# ONLINE INFORMATION REVELATION AND PRIVACY ON INTERNET- BASED SOCIAL NETWORK OF FACEBOOK: A CASE OF UUM POSTGRADUATE STUDENTS

**A Thesis submitted to the UUM College of Business**

**In partial fulfillment of the requirement for the degree**

**Master of Science Management**

**Universiti Utara Malaysia**

**By**

**NADIAH BT MOHAMAD ROSDI**

**(807426)**

**2013**

# PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree Master of Science Management from University Utara Malaysia, I agree that the university's library may it freely available for inspection. I further agree that permission for copying this thesis in any manner, in a whole or in a part, for scholarly purpose may be granted by my supervisor or in their absence, by the Dean of Postgraduate, UUM College of Business. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to University Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part shall be addressed to:

Dean of Postgraduate
UUM College of Business
University Utara Malaysia
06010 Sintok
Kedah Darul Aman

# DISCLAIMER

I am responsible of the accuracy of the opinion, technical comment, factual report, data, figures, illustrations and photographs in the article. I bear full responsibility for the checking whether material submitted is subject to copyright or ownership right. UUM does not accept any liability for the accuracy of such comment, report and other technical and factual information and the copyright or ownership right claims.

I certify that the substance of this thesis has not already been submitted for any degree and is not currently being submitted for and other degree or qualification. I certify that any help received in preparing this thesis and all sources used have been acknowledged through this thesis.

Student's Signature:

_____

(NAME: NADIAH BT MOHAMAD ROSDI )
Metric: 807426
Date: 18 February 2013

# ABSTRACT

The purpose of this study was to evaluate the online information revelation and privacy on internet based social network of Facebook of UUM postgraduatestudents. It was hypothesized that there is significant relationship between four factors which are concern for internet privacy, concern about unwanted audiences, personal network size and frequency of Facebook use. The surver were used for gathers the data from respondents for this study that were consisted of 306, as refers to UUM postgraduate students that study at UUM Kuala Lumpur campus. There were 52.9% female and 47.1 % male ranging from 20-40 years old. The data was collected and analyzed using Exploratory Factor Analysis (EFA), descriptive and regression analysis. EFA used to identify which factors that influence the online information revelation . While descriptive analysis test was used to examine students privacy protection strategies. Finally the regression analysis test is to investigate the asociation between independent variables and dependent variables. The finding indicated that frequency of facebook use have the highest mean compared to others factors. It shows that frequency of facebook use was the most affected factors to the online onformation revelation and internet privacy of UUM postgraduate students. Moreover others factors show that positively association with information revelation. Lastly the student have their own privacy strategies to protect themselves. The most often practiced by the students are the use of private email messages, exclusion of personal information and altering default privacy setting.

# ACKNOWLEDGEMENTS

An outstanding cooperation of dedicated professional at School of Business Management and OYA Graduate School of Business made the creation of the thesis a pleasure. My supervisor, Mr. Abdul Manaf Bohari, enthusiastically support and backed the project and play a large role in completing the thesis. Thank you very much for the invaluable guidance, encouragements, suggestions, comments, and assistances through-out the period of this thesis. Your kind advice will encourage me to do further research in future.

I thank the faculty staff for valuable information, supply many insightful reaction, and suggestions for final works improvements. I am particularly grateful to Mr. Nazlan B Mohamed Nazidin Coordinator of Business Management at IKIP College, who helped me a lot in SPSS. Also, I am particularly grateful to my colleagues, friends, and course-mates who in anyway help me through this research paper.

Finally, I am indebted to my husband and my sister, Iskandar bin Abdul Halim and Nabilah bt Mohamad Rosdi. Thanks a lot for giving me more chance and more time to complete this final report. Special thanks for their support, commitment, and understanding in helping me pull through this course. I appreciate the contribution from all of my family. All of you are wonderful helpmate. Thank you for everything.

Nadiah bt Mohamad Rosdi
18 February 2013

# TABLE OF CONTENTS

# CHAPTER ONE

# INTRODUCTION

## 1.0 Background of the Study

Social network sites (SNSs) is a web-based service that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site. Boyd & Ellison (2007). The uniqueness of social network sites is not that they allow individuals to meet unfamiliar person, but to a certain extent that they enable users to articulate and make visible their social networks.

Before joining an SNS, an individual is asked to fill out forms containing a series of questions. The profile is generated using the answers to these questions, which typically include descriptors such as age, location, interests, and an "about me" section. Most sites also encourage users to upload a profile photo. Some sites allow users to enhance their profiles by adding multimedia contents or modifying their profile's interface. (Sundén, 2003, p. 3) Others, such as Facebook, allow users to add modules ("Applications") that enhance their profile. The visibility of a profile differs by site and according to users' discretion. By default, profiles on Friendster and Tribe.net are crawled by search engines, making them visible to anyone, regardless of whether or not the viewer has an account. Alternatively, LinkedIn controls what a viewer may perceive based on whether she or he has a paid account. Sites like MySpace allow users to prefer

whether they want their profile to be visible for publics or for their friends only. Facebook takes a different approach—by default, users who are part of the same "network" can view each other's profiles, unless a profile owner has decided to deny permission to those in their network. Structural variations around visibility and access are one of the primary ways that SNSs differentiate themselves from each other.

This paper is mainly focusing on SNSs of Facebook users' account. Facebook becomes a growing phenomenon of SNSs. Nowadays; nearly everyone has a Facebook account. Facebook is the largest social network on the web, primarily focused on high school students to college students. Facebook has been gaining market share, and more significantly a supportive user base. Since their launch in February 2004, they have been able to obtain over 8 million users in the U.S. alone and expand worldwide to 7 other English-speaking countries, with more to follow. (Sid Yadav)Most individuals who sign up their Facebook account and reveal their information especially personal information, seemingly without much concern. Gross and Acquisti (2005) mentioned that in disclosing personal information on SNSs user effectively place themselves at a greater risk for cyber and physical stalking. This study is designed to find the important factors that influence online revelation of Facebook among postgraduates of University Utara Malaysia (UUM) Kuala Lumpur Campus.

## 1.1 Problem Statement

Previous study have attempted to determine the reason why social networks users are unconcerned and unaware of the privacy concerns associated with their online practices, but the

reasons prove to be numerous and varied (Richard and Joseph 2007). The real privacy arises when users allow people they do not know and normally would not trust to have access to the personally identifiable information they have made available. Gross and Acquisti explain that it may, in fact, stem from lack of privacy concerns. That is people allow a precarious amount of information about themselves to be available on this social networking site because they are unaware of the large number of people who are allowed to view this information. Unfortunately, this scenario has not taken seriously by the individual. They just disclose their personal information without thinking of the implications.

Facebook users in Malaysia estimated is about 12,060,200 on December 2011 by Lim Yung Hui where as socialbakers.com reported that the total number of Facebook users in Malaysia is reaching 12, 182, and 40. Almost 12 million people in Malaysia have Facebook account. Moreover, the web reported the most of the Facebook users in Malaysia are between the ages of 18-34 years old. Indeed, Lamped et al. (2006) found those university students are the heavy users of Facebook. Through his research 70 per cent of students are report spending thirty minutes or less on Facebook per day and 21 per cent indicate spending more than an hour a day on average using the site.

Berita Harian on October 2011 reported that 60,000 students in Malaysia are addicted to Facebook. Professor Madya Dr. Mohd Fadzil Che Din (Director of Institute Sosial Malaysia ISM) mentioned that FB is chosen by the students because it is convenient and less risk. The students can converse to anyone without meeting them. If this scenario did not being taken into

consideration it will end up with negative impact for them. Thus, in the future, Malaysian would have more antisocial individuals.

Moreover, reported by Berita Harian on January 2012, eventhough Facebook is indeed beneficial to the users, it is also troublesome. The biggest issues are on the privacy and the children's safety. From Facebook, people can find the information on the users easily; this shows there is no privacy of the users. In addition, some countries have taken this issue seriously because of the privacy right. In other case, Facebook is chosen by some criminals to find the victims. The children become the target as they are naive and can be conned easily. Moreover, this is 'encouraged' by the exposure of the children' identity. Recently, there are objections on Facebook from the Islamic countries. They are against the function of the Facebook which encourages people to socialize without any limit. Furthermore, an Iranian Mullah has decided that Facebook is contrast of Islamic perspectives since it can be one of the 'encouragements' to the social problems. He added that the websites which concern on the Islamic criteria solely can be used by Muslims. This is an important reminder as we are one of the Islamic countries and we must emphasize on the religious issue. Whenever there are etiquette and moral, the problem in society can be prevented.

Students remain give their information without thinking the impact that they will face in the future. However, the reasons why users willingly disclose information on their profiles have not been sufficiently investigated. (Tufekchi 2008) The problem of the study is to find out important factors influence online information revelation and privacy on internet –based social network of Facebook a case study of University Utara Malaysia (UUM) postgraduates' students.

## 1.2 Research Objectives

Specially, the objectives of this research are as follow:

a. To identify the demographic profile of University Utara Malaysia (UUM) postgraduates' students.
b. To identify which factors that influence the online information revelation revelation practices on Facebook by UUM postgraduate students.
c. To investigate the association between independent variables and dependant variable.
d. To examine students' privacy protection strategies on Facebook.

## 1.3 Research Questions

a. What are the most factors influence online revelation information and internet privacy of Facebook?
b. What are the strategies that can be used to protect privacy of UUM Facebook users?
c. How often UUM student visit Facebook?
d. To what extent UUM postgraduate student are concerned about general internet privacy.

## 1.4 Significance of the study

The importance of the study is to inform the UUM postgraduate student that their information exposure might be used for potential harmful purposes by unknown people.

We cannot predict what will happen in the future, for example strangers would know where we live or recognize our face based on information that given through Facebook. Other than that, the information given by the student would be used or sold without their knowledge or consent. Everything that they put on the Facebook might be used purposely neither we agree nor disagree.

Finally, University Utara Malaysia (UUM) postgraduate must acknowledge their own personal information regardless giving easily to the others. They have to know that it is important to keep their personal information.

Last but not least, the important of this paper is to come out with the privacy protection strategies that can be used by UUM postgraduate students on Facebook. Students must aware that basically the privacy policy is going to instruct the users on how their information is being collected and how you are going to use or even how the information will not be used.

## 1.5 Summary

When you are online, you provide information to others at almost every step of the way. Often this information is like a puzzle that needs to be connected before your picture is revealed. Information you provide to one person or company may not make sense unless it is combined with information you provide to another person or company. Knowing that nowadays anything can happen, good thing or bad thing the personal information should not easily reveal to others. Nowadays students whom involved the most in social

networking sites without doubt provide information in the web. In the future this would give disadvantages to them if too much personal information revealed. However, there are strategies that they should know in order to protect themselves from stalking or strangers to manipulate their information. Thus, at the end of this paper will be discussed the privacy protection strategies that could be practiced.

# CHAPTER TWO

# LITERATURE REVIEW

## 2.0 Introduction

"Online" refers to resources related to any aspect of living that are easily reached through a group of interconnected computer networks called the internet."Online" consist of documents on the World Wide Web, e-mail, file-sharing, newsgroups, streaming media, etc. By virtue of the internet, being online facilitates data transfer and a variety of communication services (NetLingo, 2006). Facebook, MySpace, or Twitter were label as online social networks and currently have experienced phenomenal growth in association.

At the most fundamental point, an online social network is an Internet community where individuals cooperate, often through profiles that symbolize their public persona (and their networks of connections) to others (Acquisti and Gross 2006). BorneoPost online on November 30, 2012 reported that in Southeast Asia, Malaysia ranks fourth after Indonesia, Philippines and Thailand in terms' of social media usage, Facebook where as SocialBakers research data showed that there are 13.38million FB users in Malaysia presently. Moreover the report from SocialBakers revealed that FB penetration in Malaysia was 51.15 per cent and thus the total number of Malaysia FB users grew by more than 1.22million (May 2012 - November 2012).

## 2.1 Background

### 2.1.1 Social network and Facebook

Adrian and Arnie (2011) reported that nearly 2 billion people are connected to the World Wide Web, creating seemingly limitless opportunities for communication and collaboration. By definition, SNSs are interactive websites designed to build and enhance online communities (Steinfield, C., Ellison, N.B. and Lampe, C., 2008), and connect members with common interests (Carter.H.L, Fougler, T.S, and Ewbank, A.D 2008; Shin, 2010). Of the various sites available, Facebook is unquestionably one of the most accepted and booming ones (Dickey and William, 2010; Steinfield et al., 2008).

