Social Network Privacy and Trust Concerns

Maha Faisal
Kuwait University
Computer Engineering Department
P. O. Box 5969 Safat 13060 Kuwait
(965) 2498-7753
maha.faisal@ku.edu.kw

Asmaa Alsumait
Kuwait University
Computer Engineering Department
P. O. Box 5969 Safat 13060 Kuwait
(965) 2489-7652
alsumait@eng.kuniv.edu.kw

ABSTRACT
Social Network Sites (SNS) developed to provide means of interaction and/or data sharing between multiple users. The study of online SNS privacy and trust management has few empirical studies and needs to be examined in greater depth. This pilot study evaluates the privacy aspects, trust concerns, and attitudes of young Kuwaiti social network users as well as assesses how these behaviors map against privacy vulnerabilities inherent to social networking applications. This study employed a survey with 222 participants, examining five areas: social network usage, literacy, youth social behavior, and both privacy and trust concerns.

Categories and Subject Descriptors
J.4 [**Social and Behavioral Sciences**]: - *Sociology.* K4.3[**Computers and Society**]: Organizational Impacts – *Computer-supported collaborative work.*

General Terms
Management, Human Factors.

Keywords
Social Networks Sites, Trust, Privacy concerns

1. INTRODUCTION
Social networking sites (SNS) are virtual communities that have become tremendously popular over the past few years (Riefl, 2011). This growth has not come without a price, however. The SNS have been the target of specialized phishing attacks, profile impersonation, spam, and targeted malware dissemination. New threats will emerge as attackers grow in sophistication. Two main concerns arise with this type of networking: privacy and trust management.

Social networks have earned very little trust as communication platforms and are surrounded by deep concerns about privacy. For example, Krishnamurthy and Wills (2010) studied 13 online SNS. They found that each site leaked some private information to tracking sites and several of them passed users' locations to a third party. The trust landscape of a social network (who trusts whom) plays an important role in the security and privacy domains. Trust can reside in social relationships between two users or in multiple social relations within a group of people; user-level trust can be expanded to group-level trust if trust resides in social relations rather than in a single individuals (Park, 2006). However, SNS users sometimes hesitate to trust others, especially when there is the risk that others may take advantage of the users' profiles.

Busnel et al. (2010) discussed improving social networkers' trust in the reputation, privacy, and satisfaction provided by social networks. Zhou and Hwang (2007) constructed a trust overlay network (PowerTrust) to model the trust relationships among peers. Dustdar and Bhattacharya (2011) looked at integrating people, via human-based computing, and software services into one composite social network systems. Dong et al. (2011) proposed a secure friend discovery protocol for social networks. Zhan and Fang (2011) proposed a trust maximization algorithm based on the task-oriented social networks.

Many studies (Acquisti and Gross, 2006; Tufekci, 2008; Mohamed, 2010) argue that users place themselves at greater risk for cyber and physical stalking, identity theft, and surveillance when they disclose personal information on SNS. However, the reasons why users willingly disclose information on their profiles have not been sufficiently investigated. A study aimed at this question found three important factors influencing information revelation: future audiences, general privacy concerns, and gender (Tufekci, 2008). To further investigate trust and privacy in social networks, this study continues Tufekci's (2008) and Mohamed's (2010) lines of inquiry and investigates additional factors that could influence information revelation. Our study also expands on the current literature by examining social networkers' trust concerns and privacy protection strategies.

2. RESEARCH QUESTIONS AND METHODOLOGY

2.1 Description of the Survey Instrument
Several studies suggest that privacy and trust concerns in SNS vary across many factors. Age, gender, education, and culture are the most important factors that affect online privacy concerns among individuals (Mohamed, 2010; Krasnova et al., 2010; Krasnova and Veltri, 2010). In this study, we investigated online social network privacy concerns among Kuwaiti youth and their relationship to trust. In addition, we examined how online privacy concerns correlate to the protective behaviors people take to protect their online privacy. We created survey questions to capture perceptions of social aspects in SNS; general use of the sites, SNS literacy, trust and privacy concerns, information sharing, and the development of new relationships. These questions derive from qualitative studies (Josang et al., 2007; Tufekci, 2008; Dwyer et al., 2009; Ismail , 2010; Mohamed, 2010).

iiWAS2011, 5-7 December, 2011, Ho Chi Minh City, Vietnam.

