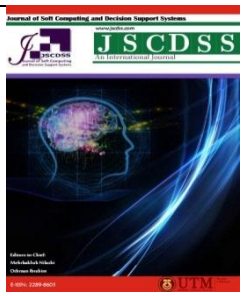
An International Journal
JSCDSS
http://www.jscdss.com
Vol.2 No.3 June 2015: 1-8
Article history:
Accepted 4 April 2015
Published online 5 April 2015

Journal of Soft Computing and Decision Support Systems



E-ISSN: 2289-8603

The Security Awareness Framework for Social Network Sites Facebook: Case Study in Universiti Teknologi Malaysia

Awil Ahmed Mohamed [a,*], Othman Ibrahim [a], Mehrbakhsh Nilashi [a]
[a] Faculty of Computing, Universiti Technologi Malaysia, 81310 Skudai, Johor, Malaysia

*** Corresponding author email address**: cawil_indho@hotmail.com

Abstract

Social networking sites are web-based services that enable users to create public or semi-public profile in a bounded system. Facebook is one of the largest and most populated prototypes of social network sites. The security management on Facebook has been important and there are many concerns raised about the amount of personal information disclosed to Facebook users, and how Facebook violates the weaknesses of users' Facebook privacy awareness. In addition, there is a little awareness for employing continuous privacy mechanisms amid active users of Facebook. Hence, this study examines Facebook usage and information disclosure, friends' requests and friends' responding, users' awareness of privacy settings and usage of privacy setting applications. The study also investigates the security awareness factors that impact Facebook users. Accordingly, a conceptual framework is proposed which includes three interrelated components consisting of the users' privacy awareness, Facebook privacy settings and the users' self-disclosure. This study uses the data analysis method called quantitative data analysis and a questionnaire is used for data collection from the respondents. After the data collection and data analyses, the findings of this study demonstrated that the majority of the respondents disclose massive amounts of individual information including basic personal private details, background information and contact details. The findings also revealed that most of the users are not interested to read the privacy policy and terms of service because they are long and complicated to read. Finally, the study put forward Facebook's privacy conceptual framework and effective guiding principles that will assist the users when interacting with Facebook privacy application features.

Keywords: Social networking sites, Privacy awareness, Security

1. Introduction

Social Networking sites are web-based services that enable users to create public profile in a surrounded system. It permits a user to communicate with other users to whom they share a links in a relation and navigate their list of connections that is made by others by those inside the system (Ellison, 2007).

Social web is believed as one of the main technical phenomenon on Web 2.0 that is connected with thousands of millions of participants. Social networking sites enable a form of self-expression for users, and enable them to share contents in conjunction with supplementary users (Squicciarini et al., 2009).

In current years, online social networking areas have undergone an increase, in regards to both the type and numbers of sites have increased as well as membership. Social networking sites, such as MySpace.com and Facebook.com persuaded nearly 110 million and sixty million active users, respectively. The advantage of the sites is that they institute confidential connections in both with friends knowing offline and those known only virtually, this aids friends to express opinions, political views, and education as well as experiences (Katherine and Heather, 2008).

The earliest identifiable social network started in 1997. The SixDegrees.com allowed users to create profiles and catalog their friends. These structures exited in some form before SixDegrees.com as students in high school or college associated via classmates.com. They allowed students to surf the web and connect with others, but users were not able to craft profiles or catalog friends until later. SixDegrees.com was the earliest social networking sites embedded these features. It therefore had many of the users, but it was ultimately, and the services ended.

MySpace, Friendster and Facebook are believed to be three key communal websites that have shaped business, research landscapes and culture. Friendster dispatched in 2002, it was projected to aid encounters of friends of friends and even facilitate to romantic friendships. MySpace added features according to users' appeal and permitted them to personalize their pages. The user did not stop the forms and added Hypertext Markup Language (HTML) to ensnare their profiles. Thus, the copy/past option was obtainable to construct special layouts and MySpace backgrounds.