Facebook at the moment is one of the leading social networking sites. It was founded in 2004 in the USA by a former Harvard student Mark Zuckerberg. In the establishment, it was created only for students' interaction tool, but nowadays it is opened for everybody who has a valid email address. The success and growth of Facebook has been incredible: after the first year, it had already one million users, and five years later, in February 2009, Facebook had already more than 175 million active users. More than half of Facebook users are outside of college, and the fastest growing demographic is those 30 years old and older. Facebook also had an influential entry to the Finnish market in the summer and early fall of 2007. In the spring of 2008, the Finnish Facebook network had over 399 000 users (www.facebook.com).

Adolescents and young adults tend to be the most frequent users of SNSs (Mason et al., 2010; Quillian and Redd, 2009; Subrahmanyam et al., 2009; Gemmill and Peterson, 2006), with current cohorts being more digitally fluent when compared with previous ones (English and Duncan-Howell, 2008). In the USA, 90 percent of teenagers and young adults participate in one or more online communities (Trusov et al., 2010), while in Europe, 59 percent of all 9 to 16 year-olds claim to have their own social network profiles, with a slightly lower percentage for boys (58 percent) than for girls (60 percent) (Livingstone and Haddon, 2011).Today, social networking has come to mean individuals using the internet and Web applications to communicate in previously impossible ways (Weaver and Morisson 2008).

With the development of social networks it offered users virtual hangout where they could be themselves, share what they are doing or working on or just express their views (Adrian M.budiman and Arnie Shakinar Abidin, 2011). Research has demonstrated that users continue to disclose personal information on Facebook. Each year, users of Facebook keep growing and they did not hesitate to disclose their information to others. (Alyson L.Young and Anabel Quan-Haase, 2005) .On the Facebook users can share a variety of information about themselves on their Facebook including photos, current address , contact information, and tastes in movies and books. They list their friends", as well as friends in other schools. In addition, users can also identify what courses they are taking and join a variety of groups with similar interests. The site is often used to obtain contact

information, to match names to faces, and to browse for entertainment (Harvey Jones, Josee Hiram Soltren,2005) Facebook was founded in 2004 by Mark Zuckerburg, a Harvard undergraduate.

The site is unique among social networking sites in that it is focused around universities. Facebook is actually a collection of sites, each focused on one of 2,000 individual colleges. Users need a @college.edu email address to sign up for a particular college's account, and their privileges on the site are largely limited to browsing the pro_les of students of that college. In May 2005, Facebook received $13 million dollars in venture funding. (Marshall, Mat and Anna Tong 2005)

Indeed, social-networking sites find themselves in a Goldilocks-style dilemma: If they share too much information, the services become a spammers' paradise. Share too little, and they defeat the power of social networking, where you can discover and communicate with people you may not know but with whom you share something in common. For that reason the amount of information shared has to be just right. Each startup has its own plan for how to deal with privacy concerns. (Jane Black. The perils and promise of online schmoozing.BusinessWeek Online, February 20, 2004.)

## 2.2 Literature Review

### 2.2.1 Social Network on Social Relationship

Social networks comprise a person's social relationships, that is, "the set of people with whom an individual is directly involved [emphasis added]" (C. S. Fischer, 1982, p. 2), such as family members, friends, and acquaintances. There are different types of social networks that can be distinguished by the kinds of relationships they include. The term global network, or directly "social network," comprises all existing social relationships of an individual with family members, spouses, friends, coworkers, neighbors, society fellows, etc., and thus conceptualizes social networks most comprehensively (Allan, 2006; C. S. Fischer, 1982; Milardo, 1989). The personal network describes a sub network of closer, personal relationships in the global network such as family members, friends, and other close confidants (Van Der Poel, 1993). Personal networks are sometimes termed support networks, as they are often seen as a resource for people's health and well-being through the exchange of support among closer network members (Allan, 2006; Hammer, 1983). Other types of networks that also focus on sub networks of the global network are the friendship network, the family network (e.g., siblings, parents, children, and spouse), and the work-related network (e.g., coworkers and supervisors).

Weaver and Morrison (2008) define social network as a network consisting of three or more entities communicating and sharing information. In the context of today's electronic media, social networking has come to mean individuals using the Internet and Web applications to communicate in previously impossible ways (Weaver and Morrison, 2008). Nosko, Wood, and Molema (2010) mentioned one

of the primary goals of the SNS is to encourage disclosure of personal information with others online. Some examples of the SNS are Facebook, Friendster, MySpace and Twitter.

Facebook (www.facebook.com) is a SNS that allows users to create personal profiles and establish connections with other users including their family, friends and colleagues. In addition to basic information such as name, profile picture and gender, which are always open to everyone, Facebook profiles also include optional information such as birthday, education, telephone numbers, address, email and photos. Users can also upload other medias such as videos and interact with other users by commenting on their profile (or 'wall'), status updates, photos or videos.

The fast growth of SNS such as Facebook, which reaches 500 million users recently (Facebook, 20 10) has coincided with an increasing concern over personal privacy. The New York Times, The Guardian, The Daily Telegraph, The Independent, and BBC News published articles on privacy and SNS including Facebook. Facebook members or users including students and adolescents provide personal information on their profiles that can be viewed by a large number of people. Rosenblum (2007) highlight that the most instantaneous risk of posting online is the obvious one of leaving a permanent digital record of comprising photos and remarks that can later be searched and accessed by third parties trying

to evaluate the character of an applicant for a job, school admission, or other competitive position for which applicants must be screened and eliminated.

These days, companies usually use search engines to do their background checks on prospective employees, and also often review SNS. As one officer observed, "You really do get a lot of information you can't ask for in the job interview, but you go on the Web and it's all right there" (Rosenblum, 2007, p. 46). As stated by Rosenblum (2007), the information can easily be gathered from Web unlimitedly. In addition, according to a recent survey by Microsoft, 75 percent of recruiters and human resource professionals in the United States of America (US or USA) reported that their companies require them to do online research about candidates, and many use a range of sites when scrutinizing applicants - including search engines, social networking sites, photo and video sharing sites, personal Web sites and blogs, Twitter and online gaming sites. Furthermore, seventy percent of US recruiters reported that they have rejected candidates because of information found online, like photos and discussion board conversations and membership in controversial groups (Rosen, 20 10).

A study done by Adrian and Arnie (2011), find out a security consultant, Ron Bowes, published details of 100 million Facebook users, which he collected by using a piece of code to scan profiles for data not hidden by users' privacy settings. The list contained the URL (web page address) of every searchable Facebook user's profile, and their unique ID (username). Bowes mentioned that

the data was published to highlight privacy issues (Emery, 2010). This matter had been highlighted all over again by McKeon (2010), who stated that the default privacy settings for a Facebook user's personal information have become more and more permissive. Facebook has changed how the personal information is classified several times, which can be confusing to some users. Based on the study the result shows higher levels of privacy perception did not result in less disclosure of personal information. On the other hand, the result shows the majority of respondents who were active users tend to be more open or disclose personal information the most.

Same goes with Jones and Soltren (2005) where they reported that the most active users disclose the most information. However, according to Lewis, Kauffman, and Christakis (2008) having a private profile is associated with a higher level of online activity. Respondents who take action to protect their online privacy spend a higher number of hours per week online on average and have also been using the Internet for a greater number of years. It follows that the more online experience the respondents have, the more they will know about possible privacy threats, and the more they will know about how to take actions to protect themselves (Paine, Reips, Stieger, Joinson, and Buchanan, 2007).

It is assumed that people's privacy perceptions and concerns reflect their privacy practices. However, previous studies on SNS reported that privacy perceptions and concerns do not parallel privacy practices (Viseu, Clement, and Aspinall,

2004; Hsu, 2006; Dwyer, Hiltz, and Passerini, 2007; Debatin, Lovejoy, Horn, and Hughes, 2009). Most scholars assume that people's privacy concerns represent how they will behave when they encounter privacy risks. As a result, scholars usually ask about respondents' privacy concerns without double-checking respondents' actual practices (Hsu, 2006).

The majority of Facebook users stated to know about ways to managed visibility and searchability of their profiles (Acquisti and Gross 2006) This give the impression that Acquisti and Gross agreed with Hsu, but however some users were unaware of those tools and options. Jones and Soltren (2005) observed that users were generally familiar with the privacy features Facebook offers, but some opted not to use the features instead. Rosenblum (2007) explained that users do not exercise in the virtual world even the routine common sense they would exercise in the real world. Believing that they are interacting in a protected environment, nearly everyone does not exercise the same common sense.

Students' reliance on social media is undeniable. Nowadays, social medias are not only tools of students but increasingly of the organizations that seek to hire them. This is proved by Roberts & Roach (2009) who stated that HR personnel frequently use social networking websites as reference checks for potential job candidates. In addition, ample evidence suggests that use of social media within organizations' communication is rapidly displacing email (Cardon & Okoro, 2010). In simpler words, students who can communicate via informal and formal

communication channels are becoming increasingly valuable in organizations. It is proved by Decarie (2010), she claimed that social media, when used appropriately, opens up a world of networking and relationship-building opportunities for students.

Facebook has become the premiere site for social networking, with more than 800 million users as of October 2011 (Facebook, 2011). The site is not only a favorite source of social connectedness, but it is even credited for helping to spread democracy and topple regimes in countries such as Egypt and Tunisia. While we tend to think of Facebook as a fairly recent phenomenon, it is grounded on well-established tools in social network theory. Two of the principle features of social networks are network size and network quality. The size of a person's network is a critical predictor of her or his ability to learn new information. Most students believe that the larger the network the better, as large networks seemingly provide more opportunities for information benefits than do smaller networks. While this is true, the flip side is that large networks require more time and energy for maintenance of high-quality ties within that network. With too many contacts, people struggle to manage the flow of information and maintain high quality, meaningful relationships with others in their network (Burt, 1992).

Granovetter, (1973) mentioned that network size does not necessarily correspond to network quality. Students typically spend only a little time with each person, rarely engaging in in-depth conversations that will help others remember them in

the future. Daunted by the number of contacts that they make, students may not feel motivated to spend time and energy maintaining potentially valuable contacts. By learning about the concepts of network size and quality, students seeking jobs begin to understand that building a smaller network with higher network quality is a better strategy than to make as many contacts as possible.

Since many of the previous studies on SNS were conducted in the Western world, there is a need for studies in other parts of the world, such as in Asia, where a large number of Internet users reside, and particularly in Malaysia, where there is a huge number of user growth. According to the Internet World Statistics updated on 30 June 2010 by Miniwatts Marketing Group (2010), there are 825 million Internet users in Asia alone. Asia makes up 42% of the Internet users worldwide, which is the highest. Malaysia has 16.9 million Internet users with a staggering 356.8% user growth since 2000. Gonzalez (2010) stated that Malaysia has 7.9 million Facebook users. The largest ever global research project into people's online activities and behaviour, Digital Life, conducted by research firm TNS, reported that the heaviest users of SNS are in Malaysia, spending an average of nine hours per week on SNS (BBC News, 2010, October 10; TNS, 2010). Fisher-Hubner (1998) pointed out that people in most Asian countries have little sense of privacy. This is supported by Hsu (2006) who mentioned that scholars in some cross-cultural research claimed that people in Asian countries do not care about individual privacy. In contrast, for Western society, it is social custom that one

does not ask others for personal information as a mark of respect (Nosko, A., & Wood, E., & Molema, Sl., 2010).

Malaysian Facebook users must be aware that there are some authorities such as prospective employers or university admission officers who can access their profiles, or unwanted information easily if they did not use Facebook privacy settings accordingly. Any Internet users can also access their personal information if they did not exercise cautions of the privacy settings, which could lead them to fall prey to identity thefts.

### 2.2.2 Social Networking as Social Function

Social Networking once means going to a social function such as a cocktail party, conference, or business luncheon. Balas (2006) defined OSN as a platform used as a mean for building online communities, where individuals from around the world can connect with each other for variety of reasons. Similarly, OSN is defined by Preece and Maloney-Krichmar (2005) as "people who come together for a particular purpose, and who are guided by policies and supported by software." Overall, OSN is an online virtual community where a user can create a profile and build a network of people with similar interests or activities.

Today, social networking is achieved through Web sites such as Facebook, or My Space. Many individuals use these sites to meet new friends, make connections, and upload personal information. These SNWs are now being used as reference

checks by human resource (HR) personnel. For this reason, SNW users, particularly university students and other soon-to-be job applicants. Although SNWs are a great way to be connected with friends, family, and friends-to-be, they can present problems when potential employers begin to search through them for information concerning job applications. Many potential employees would be mortified to learn that employers could potentially read the personal information posted on MySpace, Facebook, LinkedIn, or other SNWs. Besides, the posts on these sites might enlighten the employers about the applicants' activities even in their leisure time. A resume may be just a snapshot of a job applicant, while other personal information may be found online. Many job applicants have learned the hard way that what they post may come back to haunt them (Rodriquez, 2006)

Information that provide on the Facebook clearly give advantages to the employer. A study done by Waring R.L and F. Robert Buchanan F.R (2010) stated that. The Society of Human Resource Management (SHRM) maintains that once the candidate has been met, employers are obligated to consider the "whole of an applicant." This would include using all viable resources in getting some sense about an applicant's character and the soundness of their decision making (Fishman, 2009).