2.2 Research Questions and Methodology

The objective of this study is to investigate the Kuwaiti youth behavior on SNS. We target Kuwaiti youth to investigate the following areas:

1. Social network usage: how is it utilized (e.g., socializing, education, advertising... etc.)
2. Social network literacy: how well youth know online interaction guidelines and privacy and online risks.
3. Social behavior, such as communication, identity, and participation.
4. Privacy related behavior and trust in SNS providers and SNS members.

2.3 Measure of SNS Usage

There are many concerns about SNS usage and the appropriateness of the activities on these sites. We must understand how youth represent themselves and the information they post. Though some preliminary research has been conducted regarding SNS usage, there has been no academic examination of these systems' use by Kuwaiti youth regarding the utility, ease of use, or the reasons for SNS use. In this study, we examined those aspects.

2.4 Measure of SNS Literacy

Social media and technology tools may come naturally to youth and are part of their day to day lives. Knowing how to use these tools, however, does not always mean that youth use them in smart ways. Understanding and managing the privacy statements of the SNS are important to SNS literacy and would aid in proper protection of user information. In this study, we examined the effect of social network literacy on information disclosure.

2.5 Social Behavior

In this study, we investigated whether there is a difference between offline and online friends, basing the investigation on the following questions: How different are the youths' social network habits than their real life? Do youth make sure that they really "know" their friends? Do youth behave differently online than they would offline? We predict that youth behave differently online than they would in real life.

2.6 Privacy Concerns

Privacy concerns are fears about opportunistic behavior related to one's personal information (Dinev and Hart, 2006). Researchers often examine the relationship between privacy and online behavior. Several studies indicated that users express strong concerns about the privacy of their personal information, but express fewer concerns about safeguarding it (Awad and Krishnan, 2006). We predict that users with high privacy concerns are more careful about the information they share. They have serious concerns about the use or abuse of their information.

2.7 Trust Concerns

Trust provides the feeling that a user will gain the expected benefits without suffering negative consequences (Pavlou, 2003; Sibel et al., 2010). It could be perceived as trust in SNS provider and trust in SNS members. In our study, we predict that the more the user trusts SNS, the more the user feels open to providing access to personal information on that website.

3. RESULTS

3.1 Participants

The final survey sample consisted of 222 participants with ages ranging from 13–35 years. Participation was voluntary. Data collection occurred between February and June 2011.

Overall, 58% of the participants were female, and 57% of the participants were undergraduate students at Kuwait University. A total of 59% had used social networks for more than four years, and 66% used WhatsApp, 53% used Twitter, and 52% used Facebook.

3.2 Social Network Usage

Online social networks active usage refers to how active people are with various features of online social networks (Mohamed, 2010). This variable was measured by asking participants two questions. The first question asked how many years the participant had been using SNS: 59% had used SNS more than 4 years; 28%, 1-3 years; and 15%, less than a year. The second question asked why the participant uses SNS: 84% believed it easier to contact friends; 59% thought it easier to contact family members; and 51% used SNS to learn new things. Overall, 80% used social networks daily, while 43% often spent more than three hours daily using SNS.

3.3 Social Network Literacy

Participants were asked to react to a number of statements regarding social network literacy in SNS. On a scale of 1 to 5, with 1 reflecting a level of strong disagreement with the statement and 5 reflecting strong agreement, the average responses and standard deviations are presented in Table 1.

Table 1: Participants' Social Network Literacy

SN Literacy	Average	SD
I read the privacy statements of SNS I participate in	3.2	1.6
I understand the privacy statements of SNS I participate in	3.3	1.4
I know how to control privacy in SNS.	3.6	1.5
I know SNS vulnerabilities.	3.3	1.4
I have good skills on evaluating identifying trusted content	3.4	1.3

3.4 Social Network Behavior

The survey examined social network participants' behavior in relationship establishment and online identity.

3.4.1 Relationship Establishment

Most participants primarily use online social networking to communicate with existing acquaintances: 69% established social ties online based on real life ties (relatives, friends). They also stated that SNS enabled easy connections with existing friends (74%). A significant number (44%) declared that they gained more friends through SNS. However, only 27% found SNS attractive for making new friends.

When establishing new relations online, participants usually had a cautious attitude: 67% of participants would check a person's profile before accepting a friend request. Also, they would not accept SNS friend requests from strangers (67%) and do not trust a person based on his/her online rating (48%).

