Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook

Anil Dhami, Neha Agarwal, Tamal Kanti Chakraborty, Brijendra Pratap Singh and Jasmine Minj
Dept. of Computer Science & Engineering
Motilal Nehru National Institute of Technology Allahabad
Allahabad, India

***Abstract*— In the era of Internet technologies, social networking websites has witnessed thriving popularity. Computer mediated communication has changed the rules of social interaction and communication. Most social networking sites like Orkut, Facebook, Google+, Twitter etc. facilitates user's with the features like online interaction, sharing of information and developing new relationships etc. Online interaction and sharing of personal information in social networking sites has raised new privacy concerns. So, it requires an exploratory insight into user's behavioural intention to share information. This research aims to develop a research model, with security and privacy concerns conceptualized as an antecedent of trust in social networking site and moderator of information sharing. The study aims to understand the impact of security, trust and privacy concerns on the willingness of sharing information in social networking sites.**

Using an online questionnaire, empirical data were collected from 250 Facebook user's of different age group over the time period of 4 months. Reliability analysis, confirmatory factor analysis, structure equation modelling is 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 concern in the context of Facebook.

Practical implications: - The paper increases the understanding of user's willingness to reveal information on social networking site on their level of privacy, security and trust. The proposed ideas and discussion is equally applicable to social networking site operators with useful strategies for enhancing user's acceptance.

Findings:-The privacy concerns of research respondents were found statistically significant and suggest that privacy concerns like security, trust has a positive effect on information sharing.

Keywords—TAM(technology acceptance model), SEM (structural equation modeling), Social exchange theory.

I. Introduction

In the recent years, user's participation in the social networking sites has moved from its niche phenomenon to its highest level of mass adoption. The rapid growth of social networking sites under web 2.0 such as Facebook, Orkut, Google+, Twitter etc. felicitates million of individuals to build a public or semi-public profile with in a bounded system. Facebook has become most accessed website in the cyberspace today. Facebook statistics shows that it has 1 billion active user's as of October 2012 with 552 million daily active user's in average in June 2012[1].

The active participation in social networking sites have changed the way people build their online personal network for computer mediated communication [2] [3]. The primary objective of social networking user's is to make connections, communication and maintain relationships. But latest trends shows social networking sites like Facebook is reshaping the way people communicate. User share information and take collective action, playing an important role in, for example the Arab spring up-spring, London riots and Assam riots etc. [4] [5].

The issue of information privacy has been captivating with 25% of Americans consider themselves victims because their information privacy has been compromised [6]. Program like Beacon (2007), which is part of Facebook advertisement system that sent data from external website to Facebook has triggered user's protest over privacy issues. In addition, there are many other policies like advertisement etc. used by social networking sites where privacy and trust of the user's may be violated.

For social networking site user's, there are many privacy and trust consideration that needs to be addressed. First, the information revealed in user's profile can lead the risk like identity theft, online stalking, and cyber harassment [4]. Second, the feature like news feed makes personal information more accessible and visible to others [7]. However, social networking site operators have provided many security features for preserving the privacy of user's. Despite all such features, the impact of security, privacy, and trust on sharing of information needs to be answered. This paper focuses the impact of privacy, security, and trust on user's willingness to share information with in the social networking sites in the context of Facebook. The primary research questions of the study are:

978-1-4673-4529-3/12/$31.00 ©2012 IEEE

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

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

II. THEORETICAL BACKGROUND

A. *Previous research on privacy concerns in social networking sites*

Online social network is emerging as the web's top application [8]. Social networking sites, which are primarily used for social interaction, have received significant attention in research in recent years.

Some prior studies examined the user's acceptance of social networking sites, with behavioural intention to use. Despite, the growing importance of privacy concerns in the social networking sites context; has not been previously studied as a moderator in the TAM. In related social networking sites research, some prior studies examined the impact of privacy concerns in usage behaviour and information revelation. In [9] author has 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.

In [10] [11] [3] authors has proposed trust, security leads the direct effect on usage behaviour and information revelation with trust as central component of social exchange theory. As trust and privacy plays a crucial role in face to face communication and development of new relationship; the similar approach is used by the user's in social networking sites proposed by authors in [12] [13] [4]. Other studies have further established the privacy paradox on social networking sites. Furthermore, several risks to user's of online social network and group have been highlighted [8] [12], like embracement, stalking, identity theft. Online social networking has been criticized because user's lack trusts in site security [13]. In [13] [14] [15] authors have attempted to determine implication of privacy concerns and awareness to user's online practices and behaviour.