Marketing oneself online has been labeled personal branding by Beal and Strauss (2008) in their book Radically Transparent. They discuss the importance of creating a personal reputation using the Internet as your medium. Social network

Web sites provide a unique way for people to develop their own personal brand. These authors suggest that individuals control their online personal by putting information out there on several online resources such as MySpace, Facebook, LinkedIn, or other SNWs. Beal and Strauss (2008) make the compelling case that online activities can affect one's reputation.

The emergence of the internet has had subtle but profound changes in the way people search, locate, and access information and subsequently communicate, conduct business, and learn from each other. Online social networking (OSN), a platform that enables users to publicize personal information and to connect with others with similar interests, is one of the primary activities of Web 2.0 technologies. (Pew Internet and American Life Project, 2007). In addition, the continuous advancements in information technology is expected to visualize that OSNs will play a crucial role in future personal and commercial online interactions, as well as the location and organization of information and knowledge.(Michael, Khaldoon and Katherine.,2010) OSNs have recently gained significant popularity and are now considered among the most popular sites on the web; the purpose of such sites being to uniquely distribute information and products (Kim, Lee, and Hiemstra., 2004).

In 2007, Facebook was reported to have more than 21 million members with 1.6 billion generated page views each day (Needham and Company, 2007). In addition, a ComScore study indicates that from June 2007 to June 2008, Facebook

was the fastest growing SNS with 153 percent growth; growth that propelled Facebook past MySpace in total number of unique visitors (ComScore, 2008). Facebook, originally developed for college students, faculty, and staff has expanded to include high school, corporate, and geographic communities.

Several people are contented with higher risk-taking, based on their assumptions toward the social agreement where information that they revealed would be protected. Acquisti and Gross (2006) found that more than 75 percent of graduating students had created a social networking profile and were posting information about themselves. This study found that web site users were more comfortable with the possible risks of their disclosures being seen by others. In addition, this study found that males were higher in risk taking behavior than females. This is consistent with the literature on risk taking behavior where adolescents or young adult men have greater risk taking behavior than women (Huang, Gupta, Derevsky, & Paskus, 2007).

Individuals, no longer just consumers of information, now play a large part in creating content for others to consume (Tapscott and Williams, 2008). Much of this content is generated via SNSs, such as Facebook, MySpace, or LinkedIn .Today more than 700 million people worldwide have profiles, or collections of information about themselves, on SNSs (Comscore, 2010). Over the last five years, the number of users engaging SNSs within the United States has more than quadrupled, with now more than 46 percent of American internet users interacting

with SNSs (Lenhart, 2009). These statistics, coupled with increased attention in the popular media (e.g. Heining, 2009; Singel, 2007; Hardy, 2009) and from academics (e.g. Ellison, Steinfield. and Lampe, 2007; Tong, Van Der Heide, Langwell and Walther, 2008; Zywica and Danowski, 2008), suggest that SNSs are now playing a significant role in changing the meaning and methods of social connectivity (Boyd, 2007).

SNSs are publicly accessible virtual meeting places where users present information about them and view information about others. These sites have created a new medium for public self-expression that let individuals to connect with others who share an area of interest, but also possess the power to potentially shape public opinion, drive commerce, and change society (Klaassen, 2008; Wortham, 2009). The technologies underlying SNSs facilitate the flow of information in the form of text, photos, and videos ranging from the silly to the profound (Treese, 2006). This user-generated content is key to the success of social networking (Sullivan and Thaw, 2006). From a non-user's perspective, the content of these sites may seem to be only consumable information; however, the individuals who provide these materials are often constructing significant public self-expressions.

Three fundamental parameters of self-disclosure have been promoted in the literature (Altman and Taylor, 1973, Cozby,1973):

(1) Amount;

(2) Depth; and

(3) Duration.

Amount refers to the breadth of information disclosed, depth is associated with the intimacy of the information disclosed, and duration refers to the amount of time spent disclosing. Self-disclosure is a critical facilitator in the formation and development of interpersonal relationships (e.g. De Vito, 1986; Nakanishi, 1986;Laurenceau,Barrett, and Pietromonaco, 1998;Jourard, 1971) as it plays an important role in the formation of trust and can function as a social reward that facilitates relationship building (Worthy,Gary, and Kahn, 1969),

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 (Boyd and Ellison, 2007). In a study done by Patrick, Jacqueline and Brian 2010 shows that when 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 significantly on the site. Other information users contribute may include location (e.g. city, state, and country), political affiliation, religious affiliation, relationship status, and sexual preference. Patrick *et al*., 2010 mentioned in many cases users have the ability to self-disclose

additional information about themselves, such as general interests (e.g. hobbies), entertainment interests (e.g. favorite books, movies, music, or TV shows), photographs, and videos. All of these tools, either directly or indirectly, require users to publicly self-disclose information as they use them. Self-disclosure, both in the amount and depth, is the key to generating social benefits for SNS users, such as being connected to sources of support, opportunities, information (Donath and Boyd, 2004), creating shared identities, or feeling like users are part of a group (Joinson, 2008; Nicol, 2007). The more an individual discloses in the public space of the SNS, the more social connections they will be able to create (Sheldon, 2009), and presumably the greater the benefits they will derive from using the site.

Since the first years of the internet, scholars have examined the relationships between the internet and the public sphere. Some argued that the internet would create a new public sphere online, but found that only a lower quality duplication developing in a particular contexts (Dahlberg, 2001). However, with the emergence of SNSs, the relationship between the internet and the public sphere is becoming stronger. SNSs provide users with a greater ability to create rich online identities and describe their daily lives and happenings. These new public spaces, also known as a virtual public, are relatively transparent and open computer-mediated spaces that allow individuals to attend to and contribute to online interpersonal interactions (Jones and Rafaeli, 1999; Papacharissi, 2002; Aarseth, 1997; Carter, 2005).

As user-generated content is typically freely accessible to anyone, the public nature of a self-disclosure is increased (Goffman, 1963; Slevin, 2000). Further, because user content is stored within SNSs, it is persistent. This not only allows self-disclosures to be read, but also searched and read for an indefinite length of time by unknown future audiences. As a result, contributors lose control of their self-disclosures in an environment where the trustworthiness and morality of others who have access to the information is not governed (Ware, 1984). While individuals with profiles in social networking environments tend to have greater tolerance for risk taking (Fogel and Nehmad, 2009), all individuals seek to manage vulnerability and loss of face (Petronio, 2000). When individuals perceive too much vulnerability as a result of disclosure, they tend to become more concerned with information regulation (Derlega, Metts, Petronio, and Margulis, 1993). From the perspective of the SNS user, increased perceived publicness of a site will magnify the potential for detriment as a result of self-disclosing. As such, users who perceive a SNS to be more public will tend to regulate their disclosures and self-disclose less due to the increased risk.

### 2.2.3 Social Network as Platform of Interaction

Student life without Facebook is almost unimaginable. Ever since it's beginning in 2004, this popular social network service has quickly become both a basic tool for and a mirror of social interaction, personal identity, and network building among students. Social network sites deeply penetrate their users' everyday life and, as pervasive technology, tend to become invisible once they are

widely adopted, ubiquitous, and taken for granted (Luedtke, 2003). According to Boyd and Ellison (2008) specific privacy concerns of online social networking include inadvertent disclosure of personal information, damaged reputation due to rumors and gossip, unwanted contact and harassment or stalking, surveillance-like structures due to backtracking functions, use of personal data by third-parties, and hacking and identity theft.

In 2005, Jones and Soltren identified serious flaws in Facebook's set-up that would facilitate privacy breaches and data mining. Based on Jones and Soltren (2005) at the moment, nearly 2 years after Facebook's inception, users' passwords were still being sent without encryption, and thus could be easily intercepted by a third party. This has since been corrected. A simple algorithm could also be used to download all public profiles at a school, since Facebook used predictable URLs for profile pages (Jones & Soltren, 2005). Furthermore, the authors also noted that Facebook gathered information about its users from other sources unless the user specifically opted out. As of September 2007, the opt-out choice was no longer available but the data collection policy was still in force (''Facebook Principles,'' 2007). Even the most lauded privacy feature of Facebook, the ability to restrict one's profile to be viewed by friends only, failed for the first 3 years of its existence: Information posted on restricted profiles showed up in searches unless a user chose to opt-out his or her profile from searches (Jones & Soltren, 2005). This glitch was fixed in late June 2007, but only after a technology blogger made the loophole public and contacted Facebook (Singel, 2007). Recent attempts to

make the profile restrictions more user-friendly and comprehensive seem mostly PR-driven and still include serious flaws (Soghoian, 2008a).

Additional concerns have been raised about links between Facebook and its use by government agencies such as the police or the Central Intelligence Agency. Additionally, the Patriot Act allows state agencies to bypass privacy settings on Facebook in order to look up potential employees (NACE Spotlight Online, 2006).An online presentation ‘‘Does what happens in the Facebook stay in the Facebook?’’ (2007) points out a number of connections between various Facebook investors and In-Q-Tel, the not-for-profit venture capital firm funded by the CIA to invest in technology companies for the CIA’s information technology needs. The chief privacy officer of Facebook, Chris Kelly, accused the video of ‘‘strange interpretations of our policy’’ and ‘‘illogical connections’’ but did not substantially rebut the allegations (Kelly, 2007).

Moreover, the study by Jones and Soltren (2005) showed that 74 percent of the users were aware of the privacy options in Facebook, yet only 62 percent actually used them. At the same time, users willingly post large amounts of personal information—Jones and Soltren found that over 70 percent posted demographic data, such as age, gender, location, and their interests—and demonstrate disregard for both the privacy settings and Facebook’s privacy policy and terms of service. Eighty-nine percent admitted that they had never read the privacy policy and 91 percent were not familiar with the terms of service. This neglect to understand

Facebook's privacy policies and terms of service is widespread (Acquisti & Gross, 2006; Govani & Pashley, 2005; Gross & Acquisti, 2005). In their before and after study, Govani and Pashley (2005) noticed that most students did not change their privacy settings on Facebook, even after they had been educated about the ways they can do so.

Why do users on social networks such as Facebook reveal so much confidential and potentially embarrassing information, even if they sometimes know all the risks? This is the question asked by Professor Ronald Leenes of the University of Tilburg, speaking at the ENISA security conference in Greece. He said that there were well-publicized risks around using social networks, noting an example of British woman Hayley Jones who was allegedly killed by her ex-partner after changing her relationship status. Future employers could also look at profiles of employment candidates and finding embarrassing photos that could hurt their chances for getting the job. He used a video called from the 'Idiots of Ants' to illustrate how open we were to complete strangers, and highlighted that there was a Facebook quiz that illustrated the amount of information we are giving to app creators. It is also in the social networks' interest to keep data as long as possible, because the value of the network is in its size and the amount of information it had, according to Leenes. Leenes also revealed some of the reasons why people are open in becoming 'friends' with many different users, sometimes disclosing information to complete strangers. He said some were ignorant of the risks, while others assumed they had privacy on these networks. Some felt they had no choice

to join or be left out socially. “If ignorance is the case then we have to educate the kids about the risks," Leenes added. "You have to raise awareness. Tell the kids that their profiles may be open to other people other than their friends.” Leenes believed that many people are already aware of the risks of talking in such a public forum, but believes that they should have some form of privacy, especially if they are talking with friends. “It is a call for the re-establishment of the social more that you stay out of people’s conversations, unless you were invited to participate,” Leenes said. Other users felt that they had no choice and that “social” thinking over-rode any “logical” thinking that they had about keeping their privacy.

Research has also shown that students tend to disclose personal information on their profiles (Govani and Pashley 2005; Gross and Acquisti 2005; Tufekci 2008). For example, Gross and Acquisti (2005) found that 82 per cent of active Facebook users disclosed personal information such as their birth date, cell phone number, personal address, political and sexual orientation, and partner’s name. Tufekci (2008) has suggested that many students see a certain degree of information revelation as necessary to make SNSs useful: ‘why has a profile if your profile doesn’t say enough about whom you are?’( Acquisti & Gross 2005). Based on this previous research, we expect that student’s frequency of Facebook use will correlate with their disclosure of personal information on Facebook. That is, the more often students log into their Facebook accounts, the more information they would be likely to reveal.