3.4.2 Online Identity

Most participants sought to have both an online profile and activities that represent their true identity. Overall, 65% indicated that they never misrepresented their name, age, gender, appearance, and activities. However, 48% did not feel more confident online.

They also would rather maintain a positive online identity and refrain from actions that would damage this image. Overall, 58% think that it is difficult to discuss personal things online, and 61% do not share content on SNS that they do not want their family or teachers to see. In total, 72% were not embarrassed or disciplined after sharing something on a SNS. Additionally, 77% do not think being silly or rude online is fun.

Another significant aspect of online identity is the amount of information the participants disclosed on their SNS profiles. Participants were asked to report which of 15 salient elements (including name, gender, relationship status, e-mail address, and cellular phone number) they included on their SNS profile. These items offered insight into the amount of personal information that participants reveal on SNS. Interestingly, participants were very likely to post information such as a real name, birthday, gender, and e-mail address. Some were very likely to post pictures. Table 2 illustrates the percentage of information disclosure on the participants' profiles.

Table 2: Participants' Information Disclosure

Item	%	Item	%
Name	76%	Friend Network	24%
Email Address	59%	Interests/Hobbies	40%
Physical Address	10%	Job/Occupation	38%
Phone Number	14%	Favorite Music/Books	22%
Website	20%	Favorite TV Shows/Movies	26%
Gender	64%	Academic Status	46%
Birthday	63%	Photo	30%

3.5 Privacy Issues

This study, investigated the privacy concerns of SNS participants, their personal information exposure, and measures taken by SNS participants to protect their privacy.

3.5.1 Privacy concerns

Participants were presented with a series of statements describing privacy concerns. Participants provided a rating on a scale of 1 to 5, with 1 reflecting a level of strong disagreement with the statement and 5 reflecting a level of strong agreement.

The maximum score for this measure was 35 points. Participants were classified into three categories of privacy concerns: participants with a score of 26–35 points had high privacy concerns (19%), participants with 18–25 points had moderate privacy concerns (54%), and participants with low privacy concerns (27%) scored 17 or fewer points.

3.5.2 Degree of Exposure

When sharing profile information online, SNS participants may reveal their identity. The *degree of profile exposure* was measured based on two aspects: visibility (Who can see the information?) and sensitivity (What is shared? How sensitive is the information?).

To measure profile visibility, participants were asked to react to a number of statements regarding the people they allow to access their SNS profiles. A scale of 1 to 5, with 1 reflecting a level of strong disagreement with the statement and 5 reflecting strong agreement was used. Overall, 61% stated that they were "OK with family accessing my SNS profile." Additionally, 41% and 42% indicated that they were "OK with classmates accessing my SNS profile" and "OK with friends accessing my SNS profile", respectively. On the other hand, 64% would not allow strangers to access their SNS profile.

To measure profile sensitivity, the seventeen items revealed on participants' profiles were used to create an additive scale. Posting information regarding name, e-mail, address, phone number, website, gender, birthday, friend network, and photos were assigned 5 points each. Such profile items are considered sensitive because they can reveal the identity of the participant. Other items on the participants profile were assigned 1 point. The maximum score for this measure was 50 points. Participants were classified into three categories of information sensitivity: participants' profiles with a score of 21–50 points were highly sensitive (47%), participants' profiles with 16 – 20 points were moderately sensitive (23%), and participants' profiles with low sensitivity (30%) scored 15 or fewer points.

3.5.3 Protective actions

Participants were asked to rate the privacy protective actions they take on SNS by responding to a set of statements. A scale of 1 to 5, with 1 reflecting a level of strong disagreement with the statement and 5 reflecting strong agreement, was used. In total, 43% of the participants did not use privacy controls on SNS to hide specific content, while 26% did. Additionally 50% of the participants thought that it would be a good idea to have default privacy settings for youth and 26% did not. A total of 49% claimed that they adjusted their privacy settings regularly, while 17% did not. Participants provided neutral responses about enabling parents to contact a social networking site to access and delete content on their child's account, as well as restricting child use of SNS due to privacy concerns.

3.6 Trust Concerns

While the previous section focused on issues in disclosing private information, similar issues arise when consuming information. This variable was measured by asking participants to agree with some statements. Almost half of the participants trusted that SNS protected and did not use their personal information for any other purpose. Overall, 69% of the participants were likely to continue to share their identity information online. However, 41% of them did not believe that their identity information was well-protected from hackers. Additionally, 41% were concerned that SNS providers used their data and observed their activities, and 79% agreed that the presence of privacy policies gives a higher perception of trust. Finally, 75% of the participants believed that most profiles viewed on SNS were exaggerated to make the person look more appealing.

