JOURNAL OF INFORMATION SYSTEMS RESEARCH AND INNOVATION
http://seminar.utmspace.edu.my/jisri/

Factors Influence Self-Disclosure Amount in Social Networking Sites (SNSs)

Ahmed Hussein Elmi[1]
e-mail: ahmedhussein56@gmail.com

Noorminshah A.Iahad [2]
e-mail: minshah@utm.my

Abdirahman Abdullahi Ahmed [3]
e-mail: lakari1@hotmail.com

Author(s) Contact Details:
[1, 2, 3] Faculty of Computer Science and Information Systems, Universiti Teknologi Malaysia, 81310, Skudai, Johor, Malaysia

Abstract — Social networking sites (SNSs) are increasingly used on daily basis. SNSs users connect each other via social networks' platform with shared interests and values based on other users' self-disclosed personal information. Generally, users would like personal information to be visible to only their families, close friends and not by unknown persons or strangers. There are some cases that users wish to reveal their information to strangers who are part of a network so in this case the information that disclosed may be visibly vulnerable for hacking. The range of these privacy risks from identity thieves to both physical stalking and online; and form embarrassment to price discrimination and blackmailing. Several researches identified an increasing privacy problem that exists within SNSs. Some studies have shown how easily strangers can extract personal data about users from the network. Other studies have found that an extremely small percentage of SNSs users change their permissive default privacy settings. In this paper, we propose a model of self-disclosure with six hypotheses, and we divided the model into two main categories: (a) hypotheses that have positively related to self-disclosure amount such as perceived enjoyment and ease of use, and (b) hypotheses which have negatively related to self-disclosure which mainly fall under privacy concerns such as perception of damage and likelihood. Our study established several important concepts: privacy concerns of SNSs users decrease online community self-disclosure; perceived enjoyment increases self-disclosure; SNSs providers trust increases self-disclosure; damage and likelihood beliefs decrease self-disclosure. Meanwhile, perceived ease of use increases self-disclosure.

Keywords – privacy; profile; self-disclosure; Facebook; security concerns

1. INTRODUCTION

Social Network is considered as one of the major technological phenomenon on Web 2.0, it has about hundreds of millions of participants. SNSs facilitate a form of self expression for users, and enables them to share content with other users [1]. The privacy management on social networks especially Facebook has attracted many researchers because the large amount of information that users disclose to the public as unintentional without knowing that most social networks' profile are publicly available and also without knowing how to use the privacy settings that is allowed to their users.

The emerging and growing SNSs make users feel vulnerable, they are encouraged to share more personal information while they are not aware that all participants can access their private data, apart from their friends. Marketing personnel can view and manipulate all users' data for advertising their products without taking permission from owner [2]. The danger of privacy information is believed to occur when user revealed identifiable information about themselves to online participants who are unaware of this transparency of online data. This is referred to user's lack of privacy awareness. Govani and Pashley investigated students' awareness of privacy concerns and the affordability provided by Facebook, so they found a large percentage of students are aware of possible effects of publishing identifiable information to among university community (e.g. Stalking, identify theft), despite feeling comfortable enough in posting their private information. Even if they know how to limit the visibility of their profile, yet they did not take any action to protect their personal information [3].

The hacking information from the internet increases from time to time, while a large number of community is joining social networks. Solution tools are unlikely to protect user's data because every digital wall created has been destroyed by new technology. Expectation of misusing information published on SNSs had increased. Profile on Facebook and Myspace are used by law enforcement and workers for investigation into user's personal background. As a result, this put users in danger for physical or online attack. Furthermore, the available technology in social networks such as face recognition, in this case profile can be connected across community or may be linked with other database so this is decreasing the privacy of anonymous data. Because of cheap storage and increasingly intelligent search capabilities, information may be archived for continued accessibility, putting participants at risk indefinitely. In spite of the risks, privacy mechanisms are very weak and not encouraging for the community to join SNSs. In addition, the level of awareness of active users is poor, and they don't put emphasis in protecting their profile. Study has found several explanations for this such as poor interface design and permissive default settings, social conformance, and inherent confidence in the online community [4].The owners of social network sites have to build a new type of privacy mechanisms as responding users' requirements for saving information. There is no detailed data about attackers, the privacy features must do with confidence, vectors of behavior and reputation. One of the best solutions is to raise the awareness of users about the risk of lack concern of privacy setting in SNSs [5]. The aim of this paper is to discuss the factors that impact self-disclosure amount in the SNSs and also to propose self-disclosure model.