Jenny Sundén (2003) argues that in order for individuals to exist online they must first write themselves into being. In SNSs, such as Facebook, the process of writing oneself into existence occurs through the creation of a profile, which reveals personal information about the user. Thus Lampe et al. (2007) suggest that the inclusion of profile elements, such as a self-description, a statement of relationship status, a description of one's interests, and a photograph of oneself, enables users to signal aspects of their identity, which assist other users in making decisions about declaring friendship links. However they also argue that the ability to search SNS profiles reduces the amount of time spent locating former high school friends, current classmates, or people located in the same university or college dormitory. Furthermore, research has shown that users with larger social networks are often more forthcoming and open with their personal information on these sites. For example, Jones and Soltren (2005) revealed that users with more than three hundred friends disclosed more information concerning their interests (85.3 per cent compared to 64.1 per cent), favorite music (82.9 per cent compared to 64 per cent), and clubs (81 per cent compared to 51.5 per cent) than users with comparably smaller social networks.

Moreover research has demonstrated that general concern for Internet privacy has an effect on the information revelation behaviors of Internet users (Pew 2000; Viseu,Clement and Aspinall 2004). A 2000 Pew Internet survey reports that out of 45 per cent of individuals who have not provided real personal information to access a Web site, 61 per cent identify themselves as 'hard-core privacy

defenders.' Therefore these individuals refuse to provide personal information to use an Internet site because they believe that Internet tracking is harmful, that their online activities are not private, and that there is a need to be concerned about businesses obtaining their personal information. Research has also suggested that individuals with a comparably low level of concern for Internet privacy tend to be much more forthcoming and open with the disclosure of their personal information online. Viseu et al. (2004) found that online users who believe that privacy is only a concern once it has been lost or breached were inclined to perceive the benefits of disclosing personal information in order to use an Internet site as greater than the potential privacy risks. Furthermore, Joinson,Reips, Bucanan and Paine (in press) in their study examining privacy, trust and self-disclosure online found that trust and perceived privacy had a strong affect on individuals' willingness to disclose personal information to a web site. They also indicate that individuals' trust in the privacy threat – that is, the likelihood that a privacy breach will occur – influences their information revelation decisions.

On the other hand the literature on privacy online has suggested that Internet users are generally concerned about unwanted audiences obtaining personal information. Fox et al. [2000], report that 86 per cent of Internet users are concerned that unwanted audiences will obtain information about them or their families, 70 per cent are concerned that hackers will access their credit card information, and 60 per cent are concerned that someone will find out personal

information from their online activities. Acquisti and Gross (2006) found similar results, showing that students expressed high levels of concern for general privacy issues on Facebook, such as a stranger finding out where they live and the location and schedule of their classes, and a stranger learning their sexual orientation, name of their current partner, and their political affiliations. Despite these concerns, research has also shown that users continue to disclose personal information and often disclose accurate personal information online (Acquisti and Gross 2006; Govani and Pashley 2005; Gross an Acquisti 2005; Pew 2000; Tufekci 2008; Viseu et al. 2004). In their examination of information sharing and privacy on Facebook, Acquisti and Gross (2006) revealed that 89 per cent of students used their full name on their profiles, 87.7 per cent had disclosed their birth date and 50.8 per cent had listed their current address. Tufekci (2008) found that concern about unwanted audiences had an impact on whether or not students revealed their real name in MySpace and whether or not students revealed their religious affiliation on MySpace and Facebook. Therefore, there may be an association between an individual's concern about unwanted audiences accessing his or her profile and the amount and types of information he or she chooses to reveal on Facebook.

Govani and Pashley (2005) investigated student awareness of the privacy issues and the available privacy protection provided by Facebook. They found that the majority of the students are indeed aware of possible consequences of providing personally identifiable information to an entire university population (such as, risk of identity theft or stalking), but nevertheless, feel comfortable enough in providing their

personal information. Even though they are aware of ways to limit the visibility of their personal information, they did not take any initiative to protect the information (Govani & Pashley, 2005). In another study, Tow at al. (2008) conclude that users are often simply not aware of the issues or feel that the risk to them personally is very low, and have a naïve sense that online communities are safe.

Conversely, based on Alyson and Anabel (2009) the results suggest that students not only ‘say they are concerned’ about privacy on the Internet, they also make a concerted effort to protect themselves against possible invasions by withholding personal information on their profiles. The students have their own approach in order to protect their profiles. The strategies used most often by students to protect themselves were the exclusion personal information from their profiles, the use of private email messages to communicate, and alteration of the default privacy settings. (DeCew 1997; Goldie 2006)

All of these communicative features elude to what Halbert (2009) has referred to as the undefined nature of privacy on Facebook, which "provides opportunities for voyeuristic surveillance." (Halbert 2009). According to Halbert (2009), Facebook has become the equivalent of a "public space" (Halbert 2009), where users are under constant surveillance from various sources. This issue has been widely publicized, and various forms of media have coined the term "Facebook stalking", which "is typical, if not implicitly encouraged" (Dubow 2007) in these networks. Due to Facebook's disposition as a highly public means of communication, there are many privacy concerns that are yet to be resolved.

Theorists have attempted to resolve these issues by researching the processes of electronic communication, and more recently through attempting to redefine the concept of privacy in cyber networks.

### 2.2.4 Social Network and Online Activity

Without we realize connecting with SNS actually are exciting spaces on the Internet for attractive in privacy (Albrechtslund 2008). By virtue of being public and popular, SNS make evident privacy problems elsewhere on the Internet e.g. emails, discussion forums, chats, e-commerce etc. In no other web applications are the user communities so actively involved in privacy debates. We also assume that privacy is not something concrete, in consensus and in constant danger. Rather, we conceive privacy as a set of practices to negotiate which should remain public or private in social contexts (Phillips, 2004). Legal and other regulatory frameworks and various social mechanisms are there to ensure that individuals can practice their privacy (Gutwirth 2002, Nissenbaum 2004).

SNS are not free of common privacy breaches like communication intrusion, identity theft, phishing, stalking, information leakage etc. (ENISA 2007). However, certain characteristics of SNS open up possibilities for new kinds of privacy breaches. These breaches primarily result from the fact that users reveal detailed information to the public and map their real-life social relationships more explicitly than they would in emails or on public forums.

Facebook's own data reveals that this is a world in which 25 percent of users cannot find the security settings provided by the website, leaving them at the mercy of the default settings (Vander Veer,2008). Only 66 percent of teenage users report using their privacy settings to limit access to their profile in any way (Lenhart & Madden, 2007). Meanwhile, despite a growing awareness of the importance of their "digital footprint," the trail of personal information left behind by internet activity, only 3 percent of internet users monitor their online presence with any regularity (Madden, et al., 2007).

Studies of user behavior suggest that a significant minority are misinformed about how private their information truly is. Information that many users think is private can often be easily accessed by other users (Acquisti & Gross, 2006). To further complicate matters, there is a limit to how much control is helpful to consumers (Flatow, 2008). In fact, too many privacy options may lead to users making poorer choices about their privacy by confusing them (Flatow, 2008). For example, letting users define that only their self-designated "friends" can see blog posts can be helpful for ensuring privacy, but giving users multiple definitions of friends (ex: work friends, Tennessee friends, college friends) who all access the same profile, can actually lead to users to make more information about themselves available than if they were offered fewer, but easier-to-understand, choices (Flatow, 2008).

Research claimed by Fernandez (2008) that two facts are stand out. One is the realization that social networking sites are not truly neutral spaces. They are controlled spaces whose owners have a vested interest in promoting certain activities over others. Often the interests of the user and the site correspond, but not always. Librarians must also understand that these sites are an inherently moving target. As with most things on the Internet, social networking sites are not static and can change rapidly. While it does not currently appear to be a problem, future updates to the sites could potentially track how people use library profiles; collect information about how their users access the library catalogue, or perhaps most worryingly, do something else entirely that librarians cannot anticipate

An article on Wired.com from June 2007 shows details how user's privacy is compromised by Facebook search engine. On the day it was published, it had numerous updates and revisions as facts changed. The types of privacy concerns changed and mutated as the day went on. A similar article by the same author appeared on the ABC news website the next day, without any indication of the rapid changes in the situation. Viewing these articles side by side illustrates how deceptive a stable print article can be in this context, and how even recent newspaper articles can be out of day just days later (Singel, 2007a, 2007b). More recently, both MySpace and Facebook have added features to make it easier for users to share their data on other websites, pushing their profile out into the rest of the Internet (Greenwood, 2008). In order for users to maintain control of their information, they must remain constantly informed about changes. Libraries with

profiles on these pages will need to remain vigilant as these websites morph and take new shape. A social networking site that poses no confidentiality concerns one day can change its policies almost instantaneously within the limits of the law. These realities do not mean that libraries have an obligation to avoid social networking sites. But they are relevant when considering exactly how a library should implement and interact with these sites

Tufekci (2008) stated that students tend to use their real names and engage in high levels of self disclosure, especially on Facebook. Facebook allows users to 'tag' individuals on photographs uploaded to the site, which means identifying the person in the photograph and thereby linking the picture to that person's profile, and thus creating a searchable digital trail of a person's social activities. A 'news feed' feature shows what one's 'friends' have been doing on the site: a typical entry might read 'Sally has Left a Message on Jim's Wall', or 'Alice and Bob are now friends'. All of this activity is framed by semi-public comments people leave on each other's profiles – short salutations, humorous repartee and more. A profile on an SNS is not a static entity; rather, it is a locus of social interaction that evolves and changes to reflect various dynamics within social networks and communities.

Much of the activity on an SNS can also be conceptualized as a form of presentation of the self, in the sense of Goffman (1959). Users engage in impression management by adjusting their profiles, linking to their friends,

displaying their likes and dislikes, joining groups, and otherwise adjusting the situated appearance of their profiles (Boyd & Heer 2006; Lampe et al.2007; Tufekci 2008).

Dunbar's notion of social grooming and Goffman's concepts of the presentation of the self and impression management are complementary aspects of the construction of the social self. As Goffman articulated, 'for a complete man to be expressed, individuals must hold hands in a chain of ceremony' (Goffman 1956, p. 493). It is through social interaction and socially embedded public or semi-public action that we affirm our relations, construct our status and ultimately produce the social 'me' in the sense proposed by Mead (1934).

The expressive Internet has been expanding rapidly, a process often described in the popular press as the rise of social computing. Studies show that these tools have been assimilated as a means of social interaction and social integration for increasing numbers of people and communities (Haythornthwaite 2005; Quan-Haase 2007), and that people are increasingly using the expressive Internet in ways that complement or further their offline sociality (Wellman et al. 2001; Hampton & Wellman 2003; Hampton 2007).

Ever since SNS became mainstream, they have been rebuked for playing an active role in the 'privacy nightmare' on the Internet. SNS are held responsible for the naive voluntary auto-profiling of Internet users. Users of SNS are accused of

being uninformed, in contradiction with their privacy concerns, or simply giving in to a badly conceived trade-off between their privacy and functionality (Berendt et al. 2005). These viewpoints currently dominate the privacy debate on SNS in academia and the media.

Philips (2004) in his study assumes that privacy is not something concrete, in consensus and in constant danger. Rather, conceive privacy as a set of practices to negotiate which should remain public or private in social contexts. Legal and other regulatory frameworks and various social mechanisms are there to ensure that individuals can practice their privacy (Gutwirth 2002, Nissenbaum 2004).

SNS are not free of common privacy breaches like communication intrusion, identity theft, phishing, stalking, information leakage etc. (ENISA 2007). However, certain characteristics of SNS open up possibilities for new kinds of privacy breaches. These breaches primarily result from the fact that users reveal detailed information to the public and map their real-life social relationships more explicitly than they would in emails or on public forums.

At the same time, these public revelations have an advantage when it comes to privacy. Users act as a community to notice and inform each other of privacy problems and on ways to avoid them. They use their relationships to put pressure on SNS providers to make the relevant changes. Furthermore, user interaction might help to identify conflict in privacy interests, leading users to ask for

mechanisms to negotiate these conflicts. In this sense, SNS are an interesting domain for promoting privacy practices on the Internet that are not only motivated by the profit interests of providers. They therefore provide an interesting opportunity for doing user-driven privacy design (Gürses et. al, 2008)

Although all SNS offer some privacy controls by now, the functional effects are often not transparent enough. Previous studies suggest that users often use default settings (Mackay 1991, Gross 2005). Studies on Facebook suggest that users unwittingly make mistakes in their privacy configurations, find them time consuming (Lipford et al. 2008), or simply assume that their profiles are private (Rosenblum 2007).