Facebook is one of the most extensively utilized social websites as it has acquired 750 million users globally and has many more users from African and Asian countries than Friendster or MySpace. The security settings of Facebook, that were introduced in February 2004 by Mark Zuckerberg with his three classmates (Boyd and Ellison, 2007), that have manipulated in shared assure in present time. The number of people joining and using Facebook has increase with the ability of a large amount of personal information that is publicly available.

The security management on social networking websites particularly in that of Facebook has allured many researchers because of the colossal amount of information that users reveal to the public. This is due to an unintentional lack of knowledge that most collective networks' profiles are openly accessible and also because many users are not aware of how to use the privacy settings that social websites permit to their users (Tuunainen et al., 2009).

This research will focus on the ideal security awareness ideal for SNSs with a particular focused on Facebook and the factors that strengthen it. This study will display the danger of revealing sensitive information as users post and share personal information in SNSs. The real security dangers are believed to transpire after users expose identifiable information concerning themselves to online users who they do not know. This is because of user's lack of security awareness (Tuunainen et al., 2009).

1.1 Research background

Facebook was transmitted in 2004 by Harvard University undergraduate Mark Zuckerberg. It started as a forum for students to contact one another college campuses, at that period, 85% of undergraduate students in the U.S supported a profile and the number of participants increased daily. Facebook is open, and everyone can create their own profile (Katherine and Heather, 2008).

Facebook users have increased quickly in last five years, and surprisingly they unintentionally reveal to the public their confidential information, such as phone number, location, e-mail address and so on (Katherine and Heather, 2008).

Security settings on Facebook are openly visible, and many studies have shown that a large number of users do not care that their security settings are easily manipulated by strangers (Zorica et al., 2011). It is vital to effeciently protect users' security in SNSs. Several security protections have been provided to save information amongs Facebook users, such as shady, which is projected to safeguard messages transactions.

There are three main factors that destabilized the security of Facebook, which are (Yan et al., 2010):

- Users are too openly recognized.
- Facebook proprietors floundered to care and protect the users' security and privacy.
- There is one extra party that is actively pursuing and hunting for users' information by using Facebook.

Another vital factor that has harmed Facebook security settings is a particular search engine that some system developers call "public search" and others call "people search". Separate from the public search engine Facebook has supplementary security disclosure features (for instance, newsfeed, people you may know and counselling friends to reinforce the issue of Facebook security settings).

Facebook users go above the security settings and make everything public in terms of the default settings of the system, many users are on the brink of submissive to dangers such as harassment, solicitation, and cyber-bullying. Some users experience denigration as a result of others creating precise accounts to intimidate specific people by tagging and posting inaccurate information concerning supplementary users in order to enhance and damage their friendship or dignity. Impersonation is additionally used to manipulate other revealing their security information and images in online SNSs. (Dhami, Agarwal et al., 2013).

Typically, Facebook users like the youth have a tendency of using Facebook to flirt or to inappropriately converse with one another. They also use Facebook to make connect with other members of the social network and ultimately spend a significant amount of time on SNSs. These young people are accustomed to converse to their friends, plan engagements, and participate in social activities via the internet, but they are likely to expose intimate features of information in these open mutual web sites and are less likely to apply privacy protective behaviors. To understand the unenthusiastic workers vanishing on Facebook mass media, it is vital that users predominantly students have a conscious awareness of these issues before and after joining the SNSs. Users of the SNSs like Facebook are less responsive to the SNSs security settings even if they have been provide with advanced security settings applications.

Therefore, the main focus of this research is to recognize factors that impact the security awareness framework in users of Facebook. Furthermore, this thesis discovery aims to expose those factors most affect students in terms of security. This will consist of contrasting levels of security awareness amid postgraduate and undergraduate students in order to understand if there is a momentous difference in levels of security awareness established in levels of study.

1.2 Problem statement

Social networking sites have arisen to global mainstream attention as membership has increased dramatically. Users of SNS allocate large amount security information, encompassing profiles, political views, photographs, and entertainment with their offline or online friends.