2. RELATED WORK

A. Privacy and security concerns

Research has shown that majority SNSs users are not concerned about security and privacy issues. One of the reasons for disconcerned users is they are not aware of actual viewers of their information [5]. The relation between use SNSs and privacy concern is not clear. Generally, users would like personal information to be visible to only their families, close friends and not by unknown persons or strangers. There are some cases that users wish to reveal their information to strangers who are part of network, so in this case the information that is disclosed may be helpful to other users and companies and even third parties, this valuable information provides data sources and data mining [6]. Research found that users of the internet are usually concerned about unwanted person who will retrieve their private information.

The study was conducted by Fox et al. found that 86 percent of Internet users worried that unwanted viewers will access information about them or their relatives and families, 70 percent are afraid that hackers will surf their credit card information, and 60 percent are anxious that someone will obtain private information from their online activities [7]. Similar results were found by Acquisti and Gross, the result showed that the level of students' concern about privacy matters on Facebook such as unknown person obtain where they stay, location and schedule of their class as well as political affiliation. Although these worries, study has shown that participants in SNSs tend to disclose information and often exact private information in online community [8]. Other research has examined that information sharing and privacy on SNSs that 89 percent of users display their full name on their profile, while 87.7 percent have disclosed their birth date and 50.8 percent have exposed their current address. Tufekci investigated that concern about strangers had an influence on whether or not users disclosed their actual name in MySpace and whether or not participants revealed their religious affiliation on Facebook and MySpace [9]. Thus, maybe there is a relationship between an individual's concern about unwanted audiences suffering his or her profile and the amount and kinds of information he or she prefers to disclose on Facebook. Three main parties connect with another in SNSs: the SNS service provider, the users, and third party application.

B. Privacy settings on Facebook

If a user has valid e-mail address, one can easily register on Facebook. The user has opportunity to set his privacy settings as he wishes. If students use similar application, they will be able to access parts of profiles which are viewable to everyone from each other. Thus, it is essential for students to be aware of the importance of privacy settings. Even if students who use Facebook are not friends anymore, they still can view profiles of one another if the settings of their profiles are public. Besides that, the user's personal information is also viewable without knowing personally the owner. In the last years, the default privacy settings of Facebook have been changing quite frequently and it has been opening more and more parts of the profile in their default [11].

C. Awareness of Facebook profile visibility

By default, everyone on the Facebook appears in searches of everyone else, as well as every profile at specific institution can be accessed by every user of Facebook at that institution. Though Facebook allows an extensive privacy policy and provides very granular control to users to select what information to disclose to whom. As mentioned above, relative to a Facebook member, other users can either be friends, friends of friends, non-friend users at the same institution, non-friend users at a different institution, and non-friend users at the same geographical location as the user but at a different university (for example, Harvard vs. MIT).

Users can choose their profile visibility (who has ability to read the profile) and searchability (who can get the profile through search) by type of users. More customization privacy control is given to contact sensitive information such as address and phone number. Research has shown 30% of Facebook users claim they are not aware whether Facebook offers ways to control visibility and searchability of their profile. According to the study 18 percent do not know whether Facebook provides any way to manage who can really view their profile [8].