SNS providers have an interest in the wide release of data to a greater audience and to third-party providers. In its Privacy Policy (PP), Facebook admits that part of the user profiles may be made available to third party search engines (Facebook PP 2008). This may conflict with the users' interest to determine the visibility of their data is likely to cause indeterminate visibility and requires legal as well as social intervention

### 2.2.5 Social Network and Internet

For the past five years, social networking sites have increase rapidly from a niche activity into a phenomenon that engages tens of millions of internet users. The

quick-tempered growth in the popularity of these sites has generated concerns among some parents, school officials, and government leaders about the potential risks posed when personal information is made available in such a public setting.

Survey conducted by Pew Internet and America Life Project claim 48% of teens visit social networking websites daily or more often; 26% visit once a day, 22% visit several times a day, 91% of all social networking teens say they use the sites to stay in touch with friends they see frequently, while 82% use the sites to stay in touch with friends they rarely see in person and 72% of all social networking teens use the sites to make plans with friends; 49% use the sites to make new friends.

Still, the survey also recommends that today's teens face potential risks associated with online life. Some 32% of online teenagers (and 43% of social-networking teens) have been contacted online by complete strangers and 17% of online teens (31% of social networking teens) have "friends" on their social network profile who they have never personally met. On the other hand Alan Westin divides people into three groups. On one end of the spectrum is a minority of the population (25%) that are 'privacy fundamentalists,' deeply concerned about privacy rights, and on the other end is one fifth that are 'privacy unconcerned' (Buskin 2000). The majority (55%) are people that Westin identifies as 'privacy pragmatists,' individuals who tend not to mind personal data collection as long as

they feel informed about the solicitor, the possible gains or repercussions of releasing the information, and the safety measures put into place (Buskin 2000)

According to Harvey Jones and José Solton, "Facebook is undermined by three principal factors: users disclose too much, Facebook does not take adequate steps to protect user privacy, and third parties are actively seeking out end-user information using Facebook.8" Not only are privacy protection default settings inadequate, social networking sites often discourage users from altering default settings. Part of the research conducted by Gross and Acquisti involved determining if Facebook.com users provided real and accurate information. They found that 89% of users use their real name and, after considering a multitude of variables, they concluded that users are "by large, quite oblivious, unconcerned, or just pragmatic about their personal privacy.

If users were anxious about their privacy, and aware of the alteration that could be made to the default privacy settings, many social networking websites would be able to offer a substantially higher level of privacy protection. When considering the capabilities of Facebook.com to offer user protection, Jones and Solton explain that "From a systems perspective, there are a number of alterations that can be made, both to give the user a reasonable perception of the level of privacy protection available, and to protect against disclosure to intruders." However, since the main goal of social networking sites is to maintain a connection between users' profiles and their real world identities for the purpose of networking, the responsibility of privacy protection often falls solely on the individual. As a

result, “lasting change in online privacy will only come from a gradual development of common sense regarding what is appropriate to post in social networking forums (Jones and Soltren)” While the general consensus, from both experts and users, is that it is not the duty of social networking sites to ensure users’ privacy, social networking websites differ greatly in the amount of protection they initially provide and in the extent to which they will further provide protection.

According to Harvey Jones and José Soltren, “The environment that Facebook creates should be one that fosters good decision-making” so that “privacy should be the default, encryption should be the norm, and Facebook should take strides to inform users of their rights and responsibilities.” In fact, compared to other social networking sites, Facebook.com does a good job of providing its users with an effective level of default privacy protection. Users are provided with the default setting that no persons outside of their network can have access to their profile. For example, a student at UCLA cannot access the Facebook profile of a student at Harvard College. Moreover, privacy settings can be further restricted on Facebook.com with comparative ease. Upon realizing the varying degree of privacy protection that can be maintained by social networking sites we developed a five tiered categorization of social networking sites.

A new survey and a series of focus groups conducted by the Pew Internet & American Life Project examines how teens understand their privacy through

several lenses: by looking at the choices that teens make to share or not to share information online, by examining what they share, by probing for the context in which they share it and by asking teens for their own assessment of their vulnerability. For many online teens, particularly those with profiles, privacy and disclosure choices are made as they create and maintain social networking profiles. Of course, material shared in a profile is just one of many places where information is shared online – but it provides a snapshot into the choices that teens make to share in a relatively public and persistent online environment. Further, we went on to examine the interactions teens have with people unknown to them on social networking sites, exploring the nature of new friendships created on the networks, as well as unwelcome, and sometimes uncomfortable or scary stranger contacts.

Most teenagers are taking steps to protect themselves online from the most obvious areas of risk. The new survey shows that many youth actively manage their personal information as they perform a balancing act between keeping some important pieces of information confined to their network of trusted friends and, at the same time, participating in a new, exciting process of creating content for their profiles and making new friends. Most teens believe some information seems acceptable – even desirable – to share, while other information needs to be protected

### 2.2.6 Social Network and Daily Life

What does online mean in 2006? It is understandable that it means anything digital, from any source, at any time. Other than that, it also can be understood as the need to filter and evaluate has become increasingly critical if they are to have any meaningful role in a world of information overload and doubtful quality. Thus, we must be much better at anticipating our clients' desires, better at helping them become critical consumers of information, and better at promoting ourselves by virtue of the quality and timeliness of what we are best at: informing, educating, challenging.

As reported by USA TODAY Facebook was open to public in 2006. Whereby when Facebook first launched two years ago in 2004, it was only open to people who had valid college e-mail addresses. Last time, the site opened up to high school students. And after that, it opened up to selected work networks. Now in 2006 it will be open to virtually anyone.

Student who sign up for Facebook account tend to reveal as much information that they wanted to. According to Terremark Worldwide, Inc. with this much detailed information arranged uniformly and aggregated into one place, there are bound to be risks to privacy. University administrators or police officers may search the site for evidence of students breaking their school's regulations. Users may submit their data without being aware that it may be shared with advertisers.

Third parties may build a database of Facebook data to sell. Intruders may steal passwords, or entire databases, from Facebook.

Harvey Jones and Jose Hiram Soften (2005) explored that student want to sign up for Facebook as soon as possible before entering college. Thus, they found that Facebook was firmly entrenched in college students' lives, but users had not restricted who had access to this portion of their life. In addition they discovered that questionable information practices with Facebook, and found that third parties were actively seeking out information.

Govani and Aquisti (2005) noted that information revelation can work in two ways: by allowing another party to identify a pseudonymous profile through previous knowledge of a subject's characteristics or traits; or by allowing another party to infer previously unknown characteristics or traits about a subject identified on a certain site.

To whom may identifiable information be made available? First of all, of course, the hosting site, that may use and extend the information (both knowingly and unknowingly revealed by the participant) in different ways. Obviously, the information is available within the network itself, whose extension in time (that is, data durability) and space (that is, membership extension) may not be fully known or knowable by the participant. Finally, the easiness of joining and extending one's network, and the lack of basic security measures (such as SSL logins) at

most networking sites make it easy for third parties (from hackers to government agencies) to access participants data without the site's direct collaboration (already in 2003, Live Journal used to receive at least five reports of ID hijacking per day). Defenses lacking at social network sites.

Moreover according to Govani and Aquisti (2005) despite the fact that privacy may be at risk in social networking sites, information is willingly provided. Different factors are likely to drive information revelation in online social networks. The list includes signaling because the perceived benefit of selectively revealing data to strangers may appear larger than the perceived costs of possible privacy invasions; peer pressure and herding behavior; relaxed attitudes towards (or lack of interest in) personal privacy; incomplete information (about the possible privacy implications of information revelation); faith in the networking service or trust in its members; myopic evaluation of privacy risks or also the service's own user interface, that may drive the unchallenged acceptance of permeable default privacy settings (J. Donath and d. boyd,2005)

Many users befriend other users "even if they are precarious acquaintances or absolute strangers" (Majmudar 2005) on the Facebook, but not in a non-cyber environment. Since a number of strangers whom a user categorizes as friends have access to that user's profile, there may be privacy concerns. Hughes fields questions of privacy concerns by commenting that all of the information "has been available inside university systems already" (Majmudar 2005). However, it was noted in a comparison done at UNC by Stutzman that Facebook prompts

users to enter much more personal and social information than is asked for by the university directory (Stutzman, Evaluation 2005). The article by Majmudar brings up the point that users have extensive privacy options. It asks whether Facebook should be considered privacy concern if it gives users options (Majmudar 2005). In answer to this question, an article by Bridget Whelan shares students' comments saying that the site has an element of "'creepiness'" (Whelan 2005) and causes fear of stalking among some students (Whelan 2005). The article notes that Facebook has popularized stalker like behavior and has become a popular word on college campuses. The difficulty in resisting "the overwhelming urge to anonymously check up on old high-school acquaintances" (Whelan 2005) keeps users addicted to the site and open to looking up people and sharing their information with other users. The article doesn't conclude whether the site is merely a fun resource or a privacy invasion, but it gives students' view points on both sides of the "Internet craze" (Whelan 2005).

Reasons for Facebook's popularity as a campus networking tool over other campus networking tools include the depth of information that is encouraged by the site to be shared, viewable social networks, course tracking, and the ability to post messages for all users to see (Agraz 2004). There are also features that integrate into other services like linking an AIM away message to a user's profile and viewing a school newspaper article in which a user was featured (Agraz 2004). Features like these aren't available for all users, but many users that have them don't realize that supplemental information is attached to their profile

(Acquisti 2005). Where to draw the line between a useful feature and an invasive feature is what researches grapple over.

Users on Facebook can share a multitude of different types of data with others users. These types of data include contact information, personal information like gender, birth date, hometown, and school concentration, information regarding interests in movies, music, clubs, books, relationship status and partner, and political affiliation ( Govani and Pashley 2005) Users can in fact choose to fill in any of this information and update their information at any time. They found out that a majority of users do provide most of this information. Because the information on Facebook is personally identifiable, there is a risk that the information given by the user could be abused by stalkers or identify thieves (Wheelan 2005). A less severe consequence is that the information posted by a student will be read by individuals the information was not intended for, like university officials or other family members (Schweitzer 2005). Furthermore, information provided by students could be mined and stored for future reference. While students may not see the information they provide as a threat to their future at present, if running for political office or if they are put in the public eye for any reason the information can be published. Information could potentially be used by future employers or the government for judgment of character.

The relation between privacy and a person's social network is multi-faceted. In certain occasions we want information about ourselves to be known only by a

small circle of close friends, and not by strangers. In other instances, we are willing to reveal personal information to anonymous strangers, but not to those who know us better. (Gross and Auqisti 2005)

The extent to which user's disclose personally identifiable, private information on Facebook, has also been highly publicized in the media, typified in an article from The Boston Globe, stating that "the scope of Facebook impact may not be felt for years to come." (Schweitzer 2005). Many theorists side with this notion, believing the consequences of identity disclosure in young users may not be perceptible for many years.

With the growing popularity of online social networks, more and more personal information is being displayed on websites. This is despite the fact that privacy groups advise Internet users not to “reveal personal details to strangers or ‘just-met friends” (McCandlish 2002). Privacy groups cite social consequences of risky online behavior as harassment, stalking, and spamming (“Privacy in Cyberspace” 2005). While Internet users may feel safe behind their computers, they have “zero privacy” (Regan 2003).

Third parties can access participants‟ information without the site’s direct collaboration (Gross & Acquisti, 2005). The easiness to join and extend one’s network, and the lack of basic security measures (such as cryptographic protocols for providing secure communications on the Internet, e.g. TLS/SSL logins) in

most networking sites makes it easy also for malicious third parties, such as identity thieves, to access and misuse the users information. In the case of Facebook, third parties with permission, that is, third party application providers, have a right to access users‟ data when a user adds their application

Today people communicate more and more using digital technology, such as e-mails, instant messengers, and social networking sites. When using different online services, for instance, e-shopping or the Internet forums, the users generate a wealth of data about themselves. These electronic footprints enable third parties to build up a picture of the users‟ behavior. Even if technology and information systems are a part of everyday life for most people in developed countries, modern information and communications systems are very complex and can be confusing: the users commonly have no idea what sort of data is being gathered about them, how much, where it is held, how long it will be held, and what it will be used for (German Federal and State Data Protection Commissioners, 1997).

From the legal viewpoint, privacy is mainly protected by general human and constitutional rights, and by more specific data protection rules. The European Union has been leading the development of the data protection law, which has arguably resulted sometimes even too strict rules. However, with respect to new kind of services, such as SNSs, the laws still fail to cover them adequately. The data protection law is designed to protect individuals against malicious criminals

and overactive businesses, but it hardly stipulates social relationships between human beings

## 2.3 Conclusion

Based on the literature review it is proven that SNS has become famous year by year. Every year the users are increasing on the social site. Facebook, Twitter or MySpace have their own followers. Phenomena of Facebook have become the social site since it opened to everyone on September 2006. Since then the followers or users of Facebook keep increasing year on year. Once the users involved in Facebook they must provide their personal information such as name, email, status, sex, photos and etc. The personal information that they provided found on the literature review usually are accurate. However, the users do not hesitate to provide what they have. Even though the issue arise is about internet privacy, they keep provide the accurate information to the public. Generally they are aware about the privacy concern nevertheless the users continued to give the information about them. When talking about internet privacy, on the literature review users basically changed the privacy setting (default setting) that Facebook offered For example photos that they uploaded just can be seen by “only friends” or “everyone”.