SNS users are revealing confidential information while lacking the security knowledge Facebook. This presents various dangers for individuals, such as identity theft, hackers, blackmail, embarrassment, spam and stalking. Furthermore, there is a little awareness for employing continuous privacy mechanisms amid active users of

An International Journal JSCDSS E-ISSN: 2289-8603

Facebook. Thus, it is extremely vital to propose resolutions for protecting users' information and raising the level of users' awareness.

In this study, the main research question is defined as:

What are the security awareness factors that impact Facebook users?

To address the above question, the following research's questions are defined as:

- What type of personal information do students disclose on their Facebook profile?
- What is the student's awareness of personal features manipulation that concerns them?
- What framework is appropriate to support student awareness for Facebook security?

According to the research questions, the following research objectives are proposed as:

- To study the type of information that students post on Facebook.
- To identify features that support students' awareness for posting information concerning them.
- To develop a framework that supports student awareness of Facebook security.

This study will target undergraduate and postgraduate students at the University Technologi Malaysia (UTM) Skudai Campus. The social networking sites that are used in this research will shed light on users' awareness of Facebook security. The research covers the following points:

- Users' privacy setting awareness for postgraduate and undergraduate students.
- Users' awareness of manipulation of their confidential information.

2. Introduction of Facebook

Facebook is an ever increasing and extremely expanding social network that has exceeding previously existing social network sites. The company is growing and constantly producing new ideas, features, functionalities and platforms to increase user satisfaction. The company's progress and the supplementary rising number of users has forced the company to spread its workplaces beyond its headquarters in Palo Alto, California and open many offices in 18 domestic regions in addition to international offices. Dispatching global offices is how the company has managed and pioneered the social networking spectrum of this mobile and internet-driven period (Hasan, 2010).

Putting on target growing data knowledge groundwork skill to its associates from every single slant of their existence for disseminating and allocating of data competent and effectually by growing and crafting "digital map of people's real-world social connections" (Facebook Statistics, 2009) statistics display that "it is the second most trafficked PHP (hypertext pre-processor) site in the globe, and one of the largest MySQL installations anywhere, running thousands of databases" (Facebook Statistics, 2009). However, to reinforce its users with the allocating of information instruments, giving users beside dozens of security control features and functionalities, which give its associates the choice to manipulate their information to specific people or make it public for all community web site users, that has the default favored feature. Even though there are a lot of notice sounds and hazardous signals concerning the number of information users reveal and the loopholes of security settings.

The number of operatives retained in this social network website are potentially rising date by date (Facebook Statistics, 2009). It additionally inspires innovators to link and create something that is priceless for the community by saying that "no matter what parts of you join, you'll be building something large and new. You won't simply be discovering answers; you'll be framing questions that no one has ever asked before - and recognizing unprecedented opportunities. We welcome pioneers, In fact, we insist on them" (Facebook Statistics, 2009).

Launching new period requests has played a significant role in the quick development that Facebook has demanded the World Wide Web developers to craft in order to develop assorted new applications for the unstoppable producers. Mark Zuckerberg proclaimed in May 2007, that Facebook was "calling on all developers to build the next-generation of applications with a deep integration into, distributed across its social graph and an opportunity to build new businesses" (Debatin, Lovejoy et al., 2009).

This opportunity has given developers a medium to make competitive and efficient changes, consequently providing helpful factors and forcing the site beyond any other established social networking site. The introduction of the Facebook platform made it easy for the developers to create and develop Facebook applications that permit users easier implications like online games. Over 500 million users have enjoyed features that enhance the quality of the service of every member's experience in the internet and mobile period by keeping them in touch with family, friends, colleagues and so forth all above the world. Facebook has embraced the hearts of both young and old through the ability to connect and converse with those they love (Hasan, 2010).

If we go back before the conception of electronic contact, the evolution of the internet, and the present networking instruments, it was impossible for many people to stay connected with distant relatives, friends and loved ones. There was only little exclusion to this fact that included merely the literate and avid writers who connected across large spans via letters or those fortunate enough to afford long-distance telephone calls.