D. Types and Amounts of personal information disclosed

Researchers have focused on concerns about undergraduate and teenagers safety on the internet generally and specially on SNSs. SNSs privacy problems can stem from the interplay three factors, which include what type of SNSs security capabilities are provided, what personally identifiable information of SNSs users disclose, and what particular end user data on SNSs is sought out and used by third parties. For instance, students consciously and unconsciously reveal their information to people they do not know and actually would not trust to access to that information they made available, and maybe this information being used unexpected and a harmful way. There are many recorded cases of SNSs accessed by marketing organizations, employers, university officials, and others, resulting in difficulties for students who disclosed information without looking the consequences.

Research survey conducted in 2008 by EDUCAUSE Centre for Applied Research (ECAR) investigated information revelation issues by asking students who use social networks on what access limitation they place on their profile. They also inquired to what extent students are concerned of their profile's security and privacy. This survey found that, it is common for all age groups to include their personal photos and first name in their profile. Among SNSs participants 18 to 24 years old, around 80% include their profile to their last name, E-mail address and hand phone number. Among SNSs users who their age above 24 years, only half of them reveal their last name and E-mail address. Few older students make available to their date of birth while more than half of internet generation respondents do so [12].

3. METHODOLOGY

This paper is specifically devoted to search and review the literature on how the privacy of SNSs and self-disclosure models are perceived and reported by researchers in online social network. Following, the researchers employed a three-stage method to extract, analyze and report the literature-based findings. The first stage involved identifying the articles to be included in this review. The second stage involved designing and executing a detailed protocol that prescribed how to capture and analyze the data. The third stage entailed synthesizing the analyzed details and deriving the research findings.

In identifying the articles to be included in this review, leading social networks security and self-disclosure journals and academic conferences were considered. The total of papers that researchers reviewed were 28 papers. Paper extraction occurred in two steps. In the first step, the focus was on extracting papers that include self-disclosure issues and models. In the second step, the focus was extracting papers that address privacy on SNSs. The protocol that researchers followed was to create a folder for papers and then sorting topics as similarities, this ease in finding different issues of privacy management on SNSs as well extracting different ideas from different authors. Finally the authors succeeded to compare several models of self-disclosure and this led to construct and propose a research model as well as to elicit literature review of this study.

After comparing different models of self-disclosure, the authors found that some important factors of self-disclosure are not included into these models. So the proposed model is considered complementary of the previous self-disclosure models.

4. SELF-DISCLOSURE MODELS

The authors selected the two models below because they are very close to the research model. The first model addresses factors that impact self-disclosure amount which are perceived ease of use, perceived trust and perceived enjoyment, these factors are self-disclosure contributors, while other factors in the model are self-disclosure inhibitors such as perceived damage and perceived likelihood which fall under privacy concerns. The second model states that self-disclosure behavior, it is affected by self-disclosure intention which also has a positive relation to perceived ease of use and perceived usefulness. The authors adapted most constructors of the research model from both the two models; therefore we included those models in our paper.

A. Self-disclosure Model (1)

The following model describes self-disclosure amount and factors that impact to it. There are two types of hypotheses that are related to self-disclosure amount. One of the hypotheses positively brings to reveal information among SNSs users which is known perceived enjoyment, while other hypotheses of the model do not contribute to reveal personal data inside an online social community. The inhibitor factor is privacy concern, which is mainly influenced by the other two factors which are perceived likelihood and perceived damage.

In a Structural Equation Model with 237 respondents, the researchers found that Perceived Enjoyment and Privacy Concerns to be significant determinants of information revelation. The researchers confirm that the privacy concerns of SNSs users are primarily determined by the perceived likelihood of a privacy violation and much less by the expected damage. These insights provide a solid basis for SNSs providers and policy-makers in their effort to ensure healthy disclosure levels that are based on objective rationale rather than subjective misconceptions [13].