Besides when the users frequently log in Facebook consequently it will encourage them to update their status, their profile, chatting with their friends as well as uploaded their pictures. By updating the information without they realize they are giving the current or the present situation for instance where they have been, who they met, and etc. The more often they log in the more information that they will revealed. And thus the information

they provided is true. Indeed when News Feed had been appear in Facebook it much easier for the users as the News Feed is the center column of their home page, where as it is a constantly updating list of stories from people and Pages that they follow on Facebook. News feed stories include status updates, photos, videos, links, app activity and likes. How many friends do the users have? Based on the research done on average users have more than 200 friends in their friend list. Users usually accept or request the friend from university, high school or people they may know to be their friend. Surprisingly, even if the person they had met just once they will accept to their friend list. Therefore as result information that the users reveal known by the person that they just met once! However it is not stopped them to reveal the information. Other than that nowadays some company used the personal information contained on Facebook site to assess the user's stability before hiring them. Too much information revealed can become advantages or disadvantages to the users. Beside that there are some university admissions officers have started using the personal information on Facebook sites to assess applicant suitability prior to offering admissions; the question is the users are concern about unwanted audiences such future employer, corporations or university administrators and thus they revealed too much information? Even political parties and police officers have begun using Facebook to track prospective users in order to dig up information they wanted. Last but not least, from the literature review based on the research done we can see that more and more people reveal information in spite of knowing hazard that they will face in the future.

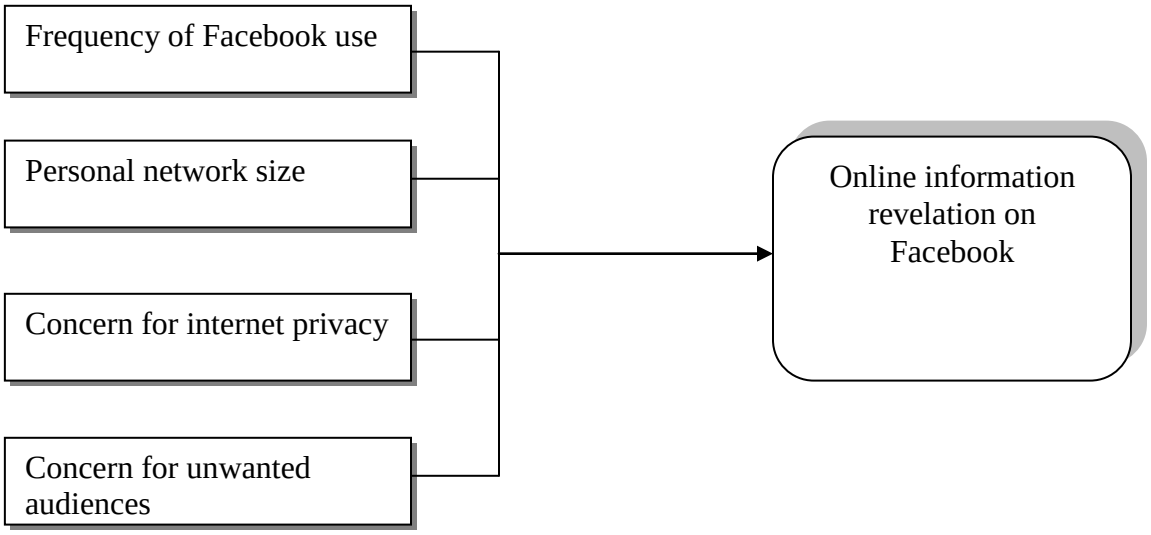
# CHAPTER THREE

# RESEARCH METHODOLOGY

## 3.0 Introduction

Based on the purpose of the research, this paper is a survey designed to obtain research evidence concerning on the online information revelation and privacy on internet-based of Facebook among University Utara Malaysia (UUM) postgraduates' students. To ensure that useful and reliable data collected, certain procedures were considered necessary in the selection of sample population and in the formulation of the questionnaire. This chapter will be explained more about method that using by the researcher in order to collect the data.

## 3.1 Research Framework and Variables Selection




Source: Adapted from Quan-Haase and Young (2009)

## 3.2 Hypothesis Testing

H1: Frequency of Facebook use will be positively associated with information revelation on Facebook.

H0: Frequency of Facebook use will be negatively associated with information revelation on Facebook.

H1: Facebook personal network size will be positively associated with information revelation of Facebook.

H0: Facebook personal network size will be negatively associated with information revelation of Facebook.

H1: Concern for internet privacy will be positively associated with information revelation of Facebook.

H0: Concern for internet privacy will be negatively associated with information revelation of Facebook.

H1: Concern for unwanted audiences will be positively associated with information revelation of Facebook.

H0: Concern for unwanted audiences will be negatively associated with information revelation of Facebook.

## 3.3 Sampling

### 3.3.1 Sample Size

The respondents were from University Utara Malaysia (UUM) City Campus postgraduates. Based on the students' statistic from Registrar Department in UUM City Campus, there was 1440 number of students' postgraduates. Therefore, according to the table of sample size for a given population (Krejcie and Morgan, 2003), the researcher need to have about 301 students as a samples.

### 3.3.2 Sampling Technique

According to Sekaran (2003), by using purposive sampling, each of the elements in the population has the equal opportunity and will be known by the researcher to be as subject for the research. It will be more clearly compared to collect data from the entire citizen. Researcher focuses on postgraduates' student at UUM City Campus in Kuala Lumpur as the respondents because this method is easy, quick and inexpensive and is the best way to collect some data for the research.

## 3.4 Questionnaire Development

Questionnaire is the main instrument of getting information from the students. It's also as a tool to record respondent answers, guideline to measuring variables of interest, simplifying the process of analyzing and interpretation of data. In this study, there were six sections which were, Section A, B, C, D, E, and F. Section A will be the demographic

profile which includes seven items. Section C, D, E and F will be independent variable which includes five to six items. Dependent variable served in Secton B consists ten items.

## 3.5 Pilot Test Results

The validity and reliability of this questionnaire were evaluated using a panel of experts, a pilot test (Cronbach, 1951). The survey was pilot tested prior to data collection on all items. The respondents were fifty (N=50) number of postgraduates students of UUM City Campus. A reliability analysis was conducted on each oh the constructs. The eleven (11) information revelation items, had a reliability of α =.61. The seven frequency of Facebook use items, had a reliability of α = .92. The eleven personal network size items, had a reliability of α = .31. Next, the four concern for internet privacy items, had a reliability of α = .42. The six concern about unwanted audiences items, had a reliability of α = .89. The eight privacy protection strategies items, had a reliability of α = .84. Coefficient alpha reliability tests run for each variable satisfied Nunally's (1978) criterion of .60 or higher as a standard for an exploratory research study, therefore, there was few items will be deleted in or order to get higher cronbach alpha. Table 3.5.1 showed the result for pilot test.

*Table 3.5.1 Pilot test before item deleted*

| Item | Cronbach's Alpha | N of Item |
|---|---|---|
| Information revelation | .61 | 11 |
| frequency of Facebook use | .92 | 7 |
| personal network size | .31 | 11 |

| | | |
|---|---|---|
| concern for internet privacy | .42 | 4 |
| concern about unwanted audiences | .89 | 6 |
| privacy protection strategies | .84 | 8 |

Few items in few sections were deleted in order to ensure the questions were reliable and valid to use in this study. Beside that, few items were deleted because to enhance the cronbach alpha more than $\alpha = .60$. Therefore, the researcher had deleted some items, and table 3.5.2 showed the result for the cronbach alpha after items deleted.

*Table 3.5.2 Pilot test after item deleted*

| Item | Cronbach's Alpha | N of Item |
|---|---|---|
| Information revelation | .64 | 10 |
| frequency of Facebook use | .92 | 7 |
| personal network size | .77 | 5 |
| concern for internet privacy | .60 | 3 |
| concern about unwanted audiences | .89 | 6 |
| privacy protection strategies | .84 | 8 |

## 3.6 Statistical Method

The data from the respondent was analyzed using Statistical Package for Social Science (SPSS) version 20.0. For this study, the data was analyzing by using descriptive statistics, an exploratory factor analysis (EFA) and regression analysis. Exploratory factor analysis (EFA) was to identify which factors that influenced information revelation among postgraduates' students in University Utara Malaysia (UUM). Besides, regression analysis was used to investigate the effect of one variable to the dependent variable.

# CHAPTER FOUR

# RESULTS

## 4.0 Introduction

This chapter will discuss about the result of the survey and investigation done by the researcher. The data that was gathered during the fieldwork has been analyzed by using a Statistical Package for Social Science (SPSS) program version 20.0. The survey results will be presented using the form of table and with the written statements. The questionnaires are formalized to obtain the information from the respondents. These questionnaires have been distributed to the respondents to get their feedback. There are 306 sets of questionnaires were distributed.

## 4.1 Overall Reliability Analysis

The overall section was tested using reliability analysis to prove its reliability with the questionnaires objective. As indicates in the Table 4.2.1 below, the Cronbach's alpha is referring to all independent variables of the study or represent as Section B, C, D, E, F and G in the questionnaires. All of these variables were studying about the information revelation, frequency of facebook use, personal network size, concern for internet privacy, concern about unwanted audiences and privacy protection strategies. The Cronbach's alpha for the 39 items measure is 0.872.

*Table 4.1.1 Overall Reliability Analysis*

| Cronbach's Alpha | N of items |
|---|---|
| .872 | 39 |

## 4.2 Demographic Profile

*Table 4.2.1 Demographic Profile*

| | Items | Frequency | Percent (%) |
|---|---|---|---|
| Gender | Male | 144 | 47.1 |
| | Female | 162 | 52.9 |
| | Total | 306 | 100 |
| Age | Less than 25 years old | 34 | 11.1 |
| | 25-30 years old | 127 | 41.5 |
| | 31-36 years old | 140 | 45.8 |
| | 37-42 years old | 5 | 1.6 |
| | Total | 306 | 100 |
| Type of Mobile | Blackberry | 86 | 28.1 |
| | iPhone | 65 | 21.2 |
| | Android | 119 | 38.9 |
| | Symbian | 16 | 5.2 |
| | Others | 20 | 6.5 |
| | Total | 306 | 100 |
| Type of Medium | Ipad | 50 | 16.3 |
| | Personal Computer | 21 | 6.9 |
| | Laptop | 52 | 17.0 |
| | Mobile Phone | 167 | 54.6 |
| | Tablet | 16 | 5.2 |
| | Total | 306 | 100 |
| | | | |

| | | | |
|---|---|---|---|
| Income | Below RM 1000 | 26 | 8.5 |
| | RM 1000 – RM 2000 | 25 | 8.2 |
| | RM 2001- RM 3000 | 141 | 46.1 |
| | RM 3001 and above | 114 | 37.3 |
| | Total | 306 | 100 |

Table 4.2.1 shows the results of the demographic information indicated that the samples are from University Utara Malaysia (UUM) postgraduates' students. The demographic variable analyzed in this study is gender, age, and type of mobile, type of medium and personal income. In this study, (N=306), the following demographic characteristics of the sample were found. Female present the highest percentage than male which was 52.9% while male was 47.1%. The age group included 45.8% for 31-36 years old, 41.5% for 25-30 years old, followed by less than 25 years old, 11.1% and the least was 37-42 years old, 1.6%. Besides, android showed the highest percentage which was 38.9%, followed by, blackberry, iphone, others and the lowest was symbian, 5.2%. For the type of medium, most of the postgraduates' students were used mobile phones which present 54.6%, followed by laptop, ipad, personal computer and the lowest percentage was tablet, 5.2%. In addition, for the personal income range between RM 2001- RM 3000 showed higher percentage compared to others which was 46.1%. the least was range between RM 1000- RM 2000 present 8.2%.

## 4.3 Mean and Standard Deviation

*Table 4.3.1 Mean and Standard Deviation for Four Variables*

| | M | SD |
|---|---|---|
| Information Revelation | 1.43 | 0.429 |
| Frequency of Facebook Use | 4.45 | 1.788 |
| Personal Network Size | 1.71 | 0.451 |
| Concern for Internet Privacy | 3.10 | 0.787 |
| Concern about Unwanted Audiences | 3.22 | 1.134 |

Table 4.3.1 showed that the highest mean for four independent variables was frequency of Facebook use, 4.45 with standard deviation 1.788. Followed by concern about unwanted, 3.22 with standard deviation was 1.134. Next was concern for internet privacy with mean 3.10 and the standard deviation was 0.787. The lowest mean among four independent variables was personal network size with mean 1.71 and standard deviation was 0.451.