B. *Concept of privacy and trust in social networking sites*

Privacy concern is the primary focus of our study. Some prior studies examined the privacy concerns in social networking sites as discussed earlier. As trust is defined as *"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 [13]."* Whereas privacy can be defined as, *"control over the flow of one's personal information, including the transfer and exchange of that information [16]".* Security is defined as *"the extent to which a user's believes that using a social networking application will be risk frees [16]".* The major categories of trust and privacy in social networking site can be defined by the following measures:

- security
- control over the flow of information in user's profile
- notification

III. RESEARCH FRAMEWORK AND HYPOTHESIS

Several theoretical models have been proposed and tested in the past to understand the privacy concerns in social networking site. Drawing on social network theory, TAM model and previous framework in [16] [13] [4]; we propose a framework for finding the willingness of sharing information in social networking sites as represented in Fig.1. The proposed hypothesis in Fig.1 was empirically tested.

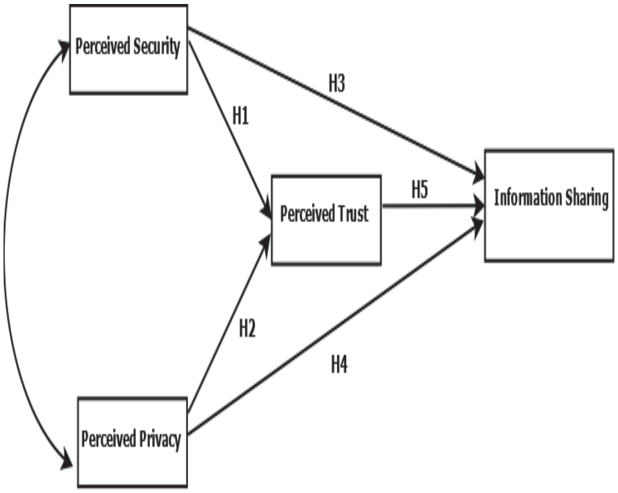

Fig. 1. Research framework

A. *Proposed hypothesis*

The proposed hypothesis aims to find impact of privacy, security, and trust on the willingness to share information in social networking site. According to proposed hypothesis; perceived security, perceived privacy and perceived trust are the factors that influence user's willingness to share information in social networking sites. Thus the proposed hypotheses are summarized in Table I.

The constructs used in our hypothesized model are defined in Table II.

TABLE I. RESEARCH HYPOTHESIS

H#	Hypothesis
H1	Perceived security is positively related to perceived trust with in social networking sites.
H2	Perceived privacy is positively related to perceived trust with in 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.

TABLE II. CONSTRUCT DEFINITIONS

Construct	Definition
Perceived privacy	Extent to which an individual have control over his information flow and protection of his profile privacy.
Perceived trust	An individual belief in the ability of social networking site that revealing information and performing any task is risk free.
Perceived security	An individual belief that using social networking site over Internet is risk free.
Information sharing	An individual belief that they will continue to share information over social networking site with regard to privacy concerns.

IV. RESEARCH DESIGN AND METHODOLOGY

A. Data collection

Data were collected by conducting an online customized questionnaire survey of Facebook user's, to test proposed research framework. The survey was conducted from July 2012 to October 2012 for the time period of 4 months. To maximize the response rate, we had utilized the search engines and emails. Likert-type scale was selected as the most appropriate measure for this study. All items of proposed research framework were measured on a five-point likert scale ranging from “strongly disagree” (1) to “agree” (5). Pilot survey was used for validating the proposed framework before the final analysis.

B. Tools and methods

Reliability analysis was performed by using SPSS 19.0. Cronbach’s alpha (α) 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) technique is used to detect relationship among constructs. SEM model was performed by using AMOS 19.0.

V. RESULTS

A. Profile of respondents

Online questionnaire was distributed through emails and search engines. A total of 265 respondents were collected over the time period of 4 month, out of which 246 were usable for the purpose of study. Table III shows the sample demographics of collected data.

B. Reliability and validity analysis

Before analyzing the research framework, reliability analysis was used to test the internal consistency of the questionnaire. Cronbach’s alpha is widely used measurement for internal consistency. For ensuring the reliability of the study, items were adapted based on acceptable cronbach’s alpha score above 0.60, based on standard values [17] [18]. Table IV represents cronbach’s alpha of the measured construct of research framework.