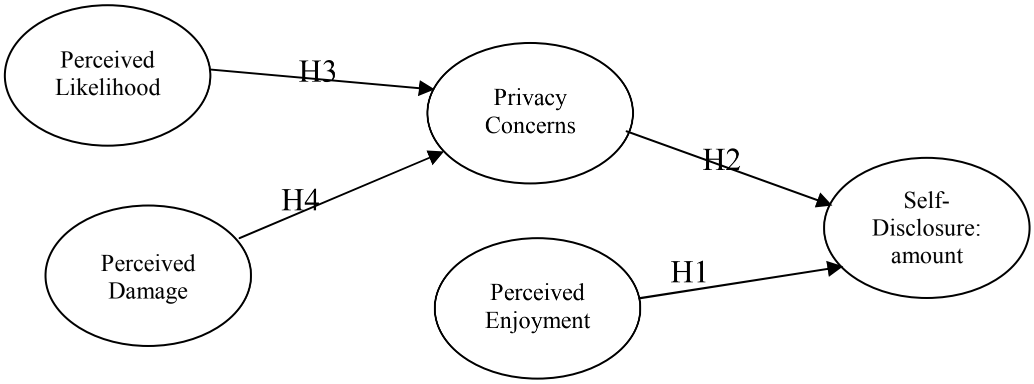

FIGURE 1: Self-disclosure model (1) [13].

B. *Self-disclosure Model (2)*

This model relates users' self-disclosure intentions and self-disclosure behaviors to certain characteristics of SNSs based on Technology Acceptance Model (TAM). This model is empirically tested through an online survey of 113 users in the context of Renren, the most popular SNSs in China, and the researchers found that users' perceived usefulness and perceived ease of use of a SNS closely associate with their self-disclosure intentions, which further leads to users' actual self-disclosure behaviors. The hypotheses of the model are:

H1: Perceived ease of use of a SNS positively affects perceived usefulness of the site.
H2: Users' perceived usefulness of a SNS positively affects users' self-disclosure intentions
H3: Users' perceived ease of use of a SNS positively affects users' self-disclosure intentions.
H4: Users' self-disclosure intentions positively affect their self-disclosure behaviors [14].

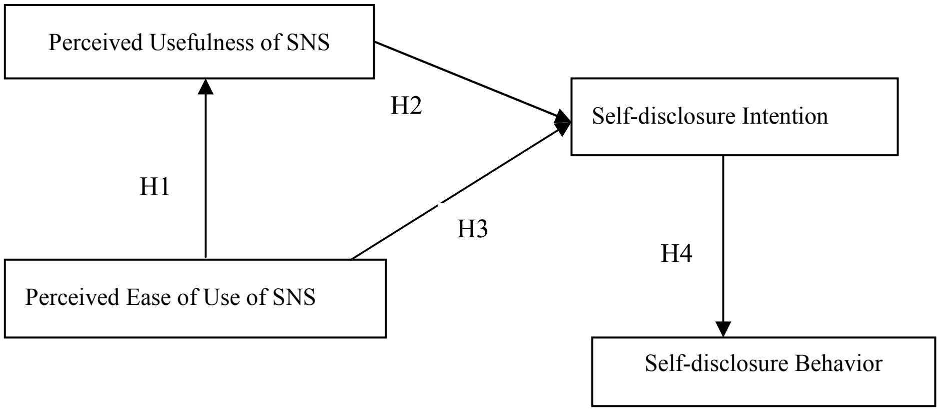
Perceived Usefulness of SNS
H2
Self-disclosure Intention
H1
H3
H4
Perceived Ease of Use of SNS
Self-disclosure Behavior

FIGURE 2: Self-disclosure model (2) [14].

5. CRITICAL REVIEW ON PREVIOUS MODELS

The closer self-disclosure model to the proposed model missed important factors that lead to self disclosure in SNSs. This model has two types of factors, self-disclosure contributors and inhibitors. The model focused only on one factor as contributor to self-disclosure which is perceived enjoyment while main self-disclosure inhibitor factor in the model is privacy concern which influenced by the two other factors; perceived damage and perceived likelihood.