Facebook has concluded this complex non-contact period has ceased; many young people cannot fathom how communication occurred two or three decades ago. Facebook has challenged and countered the established method that people converse by making the connection

An International Journal JSCDSS E-ISSN: 2289-8603

easy and providing users with many choices, which have also provided a new way of connection, contact and allocating information (Hasan, 2010). Facebook has provided the users with options to allocate photos and videos, send short messages and internet links, say hello (poke) and so forth with their family, friends, colleagues and acquaintances. The functionality of these features has meaning and is a possible resource that can support users in staying in touch with each other.

Facebook has introduced new conceptions of platforms, progressions of new features that supply the demanded of services to its members that makes Facebook a flexible and lively communal website (Hasan, 2010). For instance, Facebook dispatched Instant Messaging (IM) in 2008, giving its users the power to connect, communicate and talk to their friends and families in real time (Pasek and Hargittai 2009). Facebook additionally provided users the ability to comprise a short text messages delineating their mood, what they are doing or what they have come across that day by simply crafting a user interface feature with the question "what is in your mind?". This encourages members to express their mood, frustration, joy, sorrow and their thoughts. It is an incredible feature that brings friends together. Facebook has additionally developed many supplementary methods that have received acclaim; posting a user's photo album is one more appealing feature on Facebook. Users now have a larger and more convenient medium to connect with their family and friends visually and virtually. These innovative features have inspired their global acclaim as being the communal website and social networking pioneer (Hasan, 2010).

Facebook permits its users to craft photo album that can encompass 200 photos in each crafted album. Users additionally have privacy settings in order to control what others can see and comment on their posted photo albums. More than 300 billion photos are posted on Facebook every single day as Facebook remarked in its blog (Hsu, 2012). This expresses how this photo album feature is vital and important to the users and their friends and families for staying close to each other.

2.1 Facebook Privacy Settings

If a user has valid e-mail address, he or she can simply join Facebook. The member has opportunity to set his or her privacy settings as he or she wishes. If students use a similar request, they will be able to make parts of their profiles viewable to everyone. Therefore, it is vital that students are aware of the significance of privacy settings. Even if students who use Facebook are not friends, one can see profiles from every supplementary group if the settings of their profiles are public. Additionally, students can see much personal information without knowing the person from whose profile they are obtaining information. In recent years, the default privacy settings of Facebook have been changing sometimes quite often, and these changes have been more open, permitting more parts of the profile to be seen in their default settings.

SNSs work to reinforce privacy settings; Facebook and supplementary social networking sites include privacy as part of their default settings. It is vital for users to go into their user settings to edit their privacy options. These sites provide users with the option to not expose confidential information, such as birth date, phone number, and employment status. For users who choose to display this information, Facebook enables them to restrict access to their profile. However, even this level of protection cannot prevent friends of a user from saving a photo to their own computer and posting it elsewhere. Even so, less social networking site users have restricted their profiles (Qi and Edgar-Nevill, 2011).

Although the arrangement design of Facebook demands users to reveal potentially risky information, the design additionally includes features that permit users to protect themselves and others with whom they link from privacy threats. Specifically, Facebook gives users the opportunity to change privacy settings for their personal profile information, photos, and video information. Users can additionally control who can link them, who can see their profile and can check third party admission to their personal information. Alternatively, users can additionally retain an ''open'' profile, permitting anybody to freely browse their information. In addition, unless users opt out of the default public search settings inside the privacy settings, their profiles are available to search engines, such as Google and Yahoo. Many online locations have privacy strategies to teach users about their privacy rights, the rights of the site and how information is public and utilized by the company.

Although privacy features protect the user and all information that the user could have posted concerning supplementary people (e.g., pictures, posts, and personal details), many users do not read the privacy strategies or employ available privacy settings. Acquisti and Gross (2006, as quoted in Nosko et al., 2012) found that the majority of Facebook users did not employ the available privacy settings, even after they understood the settings. After settings were utilized they were minimal, and allowed, for example, friends of friends or the entire websites users to view their profile. This openness regarding confidential information conflicts with counseling research that has found that most people express concern about their privacy, both offline and online (Nosko et al., 2012).