## 4.4 Mean and Standard Deviation for Privacy Protection Strategies

*Table 4.4.1 Privacy Protection Strategies*

| | M | SD |
|---|---|---|
| I have excluded personal information on Facebook to restrict people i don't know from gaining information about myself | 3.88 | 1.069 |
| I have provided fake or inaccurate information on Facebook to restrict people i don't know from gaining information about me | 3.19 | 1.145 |
| I have sent private email messages within Facebook instead of posting messages to a friend's wall to restrict others from reading them message | 4.09 | 1.006 |

| | | |
|---|---|---|
| I have blocked former contacts from contacting me and accessing my Facebook profile | 2.97 | .991 |
| Certain contacts on my Facebook site only have access to my limited profile | 3.84 | .999 |
| I have changed my default privacy settings activated by Facebook | 4.05 | .977 |
| I have deleted messages posted to my Facebook wall to restrict others from viewing/reading the messages | 3.59 | 1.196 |
| I have untagged myself from images and/videos posted by my contacts | 3.46 | 1.179 |

Table 4.4.1 shows the mean for privacy protection strategies. From the result the highest mean is 4.09, that is *I have sent private email messages within Facebook instead of posting messages to a friend wall to restrict others from reading them message*

## 4.5 Regression Analysis

*Table 4.5.1 Summary of Regression Analysis*

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .962 | .926 | .925 | .18161 |

Table 4.5.1 shows the model summary of the regression analysis for the variables and R (0.962) is the correlation of the four independent variables. The R Square 0.926 or 92.6% explained the variance, meanwhile the remaining 0.074 or 7.4% variance were unexplained by the independent variables. It indicated that 92.6% of the variance (R

square) in information revelation has been significantly explained by the four independent variables which are frequency of Facebook use, personal network size, concern for internet privacy, and concern about unwanted audiences.

*Table 4.5.2 Coefficients Regression*

| Model | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. |
|---|---|---|---|---|---|
| | B | Std. Error | Beta | | |
| 1 (Constant) | .289 | .075 | | 3.858 | .000 |
| Mean frequency of Facebook use | .305 | .009 | .708 | 35.616 | .000 |
| Mean personal network size | .110 | .033 | .057 | 3.293 | .001 |
| Mean concern for internet privacy | .139 | .022 | .123 | 6.322 | .000 |
| Mean concern about unwanted audiences | .269 | .013 | .357 | 21.418 | .000 |

When referred to Table 4.5.2 on coefficients, all the independent variables had positive and strong significance correlated with dependent variable. This indicates that 0.926 or 92.60% adjusted R Square from table 4.6.1 were explained by all these four variables.

The most influence independent variable was frequency of Facebook use which Beta was 0.708 and followed by concern about unwanted audiences which Beta was 0.357. Concern for internet privacy was third which Beta, 0.123 and the lowest was personal network size which Beta 0.057.

## 4.6 Exploratory Factor Analysis

In this study, the researcher used Exploratory Factor Analysis (EFA) to identify factors that influence information revelation among University Utara Malaysia (UUM) postgraduates'. According to Coakes (2005), factor analysis is a data reduction technique used to reduce a large number of variables to a smaller set of underlying factors those summaries the essential information contained in the variable. Exploratory Factor Analysis (EFA) was performed with the principal axis factoring and varimax rotation. Cut off factor loading was set to 0.6. From this Exploratory Factor Analysis (EFA), results show that there are four (4) major factors. *Table 4.6.1.*outlined the factors.

### 4.6.1 Mean Scores, SD, Loading and Reliability for information revelation factors

*Table 4.6.1 Mean Scores, SD, Loading and Reliability*

| Item | Mean | SD | Loading | Reliability |
|---|---|---|---|---|
| Frequency of Facebook Use 4.45 | | | | |
| F:How often do you view your friend's status update? | 4.64 | 1.754 | 0.884 | 0.92 |
| F: How often do you chatting with your friend by using Facebook? | 4.32 | 1.622 | 0.860 | |
| F: How often do you update your status? | 4.31 | 2.007 | 0.844 | |
| F: How often do you update your profile on Facebook? | 4.20 | 1.919 | 0.831 | |
| F: How often do you respond to the notification on Facebook? | 4.58 | 1.618 | 0.790 | |
| F: How often do you upload pictures on Facebook? | 3.58 | 1.992 | 0.759 | |
| F: How often do you log in Facebook? | 5.53 | 1.566 | 0.695 | |
| Unwanted audiences 3.22 | | | | |

| | | | | |
|---|---|---|---|---|
| U:University admissions officers have started using the personal information on Facebook sites to assess applicant suitability prior to offering admissions. | 3.10 | 1.178 | 0.852 | 0.89 |
| U: Employers are using Facebook to monitor the extra-curricular activities of their employees | 3.08 | 1.030 | 0.847 | |
| U: Future employers will use the personal information contained on my Facebook site to assess my suitability with their company | 3.14 | 1.117 | 0.780 | |
| U: Universities are monitoring Facebook postings, personal information and images to identify university code violators (i.e. involvement in illegal activities) | 3.02 | 1.141 | 0.640 | |
| U: Police officers are using Facebook to track underage drinking and other illegal activities | 3.76 | 1.207 | 0.606 | |
| Personal Network Size 1.71 | | | | |
| P: Do you accept people you've met just once to be your friend on Facebook? | 1.66 | 0.473 | 0.772 | 0.77 |
| P: Do you accept people whom you haven't met to be your friend on Facebook? | 1.73 | 0.447 | 0.701 | |
| P: Do you request people you've met just once to be your friend on Facebook? | 1.75 | 0.435 | 0.686 | |
| Concern for Internet Privacy 3.34 | | | | |
| C: How concern you are about Facebook privacy setting? | 3.34 | 0.639 | 0.721 | 0.60 |

As we can see at the *table 4.6.1* above, frequency of Facebook use shows the highest mean, 4.45 and no questions was extracted. Followed by concern for internet privacy with the mean 3.34 but two questions was extracted. Next was concern about unwanted audiences which showed that one question was extracted with the mean 3.22.

Lastly, table above showed that the lowest mean was personal network size with the mean 1.17 and two questions were extracted. Factors with the internal correlation greater than 0.6 were used to explain the sample information revelation among postgraduates'

students. After the factor analysis of 39 studied items, 16 items remained and four factors attained to describes the sample information revelation. 23 items that were deleted due to low factors loadings.

### 4.6.1 KMO and Bartlett's Test

*Table 4.6.2 KMO and Bartlett's Test*

| | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy | | .781 |
| Bartlett's Test of Sphericity | Approx Chi-Square | 5134.440 |
| | df | 210 |
| | Sig. | .000 |

Based on *table 4.6.2* above, we can see that the Bartlett Test of sphericity is significant ($p<0.00$) and that the Kaiser-Meyer-Olkin measure of sampling adequacy is greater than .6 which is .781. Therefore, exploratory factor analysis (EFA) was suitable to be performed based on the data.

# CHAPTER FIVE

# DISCUSSION AND FUTURE RESEARCH

## 5.0 Introduction

This project paper needs to be conducted properly in order to gain better information and hence the result gathers will reliable. In this section generally talk about the limitations that faces throughout completed this project paper. After that discussion and arguments about the result finished and finally recommendation for future research that should take into consideration by others.

## 5.1 Limitation

This study had some limitations. The limitations were:

a) Time and financial constraints. For a small-scale research like this study, there Tend to be tight constraints on time and money. The researchers did not have the luxury of trying different approaches for the study if one approach did not work. Thus, the researcher only able to conduct a small scope of study to comply with the time specified. Due to this limitation, the researcher also facing the constraint to managing the data collection especially it involves with the survey.

b) Response from respondents

The researcher faced problem to get information from consumers. This is because the respondents did not give an appropriate feedback and co-operation. Another matter was the researcher difficult to get back the questionnaire from the

respondents and the researcher faced problems to collect the all data and information they need.

## 5.2 Discussion

The result on the demographic information indicated that majority of the sample was female which 52.9 per cent (52.9%) while male 47.1 per cent (47.1%). Next, the results reported that, the most users that appear to log in Facebook for UUM Postgraduates students are range from age 31-36 years old which make 45.8 per cent (45.8%) and age from 37-42 years old is the lowest users of Facebook (1.6%). Based on the result usually the type of medium that UUM Postgraduate used to surf Facebook is by using their mobile phone which 54.6 per cent (54.6%). It shows that by having mobile phone to log in the social webpage they can surf at anywhere and anytime they wanted to.

The second objective of this research is to identify UUM Postgraduate student information revelation practices on Facebook. After the exploratory factor analysis (EFA) has been tested, sixteen (16) of thirty nine (39) variables were recognized as the main questionnaire. The result of this analysis shows that frequency of Facebook use served as the highest mean (4.45) while personal network size is the lowest mean (1.71). It explained that the more frequent users log in Facebook the more information that they tend to reveal. Consequently, most of the information that revealed is truthful. It is supported by Govani and Pashley (2005), Gross and Acquisti (2005) and Tufekci (2008). In the research by Young and Quan-Haase (2009) they bring up that frequency of Facebook use will correlate with their disclosure of personal information on Facebook.

That is, the more often students log into their Facebook accounts, the more information they would be likely to reveal. On the other hand, their finding on personal network size state that users with larger social networks are often more forthcoming and open with their personal information.

The third objective is to investigate which factors that influence UUM postgraduate students' information revelation on Facebook. From the result the most influence factors is frequency of Facebook use. Therefore we can say that for this research among UUM postgraduate students they frequently update their profile, status or chatting with their friends and as a result this will lead to reveal personal information. It is supported by Johnson, Egelman and Bellovin (2011) whereby in their finding most of their participants reported using Facebook several times a day (68.8%), while very few participants said they log in less than once per week (5%). They also asked about the amount of time spent on specific activities: reading the newsfeed, creating new posts, or browsing friendless. In general, participants spend more time consuming content than they do creating content. On the other hand the lowest factor is personal network size. It shows that this variable did not affect much on information revelation. For example from the result if they have met people just once, they will not accept or request them as a friend, therefore they don't afraid of to reveal their personal information.

Moreover others variables were positively associated with users' information revelation practices. By contrast, the study by Quan-Haase and Young (2009) they find out that concern for internet privacy was negatively associated with user information revelation

practices where the student have high level of internet privacy and tended to disclose less personal information on Facebook.

Last objective is to examine students' privacy protection strategies on Facebook. There are several strategies that provided and each strategy has their unique characteristic. From the result the highest mean is 4.09 discovered that the UUM postgraduate student strategies to protect their privacy by sending email messages instead of posting messages to a friend's wall, followed by alteration of the default privacy setting and the exclusion of personal information from their profiles. This is similar with study that done by Quan-Haase and Young (2009) whereby the end result of the privacy practices by students from University in English Canada shows the same with UUM postgraduate students.

Other than that in this study the lowest mean is 2.97 where student do not blocked former contacts from accessing the Facebook profile to be a useful protective measure. The reason here because at the beginning when choosing their personal network UUM students mostly did not accept or request strangers to be in their friend list. For that reason the strategies had less chosen.

## 5.3 Future Research

The existing study has a number of boundaries. First, the information revelation scale is based on a limited number of items. Second, the model needs to consist of further variables, for example control variables, such as age, gender, and area of study. Third, the outcome of the study can only be generalized to university students. Upcoming research

could seem to be to develop the present study by examining other user groups, for instance high school or elementary school students, to scrutinize if their information revelation and privacy protection practices and behaviors on Facebook be dissimilar from those of university students.

## 5.4 Conclusion

The goal of this study was to determine online information revelation and privacy of Facebook of UUM postgraduate's students. This study focused on what factors that affects to the information revelation and privacy strategies that they practiced. As a conclusion can said that examining information revelation and privacy on Facebook requires the consideration of multiple factors. Every factor should take into considerations. Besides, difference in findings across studies is difficult to explain because they may be the result of changes happening to the audience in Facebook or differences in the culture of the country. Tufekci (2008) suggested students perceptions of the site may be differ in term of their behavior and information that they want to reveal. Many students may be more likely to withhold certain types of information from their profiles than they were before general audiences could join Facebook.

## REFERENCES


Acquisti, A. & Gross, R. (2006) Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, 6th Workshop on Privacy Enhancing Technologies, Robinson College, Cambridge University, UK.

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. In Danezis. G., & Golle, P. (Eds.), Privacy Enhancing Technologies (4258/2006, pp. 36-58). Heidelberg: Springer Berlin.