Table IV suggests that the internal consistencies of the measured constructs are acceptable for the study. The overall reliability assessment of the entire scale was observed good with a cronbach’s alpha of 0.825.

C. Model fit summary

Confirmatory factor analysis is used for the model fit of proposed framework. For structural equation model fit, various fit indices and tests has been developed. These indices and test, however can point to drawing conclusions about the extent to which a model actually matches the observed data or known as good model fit involving non experimental research. The following model fit indices are used to validate the model fit.

TABLE III. DEMOGRAPHICS OF RESPONDENTS

Profile	Items	Frequencies	Percentage
Gender	Male Female	189 56	77.1% 22.9%
Age	16-25 years 26-35 years 36-50 years	194 40 8	79.2% 16.3% 3.3%
Educational Qualification	Intermediate Graduate postgraduate	23 119 100	9.4% 48.6% 40.0%
Occupation	Student Govt. Sector Private Sector Professional	165 43 14 18	67.3% 17.6% 5.7% 7.3%

TABLE IV. CRONBACH’S ALPHA VALUES FOR MEASUREMENT MODEL

Construct	No. of items	Cronbach's alpha
Perceived privacy	4	82.6
Perceived security	4	78.5
Perceived trust	4	72.5
Information sharing	5	73.6

TABLE V. FIT INDICES FOR THE MEASUREMENT MODELS

Fit Indices	Recommended value	Measurement model
X^2		361.239
df (degree of freedom)		113
X^2/df	≤3	3.1
Goodness of fit index (GFI)	≥0.90	0.942

Adjusted goodness of fit indices (AGFI)	≥0.90	0.889
Comparative fit index (CFI)	≥0.90	0.91
Root mean square error of approximation (RMSEA)	≤0.08	0.076

1. X^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 V represents the model fit indices which satisfy their respective criterion 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 [19] [20] [21] represents a good model fit.

D. Structural paths and hypothesis test

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

Hypothesis H1 proposes that there is a positive relationship between perceived privacy and perceived trust (β=0.51; p<0.000), thus supporting hypothesis H1. This suggests that if user's have control over their information flow and protection of their profile privacy, then it increases their trust level in Facebook.

Hypothesis H2 proposes that there is a positive relationship between perceived security and perceived trust (*β*=0.25; p<0.000), thus supporting hypothesis H2. This suggests that if user's are provided with greater security while accessing their profile, then it increases their trust level.

Hypothesis H3 proposes that there is a positive relationship between perceived security and information sharing (*β*=0.22; p<0.000), thus supporting hypothesis H3. This suggests that if user's are provided with greater security level over Internet, then it leads the user's interest to share information in Facebook.

Hypothesis H4 proposes that there is a positive relationship between perceived privacy and information sharing (*β*=0.04; p<0.500), thus rejected hypothesis H4.

Hypothesis H5 proposes that there is a positive relationship between perceived trust and information sharing (β=0.25; p<0.000), thus supporting hypothesis H5. This suggest that if user's trust in the ability of Facebook, it will lead user's willingness to share information.

Thus we can conclude that perceived security, perceived privacy has a positive relationship with perceived trust in Facebook, are antecedent of perceived trust. Fig.2 and Table VI summarizes the result of hypothesis testing.

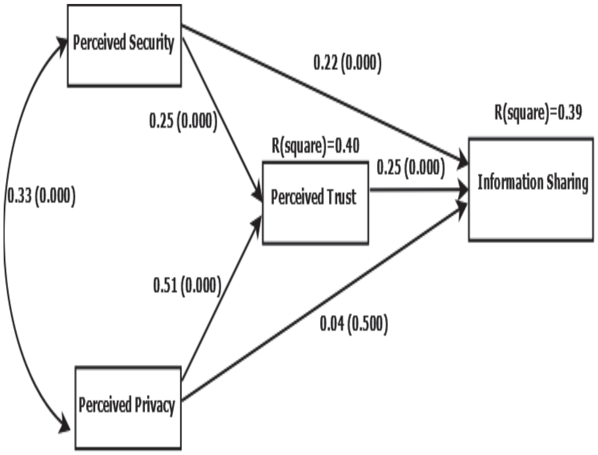

Fig. 2. Result of hypothesis testing

VI. DISCUSSION AND CONCLUSION

The primary objective of the study is to investigate the effect of user's privacy concern on usage behaviour as well as information sharing on social networking sites with reference to Facebook. Human behaviour concern has a crucial role in the deployment of social networking sites. Using extended TAM model, social exchange theory the proposed research framework is empirically tested. Our research findings suggest that user's having control over their information flow and protection of their profile is more likely trust in Facebook. Another factor that affected trust in Facebook was security features provided by Facebook and individual belief that accessing Facebook over Internet is secure. Further results suggest that perceived privacy and perceived security are antecedents of perceived trust; whereas, there is strong correlation between perceived privacy and perceived trust.