2.2 Facebook Privacy Awareness

For most of the people concerning the globe today visit at least one communal network site and go online to chat and communicate alongside supplementary people living the other factions of the world has come to be usual and indispensable part of their daily life. People could signal in e-mails, log on blogs, go online for chatting, and take part the online communal web sites. Most of these people don't discern the communal web sites and their internet groundwork as an instrument but rather as an expansion of

An International Journal JSCDSS E-ISSN: 2289-8603

their public identities and communal lives (Cavoukian, 2009).

2.3 Self-Disclosure

All of these craft and countless comparable reports transpire every single date concerning Facebook and supplementary communal web sites, because of plainly misinterpretation and misbehavior actions like posting contents in what students think private on their communal web accounts. Many users are fishing the students' accounts and what is going concerning them. Scammers, hackers, reporters, police, high school and college and university admission officers, employers, parents and summer camp managers are all discerning. Meanwhile, the students are uninformed and un-realized that as quickly as they post or tag something on Facebook, it is out of their hand and out of their control and ownership of that posted contents "it is quite an eye opener" (Fodeman and Monroe, 2009).

Self-disclosure is devoted to what people intentionally and voluntarily allocate concerning their confidential matters like feelings, thoughts and experience to others (Jia, Zhao et al. 2010; Shin, Ko et al. 2011). It reflects to the large number of data shared on the user's profile, in supplement to the procedure of communication alongside others. Facebook users are revealing a large number of personal information in online communities. A self-disclosure on Facebook reveals that the majority of the people exceptionally students reveal data like their relationship status, email address and birthday to an average of concerning 300 friends and many other countless networked connections. Acquistic and Gross (2006) specified that the large vast of users provide their real names, complete birthday and clear photo pictures for themselves in their profiles. People can additionally post albums of pictures and videos from parties, ceremonies of both themselves and their friends.

3 Proposed Conceptual Framework

Proposed Conceptual framework describes the entities or concepts and the relationships between these entities. Conceptual framework also simplifies visual representation of the problem formulated or system being examined.

As mentioned in the literature review and the researcher's topic stated, this conceptual framework emphasis on the user's privacy awareness, Facebook privacy settings and users' self-disclosure, because Facebook has already put the responsibility of the privacy control on the shoulders of its users. The privacy setting status which can pioneer the user in to one of two ways, either the harmless road (applying privacy settings) or the treacherous route (default publicly privacy setting).

Privacy awareness and privacy application would lead the level of information sharing violation. Going back what researchers has said from these contents, a study made by Alessandro Acquisti stated that less 3% of the users are able to read privacy policy, while 75% of the users believe that the availability of privacy policy means the existence of information privacy protection (Acquisti and Gross, 2006). Another researcher stated that the privacy paradox results from unawareness and lack of privacy concerns, also described data privacy can be broken not only by exposing the protected secrets but enlarging and increasing the original information accessibility (Solove, 2007).

As the title of the research states, the research objectives and the research questions have been emphasized, and as mentioned in the literature review, the information provided by privacy and self-disclosure related models, users' awareness, the privacy settings and the amount of information users disclosed are the basic fundamentals and the controlled contents of this proposed conceptual framework. The proposed conceptual framework institutes three interrelated components consisting of the users' privacy awareness, Facebook privacy settings and the users' self-disclosure as illustrated in Fig. 1.

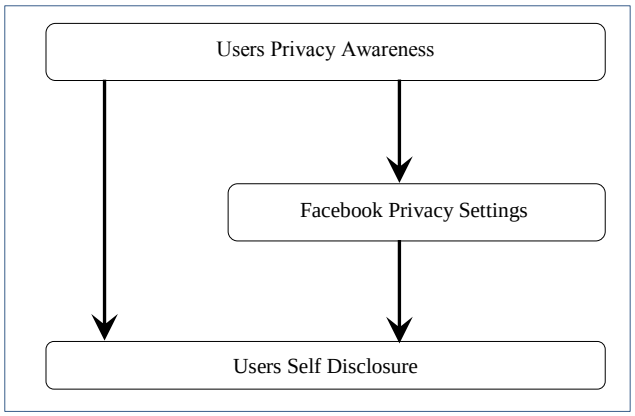


Fig. 1. Proposed Conceptual Framework.

