Library Philosophy and Practice (e-journal)   Libraries at University of Nebraska-Lincoln

February 2017

Personal Information Sharing Behavior of University Students via Online Social Networks

Ghulam Murtaza Rafique

PhD Scholar at Department of Information Management, University of the Punjab, Lahore | Librarian at Government Punjab Public Library Lahore, ghulam_murtaza692@hotmail.com

Follow this and additional works at: http://digitalcommons.unl.edu/libphilprac

Part of the Scholarly Communication Commons, and the Scholarly Publishing Commons

Personal Information Sharing Behavior of University Students via Online Social Networks

Abstract

Background – With privacy concerns growing on a daily basis, it is important to understand how university students guard their personally identifiable information. Despite the students' perceived readiness and several studies on the topic, it is not fully understood what personally identifiable information university students are sharing via Online Social Networks (OSNs).

Purpose – Therefore, the purpose of this study was to determine the personal information sharing behavior of university students through online social networks.

Design/methodology/approach – Quantitative approach was used and a survey questionnaire was solicited to collect the data from 250 out of 712 master's students of faculty of Economics and Management Sciences, University of the Punjab, Lahore, Pakistan. Equal sized stratified simple random sampling technique was used to select the required sample size.

Findings – The findings revealed that most of the university students shared their personal information like first name, last name, and the college they attended on OSNs. They rarely updated their profiles and labeled the uploaded photos/ videos with their own names. They mostly used their cell phones to use OSNs and female were conscious to disclose their personal information on OSNs as compared to male students.

Originality/value – This study would help the policy makers to establish or develop different types of information security laws to protect the information of individuals on social networking sites. It would also help the students to keep their personal information secret while using Web 2.0 technologies.

Keywords- Information sharing, Personal Information, Pakistan, Students, University

Introduction

The use of Social Networking Sites (SNSs) among students and adolescents has been increasing day-by-day to meet, interact and keep in touch with one another. SNSs permit their users to create their personal profiles, in which they reveal a lot of their personal information i.e. real name or a pseudonym, photographs, birthday, hometown, religion, ethnicity, and personal interests (Dwyer, Hiltz, & Passerini, 2007; Tuunainen, Pitkänen, & Hovi, 2009). This information may be used for nefarious purposes by third parties and unsavory individuals which causes many privacy issues. However, little research has been conducted to determine the behavior of sharing personal information by university students via SNSs and Internet. Previous studies only focus on the students under 18 (teenagers) and does not fully understand how students share their personal identifiable information (PII) in online SNSs (Flinn, 2009a; Hinduja & Patchin, 2008; Lenhart, 2007). Therefore, it is needed to determine the personal information sharing behavior of university students via SNSs and Internet by identifying the types of personally identifiable information shared and the traits of students who share personally identifiable information.

The continuously increasing popularity of the World Wide Web (www) caused the rising number of types of services which are available through computer networks. People who use these services, created a new kind of virtual societies usually called online social networks, (Cheung, Chiu, & Lee, 2011; Howard, 2008; Krishnamurthy & Wills, 2009; Leskovec, Backstrom, Kumar, & Tomkins, 2008). They can also be named as web-based social networks (Golbeck & Hendler, 2006), computer-supported social networks (Wellman et al., 1996) or virtual communities (Castells, 2001). Online Social Network Sites (SNSs) are "web sites 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, p. 211).

Users of SNSs share a plenty of their Personally Identifiable Information (PII) on online SNSs, either consciously or un-consciously (Hinduja & Patchin, 2008). PII is:

Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (Koontz, 2008, p. 28).

There are extensive literature discussing the history, developments and the use of online Social Networking Sites (SNSs) by students and adolescents. SNS applications are growing; campus administrators are exploring ways to use SNSs; and faculty is experimenting with SNS tools to support learning. At the same time, students continue to seamlessly adopt and adapt these services in their lives. It is essential that higher education understand SNS practices of students because these sites are fundamentally changing the social fabric of the university (Ellison, 2008). However, there is a dearth of literature describing the students' current practices to share their personal information via SNSs and Internet.