The authors ignored the importance of perceived trust in self-disclosure amount. Research has found that trust beliefs regarded counter balance the negative influence of privacy concerns of self-disclosure [15]. The trust factor plays essential role in disclosing personal information to SNSs. Mayer et al. define trust as "the willingness of a party to be vulnerable to the actions of another party" [16]. Thus, users might rely on the SNSs providers not to abuse their information for its personal gain. Beyond anticipated benefits, Dwyer et al. argue that trusting beliefs may also counter-balance the negative influence of privacy concerns [17].

Other studies exposed that perceived ease of use impact online trust in general online communication [18]. Perceived ease of use is defined as: "the degree to which a person believes that using a particular system would be free of effort" [19]. Perceived ease of use is key deriving to social network acceptance [14].

In order to formulate self-disclosure model, it must have the important factors that impact self-disclosure in SNSs either inhibitors or contributors. The most significant factors that the closer self-disclosure model to the research model missed are perceived trust and perceived ease of use based on the review above. The researchers included these factors to that model and intended to know their influence to self-disclosure amount with the other factors that previous model discussed.

TABLE 1: Summary of reviewed papers of the critical review on previous models

Author(s)	Title of the paper
Krasnova, 2009	Self-Disclosure in Online Social Networks
Mayer et al. ,1995	An integrative model of organizational trust
Dwyer et al., 2007	Trust and privacy concern within social networking sites
Corritore et al., 2003	On-line trust: concepts, evolving themes, a model
Davis, 1989	Perceived ease of use, and user acceptance of information technology
Yanli et al., 2010	Effects of System Characteristics on Users' Self-Disclosure in Social Networking Sites

6. PROPOSED MODEL

The proposed conceptual model consists of six hypotheses and the aim of forming this model is to better understand the revelation issues and self-disclosure in SNSs. Perceived ease of use, perceived enjoyment and perceived trust are related directly to the self-disclosure amount. Users tend to reveal much information about them when they believe using SNSs are ease as well when they feel enjoyment and also trust in SNSs providers, this encourages users to share sensitive information with other users because they believe the owners of SNSs will protect and not give third parties to their information and users believe SNSs providers continue to provide efficient service. If a person has privacy concerns, they are more likely to keep their information and not give it to strangers and unwanted persons.

Rooted in the study of verbal communication, self-disclosure has been referred to as the "process of making the self known to others" ([14]. Self-disclosure is the process of revealing personal information about oneself verbally to another or others. Self-disclosure of intimate information is based on trust. Because disclosing intimate information about oneself puts that individual in a vulnerable position, people tend to disclose to trusted partners [20]. Given self-disclosure plays such an integral role in relationship formation and development, it is a particularly relevant issue in the context of SNSs. SNS self-disclosure is any message, or information about the self that a person communicates within the site. The creation of an online identity, or profile, is a feature found in all SNSs [21]. Creating profiles, users are asked to disclose information, such as their name, e-mail address, gender, and date of birth. Provision of personal and contact information is often encouraged, and the information is subsequently displayed prominently on the site [22].

Self-disclosing on an SNS brings joy to the person who discloses and their network friends, the risk of disclosing potentially damaging information is large. There are factors that influence self-disclosure in SNSs, such as trusting to SNSs providers, enjoyment for participating online community and perception of ease of use. These factors are effectively contributing users' self- disclosure. There are other factors that preventing revelation in online community such as perceiving damage if the participant disseminated personal information e.g. (phone number, photo, location, affiliation).

A. Privacy Concerns

As discussed, the impact of privacy concerns on self-disclosure has been studied thoroughly within the online context. Hogben mentioned that SNSs privacy risks range from organizational threats such as e.g. digital dossier aggregation by the third parties to dangers stemming from the user social environment such as online stalking, bullying or reputation slander [23]. Driven by media coverage, users are becoming increasingly aware of the privacy risks they face on the platform. In the light of daunting privacy concerns restriction of the amount of self-disclosure appears to be the most natural response. Privacy concern is concerns about opportunistic behavior related to one's personal information [24].