3.1 Data collection and analysis

A preliminary survey was conducted early in the research process and followed by the actual survey from the undergraduate and postgraduate students in the Faculty of Computing at Universiti Teknologi Malaysia (UTM). The researcher selected a random sample selection method for his research study because it permits an equal opportunity to select a diverse representation from the targeted research population. Questionnaires were designed and distributed to all members related to the study. In this pilot, 37 of 40 preliminary surveys returned their feedback. In this case three questionnaires were missed.

The survey questionnaires are established by the quantitative data analysis method. The survey questionnaires contained around eight questions, comprised of demographic questions and users' security setting awareness questions. Later when accumulating data, the researcher uses SPSS software for the analysis of the questions.

Reliability analysis allows researchers to study the properties of measurement scales and the items that form them. The reliability analysis procedure calculates a

An International Journal JSCDSS E-ISSN: 2289-8603

number of commonly used measures of scale reliability and also provides information about the relationships between individual items in the scale. The reliability analysis was conducted in order to ensure the internal validity and consistency of the items used for each variable. Table 1 presents the reliability of the measurement scales. Thomas suggests that an Alpha of 0.75 or greater is acceptable for instruments that assess knowledge and skills, and 0.50 or greater is acceptable for attitude and preference assessments (Thomas et al., 2005). Therefore, this result illustrates that the questionnaires are reliable measurements and can be used in the research.

Table 1

Cronbach's Alpha.

Scale Items	Cronbach's Alpha
Demographic Background	0.806
Users' Privacy Awareness	0.848
Facebook Privacy Settings and User's Self Disclosure	0.764

The next step was examining the construct validity. According to this, the construct validity of each factor was tested to verify the validity of items for measuring the privacy concern and self-disclosure amount in SNSs. There are two types of construct validity. The first type is the correlation between total scores, and the second type is factor analysis. This preliminary study has been conducted using analysis of the correlations between total scores to test construct validity because the factor analysis requires a large number of respondents, and there are not enough participants in the pilot study to perform it. The result of the correlations between total scores is stated in Table 2.

Table 1

Item-Total Statistics for Users' Security Awareness on SNSs.

Scale Items	Number of Items	Corrected Item-Total Correlation
Demographic Background	3	0.600
Users' Privacy Awareness	3	0.644
Facebook Privacy Settings and User's Self Disclosure	2	0.692

The result of the all items showed that the correlations of total scores are valid. As the table above depicts, the item-total correlation for the all items leads to a number more than 0.5, which indicates items significantly correlate each other with a total score of the questionnaire items.

3.2 Findings

After the data collection and data analyses, the results concluded that most of the users are aware of the system's privacy existence, which is a good sign for the wellbeing of the users. However, the findings also conclude that the majority of the users do not use, apply, customize or modify the system's default privacy settings, which is a bad sign for safety of the users. Taking these findings into account, we determined to redesign and reshape the proposed privacy and awareness conceptual framework in order to develop more tenable conceptual framework that can guide and escort the users to the Facebook privacy settings. In order to improve the users' usability and application of the system's privacy existence, four more privacy mechanisms are supplemented into the prior conceptual framework.

The extra components of the conceptual framework are copied and referred from Facebook's main privacy setting functions which the researcher has attempted to make straightforward to the users as they become familiar with the system's privacy settings and hopefully utilize it. These four additional components are control privacy when one posts, controlling one's default privacy, editing one's profile and editing settings as illustrated in the subsequent figures and discussion.

Hence, the proposed conceptual framework in the literature review is expanded by adding the control privacy settings applications provided by Facebook, as shown in Fig. 2.

