. (1985) 'Trust as a social reality', *Social Forces*, Vol. 63, No. 4, pp. 967–985.
26. Coppola, N., Hiltz, S. R. and Rotter, N. (2004) 'Building trust in virtual teams', *IEEE Transactions on Professional Communication*, Vol. 47, No. 2, pp. 95–104.
27. Jarvenpaa, S. and Leidner, D. (1998) 'Communication and trust in global virtual teams', *JCMC*, Vol. 3, No. 4, <http://www.ascusc.org/jcmc/vol3/issue4/jarvenpaa.html>, accessed December 2013.
28. Meyerson, D., Weick, K. E. and Kramer, R. M. (1996) 'Swift trust and temporary groups' in Kramer, R. M., (ed) *Trust in Organizations: Frontiers of Theory and Research*, Sage, Thousand Oaks, CA.
29. Piccoli, G. and Ives, B. (2003) 'Trust and the unintended effects of behavior control in virtual teams', *MIS Quarterly*, Vol. 27, No. 3, pp. 365–395.
30. Metzger, M. J. (2004) 'Privacy, trust, and disclosure: Exploring barriers to electronic commerce', *Journal of Computer-Mediated Communication*, Vol. 9, No. 4, pp. 1143–1168.
31. Belanger, F., Hiller, J. S. and Smith, W. J. (2002) 'Trustworthiness in electronic commerce: The role of privacy, security, and site attributes', *Journal of Strategic Information Systems*, Vol. 11, No. 3, pp. 245–270.
32. Camp, L. J. (1999) 'Web security and privacy: An American perspective', *Information Society*, Vol. 15, No. 4, pp. 249–256.
33. Chellappa, R. K. (2008) 'Consumers' trust in electronic commerce transactions: The role of perceived privacy and perceived security', Unpublished manuscript, Emory University, Atlanta, GA.

34. Suh, B. and Han, I. (2003) 'The impact of customer trust and perception of security control on the acceptance of electronic commerce', *International Journal of Electronic Commerce*, Vol. 7, No. 3, pp. 135–161.
35. Govani, T. and Pashley, H. (2005) 'Student awareness of the privacy implications when using Facebook', Paper presented at the Privacy Poster Fair at Carnegie Mellon University School of Library and Information Science, USA, <http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf>, accessed 14 December 2005.
36. Tufekci, Z. (2008) 'Can you see me now? Audience and disclosure regulation in online social network sites', *Bulletin of Science, Technology and Society*, Vol. 28, No. 20, pp. 20–36.
37. Chiaramonte, P. and Martinez, E. (2006) 'Jerks in space', *The New York Post*, 18 March, p. 6, New York.
38. Hass, N. (2006) 'In your Facebook.com', *The New York Times*, 8 January, Section 4A, pp. 30–31, New York.
39. Mintz, J. (2005) 'Friendster's "Eww" moment', *The Wall Street Journal*, 8 December, Section B1, p. 23.
40. Read, B. (2006) 'Think before you share: Students' online socializing can have unintended consequences'. in *Chronicle of Higher Education*, Washington DC, p. 121.
41. George, D. and Mallery, P. (2003) *SPSS for Windows Step by Step: A Simple Guide and Reference. 11.0 update*, Allyn & Bacon, Boston, MA.
42. Dinev, T. and Hart, P. (2006) 'An extended privacy calculus model for e-commerce transactions', *Information Systems Research*, Vol. 17, No. 1, pp. 61–80.
43. Iacobucci, D. (2010) 'Structural equations modeling: Fit indices, sample size, and advanced topics', *Journal of Consumer Psychology*, Vol. 20, No. 1, pp. 90–98.
44. Scott, J. (1995) 'The measurement of information systems effectiveness: Evaluating a measuring instrument', *ACM SIGMIS Database*, Vol. 26, No. 1, pp. 43–61.
45. Bagozzi, R. and Yi, Y. (1988) 'On the evaluation of structural equation models', *Journal of the Academy of Marketing Science*, Vol. 16, No. 1, pp. 74–94.