Westin defined privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” [25]. Privacy Concerns as a product of two variables: perceived likelihood of an event and perceived damage if the event takes place [13].

We hypothesize that:
Hypothesis 1: Privacy Concerns are negatively related to Self-disclosure.

B. Perceived Likelihood

The construct of perceived likelihood represents the subjective probability that a negative event will take place and corresponds to the notion of “susceptibility” used in the Health Belief Model often applied to predict the degree of the preventive behavior. Arguments show that users are likely to misjudge the likelihood of privacy abuse happening to them. Aiming to understand the role of perceived likelihood in the formation of risk perceptions we integrate it as a direct antecedent of individual privacy concerns in this model [26].

We hypothesize that:
Hypothesis 2: Perceived likelihood of privacy threats is positively related to Privacy Concerns.

C. Perceived Damage

Beyond financial loss as a result of e.g. identity theft, possible damage arising from participation in SNSs can be attributed to negative psychological and social consequences such as detrimental impact on one’s sense of worth, social standing and relations, or employment. It is important to note that the perception of damage highly depends on personality and cultural context [13]. The expected magnitude of the damage resulting from such negative events as, for example, access to personal information by the potential employer will be an important element contributing to individual privacy concerns.

We hypothesize that:
Hypothesis 3: Perceived damage from privacy threats is positively related to Privacy Concerns.

D. Perceived Enjoyment

Perceived enjoyment is affective cognition that one’s SNS use behavior is enjoyable in its own right apart from any anticipated personal gain or performance related outcomes [24]. Rosen and Sherman propose a modified technology acceptance Model (TAM), in which perceived usefulness is substituted by perceived enjoyment arguing that SNSs can be described as hedonic information systems with enjoyment constituting their primary value. Similarly, Sledgianowski and ulviwat have found Playfulness to be the strongest predictor of SNS intentional and actual use [13]. Hogben mentioned a sense of connectedness, self-enhancement, and possibility to interact and share experiences with like-minded individuals as possible benefits of SNSs. Recognizing presence of numerous gratification elements SNSs provide, it is considered enjoyment to be their central benefit [23]. Indeed, SNSs, such as Facebook or MySpace, are organized and presented in a way that enables pleasurable user experiences so that users participate and (self-) communicate more [13].

We hypothesize that:
Hypothesis 4: Perceived enjoyment benefits are positively related to Self-disclosure.

E. Perceived ease of use

Perceived ease of use is defined as: “the degree to which the prospective user expects the target system to be free of effort” [19]. Mayer et al. define trust as “the willingness of a party to be vulnerable to the actions of another party”. Thus, users might rely on the SNS provider not to abuse their information for its personal gain [16]. Technology Acceptance Model (TAM) originated from Theory of Reasoned Action (TRA), and can be regarded as a special case of TRA with only two salient beliefs: perceived ease of use and perceived usefulness. The predictive power of perceived ease of use and perceived usefulness for users’ technology acceptance has been empirically confirmed by numerous studies. Specifically, users’ perceived ease of use enhances their perceived usefulness and both constructs significantly improve users’ intention to accept the technology [14].

We hypothesize that:
Hypothesis 5: Perceived ease of use is positively related to Self-disclosure

F. Perceived Trust in social network providers

The trust factor plays an important role in revealing private information to social network providers. Trust can be defined as the willingness to accept a vulnerable situation based on a positive expectation regarding the actions of others [27]. Thus, users might rely on the SNS provider not to abuse their information for its personal gain. The context of trust has two dimensions. First, SNS members trust other community members not to misuse the thoughts, life experiences and other sensitive information that they share. Second, individual SNS members trust the providers of these sites to secure their personal data [28]. In this study, it was selected only in exploring the trust of SNSs users to SNSs providers. Perceptions regarding trust are often integrated into models based on PC rationale. Viewing trust as a facilitator of communication, Dwyer et al. conceptualize trust in provider and trust in members as direct determinants of information sharing on SNSs. Users' trust of social network providers lead to share more information about users without feeling any danger and consequence that can possibly occur. Hence, perceived trust is usually related to self disclosure [26].