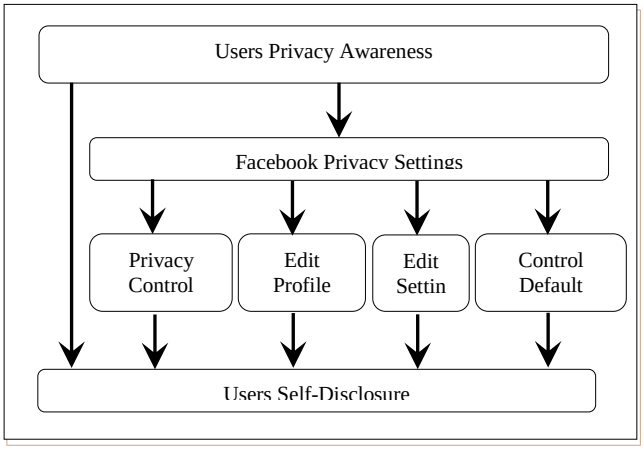


Fig. 2. Expanded Proposed Conceptual Framework.

This conceptual framework would facilitate users to interact the system privacy settings after raising users' awareness on the lack of privacy setting customization. This conceptual framework eradicates and eliminates the unawareness issues and privacy condemnation on Facebook. This conceptual framework guides the users to become aware first, and then visit and read Facebook's privacy settings. Afterward, users can one by one modify, customize and change the privacy settings by following the four major functions under the privacy settings, starting from privacy control when one posts, edit privacy when editing profile, edit settings and control default privacy settings. After that, any user that self-discloses will be much more protected and confidential than with the original system's default publicity.

An International Journal JSCDSS E-ISSN: 2289-8603

4 Research achievements

Facebook has provided the largest necessary privacy setting applications that none of the other SNSs has ever offered. Users are aware of the system's privacy settings availability and the public default of this widely open SNS media, however very few of them have taken the necessary steps to apply the privacy settings in order to change their default privacy setting status. According to the revision of the research objectives and research questions, the researcher has achieved the research expectations, research goals, research results and outcomes as the subsequent successive points indicate.

Objective 1: The first objective was to study the type of information that students post on Facebook. The majority of the users discloses and share different types of personal information and large amounts of personal private details with this significantly expansive SNS, including the basic information, background facts and contact details which are the most susceptible details. This objective has been achieved through data collection, data analysis and research findings.

Objective 2: The second objective was to identify features that support students' awareness for posting information concerning them. Most of the users are aware of Facebook privacy setting features and it is public default status, however most of them do not view the privacy settings and do not customize their privacy preference as observed in their profile data. The majority of the users are still public by default, though they have stated that they are aware of the availability of these security settings.

Objective 3: The third objective was to develop a conceptual framework that supports students' awareness of Facebook security. The researcher has designed and proposed a Facebook privacy conceptual framework. The framework consists of three interconnected components derived from the literature review theory concepts and privacy related models. The three components of this conceptual privacy framework are users' awareness of the privacy systems, Facebook's privacy settings and self-disclosure of the users. After the data collection, data analysis and research finding, the researcher reviewed the previous conceptual framework and redesigned it by adding additional important privacy mechanisms.

5 Conclusion

The aim of this study is to identify the types and amounts of information users disclose about themselves while using Facebook social media, to observe and study users' awareness of the sites' privacy settings and how they use and apply these privacy settings. The study also highlights proposing Facebook's privacy conceptual framework and recommending effective guidelines that can facilitate users when applying Facebook's privacy settings. Users share, post and disclose large amounts of dissimilar types of private information, including basic information, background and contact information, on this privacy-free SNS. The majority of users are very aware of the accessibility of Facebook's privacy settings; however, few of them exercise concern in order to control and restrict the publicity of their collective information. The majority of the users have not read Facebook's privacy policy and terms of service, whilst many of them are unaware of how Facebook has divulged their information with third parties.