4. CONCLUSIONS

This study investigated the online social network usage of 222 Kuwaiti youth. It also examined privacy and trust concerns. Privacy concerns and trust enhancement are two important factors for user participation and information disclosure. Our study serves as a roadmap for SNS providers to invest their efforts and money into specific mechanisms to lower user privacy concerns, promote an atmosphere of trust, and thus increase user activity and network sustainability.

A number of key findings have been presented as a result of this study. As expected, a significant percentage of youth utilizes SNS. The younger the participants, the more they use SNS. Most

participants primarily use online social networking to communicate with their relatives and friends. Kuwaitis tend to protect their online privacy. The Kuwaiti and Arab cultures tend to be conservative and favor collective over individual interests, which may play a role in the observed tendencies of protecting personal information and privacy. However, the type of identity information that is disclosed in SNS is very interesting.

More than half of the participants reported knowing how to use privacy settings and adjusting these settings regularly. When participants know the consequences of information disclosure, they can more effectively manage SNS privacy settings. For SNS providers to make a virtual reality more compelling powerful than the actual one, they need to promote trust in SNS providers. Youth expressed that they cannot authenticate the identity of their conversation partners. They also seek to have positive online self-images.

Future work will involve determining the correlation between several variables investigated by this study, including privacy concerns and relation establishment in SNS, SNS literacy and information disclosure, SNS usage, and both privacy concerns and information disclosure.

5. ACKNOWLEDGMENTS

The authors would like to acknowledge the support by Kuwait University under a research grant no. EO03/11.

6. REFERENCES

[1] Acquisti, A. and Gross. R. **2006**. Imagined Communities: Awareness, Information Sharing and Privacy on The Facebook. In *Proceedings of the 6th Workshop on Privacy Enhancing Technologies*, Cambridge, UK, 2006.

[2] Busnel, Y., Serrano-Alvarado, P. Lamarre, P. **2010**.Trust your social network according to satisfaction, reputation and privacy. In *Proceedings of WRAS '10 the Third International Workshop on Reliability, Availability, and Security*. July 25-28, 2010,Zurich, Switzerland.

[3] Dong, W., Dave, V., Qiu, L. and Zhang, Y. **2011**. Secure Friend Discovery in Mobile Social Networks, In *Proceedings of the 30th IEEE International Conference on Computer Communications (Infocom 2011)*, Shanghai, China, April 2011**.**

[4] Dustdar, S., Bhattacharya K. **2011**. The Social Compute Unit, *IEEE Internet Computing*, 15(3). 64 - 69.

[5] Dwyer C., Hiltz S. R., Passerini K., **2007**, Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace, In *Proceedings of the Thirteenth Americas Conference on* Information *Systems,* Keystone, Colorado.

[6] Ismail S., **2010**, An Evaluation of Students' Identity-Sharing Behavior in Social Network Communities as Preparation for Knowledge Sharing, *International Journal for the Advancement of Science & Arts*, 2010, 1(1), 14-21.

[7] Josang, A.; Ismail, R.; Boyd, C. **2007**. A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems* 43 (2).

[8] Krishnamurthy, B. and Wills, C. E. **2010**. On the leakage of personally identifiable information via online social networks. *ACM SIGCOMM Computer Communications Review*, Jan. 2010.

[9] Lazzari, M. **2010**. An experiment on the weakness of reputation algorithms used in professional social networks: the case of Naymz", *Proceedings of the IADIS International Conference e-Society 2010*, Porto, Portugal, March 18-21, 519-522.

[10] Mohamed. A. **2010**. Online Privacy Concerns Among Social Networks' Users. *Cross-Cultural Communication*., 6(4), 74-89.

[11] Solove, D. J. **2007**. The Future of Reputation: Gossip, Rumor, and Privacy on the Internet. 2007 .

[12] Tufekci, Z. **2008**. Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology and Society. 28, 20 (2008), 20--36.

[13] Zhan, J. and Fang X. **2011**. Trust maximization in social networks. In *Proceedings of the 4th international conference on Social computing, behavioral-cultural modeling and prediction SBP'11*. 205-211.

[14] Zhou, R. and Hwang, K. 2007. PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing. IEEE Transactions on Parallel and Distributed Systems, 18(4), 460-473.