We hypothesize that:
Hypothesis 6: Perceived trust is positively related to self-disclosure.

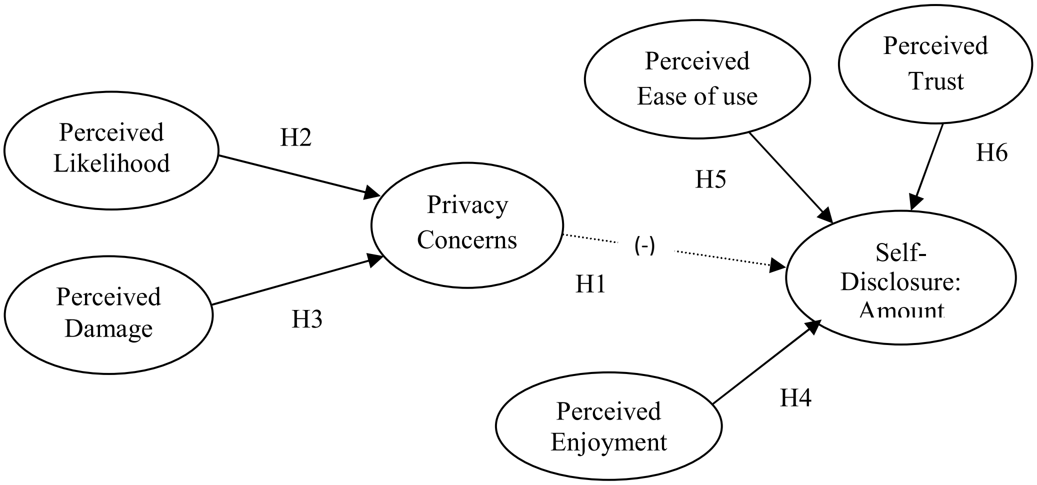

FIGURE 3: Research model

7. CONCLUSION

SNS provides its users with a chance to share information. Along with the benefits of making it easier to keep in touch and find out about others more easily, there are risks and concerns with sharing information with large amounts of people. The paper discusses the factors that impact on users of SNSs according to privacy awareness. There are many factors that influence and lead users to reveal and post too much information on SNS's platform such as perception of ease of use , perceived trust in SNSs providers as well as perceived enjoyment where other factors are negatively related to self-disclosure such as perceived damage and perceived likelihood. In this study, we discussed self-disclosure and the factors that lead users of SNSs to reveal important information. We discussed self-disclosure model which consists six hypotheses where some of them inhibit self-disclosure amount and other hypotheses contribute to self-disclosure such as perceived trust. In this study we looked only one side of perceived trust which is mainly focusing providers of SNSs. So, it is needed for further research which deeply studies the perceived online community trust and study how users' trust to the other online community.

REFERENCES

[1] Anna C, S., Mohamed, S. & Federica, P. (2009). Collective Privacy Management in Social Networks.
[2] Zorica, M. B., Biskupic, I. O., Ivanjko, T. & Spiranec, S. (2011) Students and Privacy in the Networked Environment. Mipro, 2011 Proceedings Of The 34th International Convention, 23-27 May 2011. 1090-1094.

[3] Govani, T. & Pashley, H. (2005). Student Awareness of the Privacy Implications When Using Facebook. Unpublished Paper Presented At The "Privacy Poster Fair" at the Carnegie Mellon University School Of Library And Information Science, 9.

[4] Katherine, S. & Heather, R., Lipford. (2008). Strategies and Struggles With Privacy in an Online Social Networking Community.

[5] Nagy, J. & Pecho, P. Social. (2009) Networks Security. Emerging Security Information, Systems and Technologies, 2009. Securware '09. Third International Conference on, 18-23 June 2009. 321-325.