In conclusion, governments, educational institutions, media, organizations and companies will need to raise SNSs users' awareness in order to notify Facebook users of the danger and impacts of sharing massive amounts of personal information on public and far-reaching SNSs and how the provision of privacy setting applications may diminish this kind of predicament.

References

Acquisti, A. and Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. Proceedings of the 2006 Privacy enhancing technologies: Springer, 36-58.

Boyd, D. M. & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13, 210-230.

Cavoukian, A. (2009). Privacy by design. Take the Challenge. Information and Privacy Commissioner of Ontario, Canada.

Debatin, B., J. P. Lovejoy, et al. (2009). "Facebook and online privacy: Attitudes, behaviors, and unintended consequences." Journal of Computer Mediated Communication 15(1): 83-108.

Dhami, A., N. Agarwal, et al. (2013). Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook. Advance Computing Conference (IACC), 2013 IEEE 3rd International, IEEE.

Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer- Mediated Communication. 13(1), 210-230.

Facebook Inc. (2009). Facebook Statistics, http://www.facebook.com/press/info.php?statistics

Fodeman, D. and Monroe, M. (2009). The impact of Facebook on our students. Teacher Librarian. 36(5), 36-40.

Hasan, K. F. (2010). The Dark Side of Facebook Games, WORCESTER POLYTECHNIC INSTITUTE.

Hsu, Y.-L. (2012). "Facebook as international eMarketing strategy of Taiwan hotels." International Journal of Hospitality Management 31(3): 972-980.

Jia, Y., Y. Zhao, et al. (2010). Effects of system characteristics on users' self-disclosure in social networking sites. Information Technology: New Generations (ITNG), 2010 Seventh International Conference on, IEEE.

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

Nosko, A., Wood, E., Kenney, M., Archer, K., De Pasquale, D., Molema, S. &Phulari, S., Khamitkar, S., Deshmukh, N., Bhalchandra, P., Lokhande, S. & Shinde, A. (2012). Understanding Formulation of Social Capital in Online Social Network Sites (SNS). arXiv preprint arXiv:1002.1201.

Pasek, J. and E. Hargittai (2009). "Facebook and academic performance: Reconciling a media sensation with data." First Monday 14(5).

Qi, M. and Edgar-Nevill, D. (2011). Social networking searching and privacy issues. Information Security Technical Report. 16(2), 74-78.

An International Journal JSCDSS E-ISSN: 2289-8603

Shin, S., Y. Ko, et al. (2011). The conflict between privacy and self-disclosure in Social Networking Services. Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, IEEE.

Solove, D. J. (2007). The future of reputation: Gossip, rumor, and privacy on the Internet, Yale University Press.

Squicciarini, A. C., Shehab, M. and Paci, F. (2009). Collective privacy management in social networks. Proceedings of the 2009 Proceedings of the 18th international conference on World wide web: ACM, 521-530.

Thomas, A. L., Sang, H. L., John, C. W. & Richard, M. F. (2005). A Study of the Reliability and Validity of the Felder-Soloman Index of Learning Styles. In: American Society for Engineering Education Annual Conference & Exposition.

Tuunainen, V. K., Pitkänen, O. and Hovi, M. (2009). Users' Awareness of Privacy on Online Social Networking sites-Case Facebook. 22nd Bled eConference eEnablement: Facilitating an Open, Effective and Representative eSociety, Bled, Slovenia: http://ecom. fov. uni-mb. si/proceedings. nsf/0/9b675b5e811394f0c125760000390664/$ FILE/1_Tuunainen. pdf.

Yan, Z., Zexing, H., Huaixi, W., Hongxin, H. & Gail-Joon, A. (2010). A collaborative framework for privacy protection in online social networks. In: Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th I nternational Conference on, 9-12 Oct. 2010 .

Zorica, M. B., Biskupic, I. O., Ivanjko, T. & Spiranec, S. (2011). Students and privacy in the networked environment. In: MIPRO, 2011 Proceedings of the 34th International Convention, 23-27 May 2011. 1090-1094.

An International Journal
JSCDSS
E-ISSN: 2289-8603