Agraz, Diana. (2004), ìMaking Friends Through Social Networks: A New Trend in Virtual Communication's Stanford.edu. Retrieved on October 2010 from <http://www.stanford.edu/ ~aneesh/NewFiles/Dian%20Agraz.pdf>.

Albrechtslund, A. (2008) "Online Social Networking as Participatory Surveillance", First Monday, (13:3).

Altman, I. and Taylor, D.A. (1973), Social Penetration: The Development of Interpersonal Relationships, Holt, Rinehart & Winston, New York, NY.

Berendt, B., Günther, O., and Spiekermann, S. "Privacy in e-commerce: stated preferences vs. actual behavior", Communications of the ACM, Volume 48, Number 4, pp. 101-106, 2005.

Boyd, D. (2007), "Social network sites: public, private, or what?", Knowledge Tree, Vol. 13.

Boyd,D.& Heer,J.(2006) Profiles as conversation: networked identity performance on friendster,in Proceeding of the Hawai International Conference on System Sciences, Persistent Conversation Track, IEEE Computer Society,47 January ,Kauai, HI.

Boyd,d.,& Heer,J. (2006,January). Profiles as conversation: Networked identity performance on Friendster. Paper presented at the proceedings of the Hawaii International Conference on System Sciences, Persistent Conversation Track,Kauai,HI.

Buskin,J.(2000). "Choice and Trust," *Wall Street Journal*, (April17),R 34.

Carter, H. L., Foulger, T. S., & Ewbank, A. D. (2008). Have you googled your teacher lately? Teachers'use of social networking sites; common sense doesn't necessarily prevail when teachers plunge into the world of social networking sites. disastrous consequences can ensue, and the authors urge educators to consider the potential outcomes before they post. Phi Delta Kappan, 89 (9), 681(685). Communication Research, Vol. 13, pp. 167-90.

ComScore (2008), "Social networking explodes worldwide as sites increase their focus on cultural relevance", comScore.com, August 12.

Comscore (2010), "Press releases", available at: www.Comscore.Com/press/pr.Asp . Retrieved on November 2012

Cozby, P. (1973), "Self-disclosure: a literature review", Psychological Bulletin, Vol. 79, pp. 73-91.

De Vito, J.A. (1986), The Interpersonal Communication Book, Harper & Row, New York, NY.

Derlega, V.J., Metts, S., Petronio, S. and Margulis, S.T. (1993), Self-disclosure, Sage Publications,Newbury Park, CA.

Dubow, B. 2007, 'Confessions of "Facebook Stalkers"', USA Today, from <http://www.usatoday.com/tech/webguide/internetlife/2007-03-07-facebook-stalking_N.htm>.

Emery, D. (2010, July 29). Details of 100 million Facebook users collected and published. BBC News. Retrieved from http://www.bbc.co.uk/news/technology-10796584.

Emery, D. (2010, July 29). Facebook data harvester speaks out. *BBC News.* Retrieved from http://www.bbc.co.uk/news/technology- 10802730.

ENISA Position Paper #1, "Security Issues and Recommendations for Social Networks", Giles Hogben (Ed), European Network and Information Security Agency, 2007. Everything, Portfolio, New York, NY.

Fishman, N. 2009. *Background screening trends: Social networking among issues to spark hiring controversies.* Retrieved January 2010 from http://www.shrm.org/hrdiscipline/staffingmanagement/Articles/pages/baclgroundscreening/trends.aspx

Flatow, I. (2008). Web privacy concerns prompt Facebook changes. On Science Friday [Radio Podcast]. New York: NPR ScienceFriday Inc.

Goffman,E.(1956)The nature of deference and demeanor, American Anthropol-ogist vol.58,no.3,pp.475499.

Goffman,E.(1959) The Presentation of Self in Everyday Life,Double day Anchor Books,Garden City,New York.

Greenwood, B. (2008). MySpace, Facebook, Google integrate data portability. Information Today 25 (6):27.

Gross, R., Acquisti, A., and Heinz, H. J. "Information revelation and privacy in online social networks", in Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, 2005.

Gross, Ralph and Acquisti, Alessandro (2006). Information Revelation and Privacy in Online Social Networks. pp. 71-79

Gross, Ralph and Alessandro Acquisti. (2005)Information Revelation and Privacy in Online Social Networks.î WPES í05 7

Gürses, S., Berendt, B., Santen, T.(2006) "Multilateral security requirements analysis for preserving privacy in ubiquitous environments", in Proceedings of the UKDU Workshop Berendt, B., Menasalvas, E. (Eds.), pp. 51-64.

Gutwirth, S. (2002) "Privacy and the Information Age", Rowman and Littlefield:Maryland.

Hampton,K.& Wellman,B.(2003) Neighboring in netville: how the internet supports community and social capital in a wired suburb, City and Community,vol.2,no.4,pp.277311.

Hampton,K.N.(2007) Neighborhoods in the network society :the e-Neighbors study, Information,Communication&Society,vol.10,no.5,pp.714748.

Hardy, Q. (2009), Web 2.0's Corporate Plea, Forbes, London.

Haythornthwaite,C.(2005) Social networks and Internet connectivity effects, Information, Communication & Society,vol.8,no.2,pp.125147.

Heining, A. (2009), "Facebook privacy changes, aimed at openness, may trigger the opposite", The Christian Science Monitor, May 15

J.Donath and D.boyd.Public (2004) displays of connection. *BT Technology Journal*,22: 7182

Joinson, A.N., Reips, U-D., Buchanan, T.B., and Paine Schofield, C.B. in press. Privacy, trust and self-disclosure online. Human-Computer Interaction..from http://www.joinson.com/

Jones, H., & Soltren, J. H. (2005). Facebook: Threats to privacy. Retrieved on November 2011

Jones, Harvey and Soltren, Jose Hiram. Facebook: Threats to Privacy. December 15, 2005. pp 1, 4, 16, 34, 35.

Jourard, S.M. (1971), The Transparent Self, D. Van Nostrand, New York, NY.

Kent (2011), Malaysian Facebook Users Hits 12Millions. Retrieved November,11,2012 from www.socialbakers.com

Kim, W., Lee, C. and Hiemstra, S. (2004), "Effects of an online virtual community on customer loyalty and travel product purchases",Tourism Management, Vol.25 No.3

Klaassen, A. (2008), "Facebook vs. Google's adword", Advertising Age, Vol. 78 No. 6.

Lampe,C.,Ellison,N.,& Steinfield,C. (2007). A familiar Face(book):Profile elements as signals in an online social network. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 435-444). New York:ACM Press.

Lenhart, A. (2009), The Democratization of Online Social Networks: A Look at the Change in A Look at the Change in Demographics of Social Network Users over Time, Pew Research Center Internet & American Life Project, Milwaukee, WI.

Lenhart, A., & Madden, M. (2007). Teens, privacy, and online social networks: How teens manage their online identities and personal information in the age of MySpace. Reports: Family, Friends & Community. Retrieved October 20, 2011, from http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf

Lenhart, L., & Madden, M. (2007). Pew internet:Pew Internet and American Life Project.

Lipford H. R., Besmer A., and Watson, J., (2008) "Understanding Privacy Settings in Facebook with an Audience View," 2008 USENIX Workshop on Usability, Psychology, and Security

Mackay W. "Triggers and barriers to customizing software," Proceedings of CHI'91, 1991 ACM Press, pp. 153–160.

Madden, M., Fox, S., Smith, A., & Vitak, J. (2007). Digital footprints: Online identity management and search in the age of transparency. Reports: Internet Evolution. Retrieved October 2008, from http://www.pewinternet.org/pdfs/PIP_Digital_Footprints.pdf.

Majmudar, Nishad. ìFacebook users say friendship has its limits ñ or ought to Democratic and chronicle.com. 28 August 2005. Retrieved on 27 September 2011 < http://www.democrat and chronicle.com/apps/

McCandlish, Stanton. "EFF's Top 12 Ways to Protect Your Online Privacy." Electronic Frontier Foundation. 10 April 2001. Retrieved on 8 December 2011 <http://www.eff.org/Privacy/ eff_privacy_top_12.html>.

Mead,G.H.(1934) Mind,Self,and Society from the Stand point of a Social Behaviorist, ed.C.W. Morris, University of Chicago Press,Chicago.

Morrison.C (2010) Malaysia ranks fourth in Southeast Asia's FB usage. Retrieved November 2012 from http://www.theborneopost.com/2012/11/20/malaysia-ranks-fourth-in-southest-asias-fb-usage

Nakanishi, M. (1986), "Perceptions of self-disclosure in initial interaction", Human Communication Research, Vol. 13, pp. 167-90.

NetLingo (2006), NetLingo: The Internet Dictionary, available at: www.netlingo.com (accessed 10 July 2012).

Nissenbaum, H., "Privacy as Contextual Integrity", Washington Law Review, (79:1), 2004, pp. 119-158.

Nosko, A., & Wood, E., & Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of Facebook. Computers in Human Behaviour, 26, 406-41 8.

Phillips, D. J. (2004) "Privacy Policy and PETs", New Media and Society, (6:6), pp. 691-706.

Quan-Haase,A.(2007) University students local and distant socialites: using and integrating modes of communication on campus, Information, Communication & Society,vol.10,no.5,pp.671693.

Quan-Haase,A. & Young A.L (2009). Information Revelation and Internet Privacy Concerns on Social Networks Sites: A Case study of Facebook, University Park, Pennsylvania, USA. Retrieved on October 2010.

Regan, K. "Online Privacy Is Dead – What Now?" E-Commerce Times. 2 January 2003. 8 Dec 2005 <http://www.ecommercetimes.com/story/ 20346.html>.

Rosenblum, D. "What Anyone Can Know: The Privacy Risks of Social Networking Sites," IEEE Security and Privacy, Vol. 5, No. 3, 2007, pp. 40-49.

Schweitzer, S(2005), 'When students open up - a little too much', Boston.com, < http://www.boston.com/news/local/new_hampshire/articles/2005/09/26/when_students_open_up____a_little_too_much>.

Singel, R. (2007), "Private Facebook pages are not so private", Wired, 28 June.

Singel, R. (2007). Facebook private profiles not as private as you think they are -- UPDATED with Facebook changes. Retrieved May 16 2010, from http://blog.wired.com/27bstroke6/2007/06/facebook-privat.html

Singel, R. (2007). Private Facebook pages are not so private. Retrieved June 2010, from http://abcnews.go.com/Technology/Story?id=3325951&page=1.

Steinfield, C., Ellison, N. and Lampe, C. (2008) Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology*, 29 (6), 434-445.

Stutzman, Fred. An Evaluation of Identity-Sharing Behavior in Social Network Communities. Ibiblio.org. 2005. Retrieved October 2011 <http://www.ibiblio.org/fred/pubs/stutzman_pub4.pdf>.

Sullivan, B. and Thaw, J. (2006), "Facebook, courted by yahoo, won't sell, director says", Bloomberg, Retrieved on December 2011.

Sundén, J. 2003. Material Virtualities: Approaching online textual embodiment. Peter Lang, New York.

Tapscott, D. and Williams, A.D. (2008), Wikinomics: How Mass Collaboration Changes Everything Portfolio, New York, NY.

Treese, W. (2006), “Ten years on internet time”, ACM Digital Library, Vol. 10 No. 3, pp. 15-17.

Tufekci,Z.(2008)Can you see me now? Audience and disclosure regulation in online social network sites, Bulletin of Science,Technology and Society,vol.28,no.1,pp.2036.

Vander Veer, E. A. (2008). Facebook: The missing manual. Sebastopol, CA: Pogue Press/O'Reilly.

Viseu, A., Clement, A., and Aspinall, J. 2004. Situating privacy online: Complex perception and everyday practices. Information, Communication & Society. 7, 1 (2004), 92-114.

Whelan, B. (2005), 'Facebook, a Fun Resource or Invasion of Privacy', Athensnews.com, <<http://athensnews.com/issue/article.php3?story_id=21491>.>.

Whelan, Bridget. Facebook (2005) a fun resource or invasion of privacy.î Athensnews.com. 08 September 2005. Retrieved September 2011 <http://athensnews.com/issue/article.php3?story_id=21491>.

Wortham, J. (2009), “Facebookers approve new policy, but still hate redesign”, New York Times, April 24.

Worthy, M., Gary, A.L. and Kahn, G.M. (1969), “Self-disclosure as an exchange process”, Journal of Personality and Social Psychology, Vol. 13, pp. 59-63.

Zywica, J. and Danowski, J. (2008), “The faces of Facebookers: investigating social enhancement and social compensation hypotheses; predicting Facebook and offline popularity from sociability and self-esteem, and mapping the meanings of popularity with semantic networks”, Journal of Computed-Mediated Communication, Vol. 14, pp. 1-34.