[6] Xi, C., & Shuo, S. (2009). A Literature Review of Privacy Research on Social Network Sites. Paper Presented at The Multimedia Information Networking and Security, 2009. Mines '09.

[7] Fox, S., Rainie, L., Horrigan, J., Lenhart, A., Spooner, T. & Carter, C. (2000). Trust and Privacy Online: Why Americans Want to Rewrite the Rules, Pew Internet and American Life Project.

[8] Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on The Facebook.

[9] Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. Bulletin of Science, Technology & Society, 28, 20-36.

[10] Alyson L. Young, A. L. (2009). Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook. . In Proceedings of the Fourth International Conference on Communities and Technologies (Pp. 265–274), New York.

[11] Nemec, L., Holbl, M., Burkeljca, J. & Welzer, T. (2011). Facebook as a Teaching Tool. Eaeeie Annual Conference (Eaeeie), 2011 Proceedings of the 22nd, 13-15 June 2011. 1-4.

[12] Ecar. 2008. Social Networking Sites.

[13] Hanna, K., Elena, K. & Oliver, G. (2009). "It Won't Happen To Me!": Self-Disclosure in Online Social Networks. Americas Conference on Information Systems. Association for Information Systems.

[14] Yanli, J., Yi, Z. & Yuli, L. Effects of System Characteristics on Users' Self-Disclosure in Social Networking Sites. Information Technology: New Generations (Itng), 2010 Seventh International Conference on, 12-14 April 2010. 529-533.

[15] Krasnova, H. (2009). "It Won't Happen To Me!": Self-Disclosure In Online Social Networks. Paper Presented at the Amcis 2009 Proceedings.

[16] Mayer, R. C., Davis, J. H. & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. Academy of Management Review, 709-734.

[17] 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 Amcis, 2007. 1-12.

[18] Corritore, C. L., Kracher, B. & Wiedenbeck, S. (2003). On-Line Trust: Concepts, Evolving Themes, a Model. Int. J. Hum. -Comput. Stud., 58, 737-758.

[19] Davis, F. D. (1989). Perceived Usefulness, Perceived Ease Of Use, and User Acceptance of Information Technology. Mis Quarterly, 319-340.

[20] Sheldon, P. (2009). "I'll Poke You. You'll Poke Me!" Self-Disclosure, Social Attraction, Predictability and Trust as Important Predictors of Facebook Relationships . Cyberpsychology: Journal of Psychosocial Research on Cyberspace.

[21] Boyd, D. M., & Ellison, N. B. (2007). Sns: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13 (1), 210-230.

[22] Jacqueline, C. P., Patrick, J. B. & Brian, S. B. (2009). I Didn't Know You Could See That: The Effect Of Social Networking Environment Characteristics on Publicness And Self-Disclosure. Proceedings of the Fifteenth Americas Conference On Information Systems, San Francisco, California August 6th-9th 2009, 2009.

[23] Hogben, G. (2007). Security Issues and Recommendations For Online Social Networks, Position Paper. Enisa, European Network and Information Security Agency.

[24] Harrison, M., Nancy, L. & Tripp, J. (2011). Social Networking Information Disclosure And Continuance Intention: A Disconnect. The 44th Hawaii International Conference on System Sciences.

[25] Westin, A. F. (1968). Privacy and Freedom. Washington and Lee Law Review, 25, 166.

[26] Hanna, K. & Natasha, F. V. (2010). Privacy Calculus on Social Networking Sites: Explorative Evidence From Germany And USA. Proceedings of the 43rd Hawaii International Conference on System Sciences.

[27] Mesch, G. S. (2012). Is Online Trust And Trust In Social Institutions Associated With Online Disclosure Of Identifiable Information Online? Computers In Human Behavior, 28, 1471-1477.

[28] Michel, W., Ini, V. & Wannes, H. (2012). Connecting and Protecting? Comparing Predictors of Self-Disclosure and Privacy Settings Use Between Adolescents and Adults. Journal of Psychosocial Research on Cyberspace.