In terms of information sharing, when trust is exerted through privacy and trust it leads user's willingness to share information. Whereas privacy has no direct effect on sharing of

TABLE VI. SUMMARY OF HYPOTHESIS TESTS

Hypothesis	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	0.500	No
H5:Perceived Trust→ Information Sharing	0.25**	0.000	Yes

information, which is an interesting result of the study. It shows that trust in the ability of Facebook will lead a user's tendency to share more information.

Aside from theoretical values, the results have significant practical implications. The findings may provide social network operators a better understanding of how privacy concern may affect user's acceptance and information revelation with privacy concerns in social networking sites. This study gives a perception to operator for understanding user's sense of belonging for sharing information, user's privacy concern; which leads operator to develop and promote corresponding application to the user's.

There are certain limitations to this study. First; most of the research respondents were belonging to the age group of 16-35 years, which may not cover the general population of social networking sites user's. Second; social network user's belong different countries across the world having different cultures, different perception towards privacy concern, which potentially have different influences on usage behaviour.

VII. References

[1] Facebook, "News room." http://newsroom.fb.com/.

[2] T. Correa, A. W. Hinsley, and H. G. de Zúñiga, "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, 2010.

[3] K.-Y. Lin and H.-P. Lu, "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, 2011.

[4] R. Gross, A. Acquisti, and H. J. H. III, "Information revelation and privacy in online social networks," in WPES, pp. 71–80, 2005.

[5] B. Doerr, M. Fouz, and T. Friedrich, "Why rumors spread so quickly in social networks," Commun. ACM, vol. 55, no. 6, pp. 70–75, 2012.

[6] N. Mohamed and I. H. Ahmad, "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, 2012.

[7] danah boyd, "Facebook's privacy trainwreck exposure, invasion, and social convergence," The International Journal of Research into New Media Technologies, 2008.

[8] C. M. K. Cheung, P.-Y. Chiu, and M. K. O. Lee, "Online social networks: Why do students use facebook?," *Computers in Human behavior*, vol. 27, no. 4, pp. 1337–1343, 2011.

[9] S. Chai, S. Bagchi-Sen, C. Morrell, H. Rao, and S. Upadhyaya, "Internet and online information privacy: An exploratory study of preteens and early teens," Professional Communication, IEEE Transactions on, vol. 52, no. 2, pp. 167–182, 2009.

[10] D. Shin, "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, 2010.

[11] I. Ajzen, "The theory of planned behavior," Organizational behavior and human decision processes, vol. 50, no. 2, pp. 179– 211, 1991.

[12] N. M. Almadhoun, P. D. D. Dominic, and L. F. Woon, "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," in *ICCSCE*, pp. 426–431, 2011.

[13] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of facebook and myspace," in AMCIS, p. 339, 2007.

[14] R. Goettke and J. Christiana, "Privacy and online social networking websites," Computer Science 199r: Special Topics in Computer Science Computation and Society: Privacy and Technology, 2007.

[15] T. Govani and H. Pashley, "Student awareness of the privacy implications when using facebook," unpublished paper presented at the âAIJPrivacy Poster FairâAI at the Carnegie Mellon University School of Library and Information Science, vol. 9, 2005.

[16] D. Shin, "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, 2010.

[17] SPSS for Windows step by step: A simple guide and reference.

[18] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," Information Systems Research, vol. 17, no. 1, pp. 61–80, 2006.

[19] D. Iacobucci", ""structural equations modeling: Fit indices, sample size, and advanced topics"," "Journal of Consumer Psychology", vol. "20", no. "1", pp. "90 – 98", "2010".

[20] J. Scott, "The measurement of information systems effectiveness: evaluating a measuring instrument," ACM SIGMIS Database, vol. 26, no. 1, pp. 43–61, 1995.

[21] R. Bagozzi and Y. Yi, "On the evaluation of structural equation models," Journal of the academy of marketing science, vol. 16, no. 1, pp. 74–94, 1988.