Many studies exist about information and knowledge sharing behaviors and practices of students; however, few focus on personal information sharing behavior of university students. Therefore, the undertaken study describes the current practices and behavior of university students to share their personal information through SNSs. Despite an increase interest in SNSs and their usage, it is surprising that little empirical researches had actually been conducted to determine the

personal information sharing practices of university students through SNSs, especially from the perspective of Pakistani origin. The search of literature shows that no such study has so far been conducted in the field of Librarianship at the time of this research; as much work on SNSs has been produced in the field of Computer Sciences.

This study is important for several reasons. First, to understand how much and what type of PII students share through SNSs. Second, identifying the traits of students who share personally identifiable information. Finally, very important, this study will provide guidelines for policymakers and telecommunication authorities in formulating information privacy laws to prevent individuals especially students from different cybercrimes related to the study.

Research Questions

The study will answer the following research questions:

1. What personally identifiable information are university students sharing?

2. Which are identifying factors those affect how students share personally identifiable information?

3. What is the comparison between specific demographics of university students who share personally identifiable information?

Rationale and Significance of the Study

The use of online SNSs among masses is continuously escalating due to the immense proliferation of Web 2.0 technologies and also due to the easy access to internet via smart phones, *i*-pads, and personal computers. Especially, students are more likely to involve in using these SNSs like Facebook, Twitter, and LinkedIn etc. While using these online social media, the students share a plenty of their personal information onto their profiles. Only few studies have been conducted to determine the personal information sharing behavior of students in this regard. An extensive

search for literature has shown that in Pakistan, no such study had been carried out to determine the personal information sharing behavior and attitude of students via Internet and Online SNSs. So the intention to conduct this study is to reveal the clear and actual picture of disclosing personal information by university students via Online SNSs in Pakistan.

This study is important because it will add new knowledge in the area of information science. This study will inform the users of social media about the effect of Online SNSs in their daily and academic lives. And importantly, this research will inform the university students that how much personal information, they are unveiling while using online social networks consciously or unconsciously.

Furthermore, this research will support the policy makers in planning and designing the information privacy policies. This research will also facilitate the legislative authorities in making the data protection law for the users of the Online SNSs and internet.

Definition of Terms

It is important to have operational definitions of the terms used in the study.

Personal information

In this study the term refers to 'any information that could be used to know the identity and build a profile of an individual is being regarded as personally identifiable information, including information that is regarded as public. Because photos and videos may contain additional information such as license plate number on cars, house numbers, and names of family/friends, photographs and videos is included in the list of personally identifiable information'.

Online social networking sites (Online SNSs)

For this study, this term refers to 'web sites that allow members to construct a public or semipublic profile and formally articulate their relationship to other users in a way that is visible to anyone who can access their profile'.

Limitations and Delimitations of the Study

This study only focused on the personal identified information (PII) shared on OSNs by university students. It had not covered all the information related to the university students. Furthermore, this research was conducted within the following parameters:

- Only enrolled students of the Faculty of Economic and Management Sciences at University of the Punjab was included in this research.

- The sample population selected for this study was limited to only master's students of the above mentioned Faculty.

Literature Review

In 20th century, the individuals kept in touch via one-to-one interaction and telephone; while in 21st century, the computer mediated means (with the help of internet) are using for this purpose which are most convenient and rapid than previous (Lenhart & Madden, 2007; Lenhart, Rainie, & Lewis, 2001; Subrahmanyam, Greenfield, Kraut, & Gross, 2001; Tidwell & Walther, 2002). Like other tool and services, the internet has also been gradually developed and enhanced since its inception. Internet was made the first move in 1991. The generation of Web is flourished using the course of Web 1.0, Web 2.0, Web 3.0 and now Web 4.0 technologies (Olivia, 2011). With the immense proliferation in Web 2.0 technologies, there is a lot of opportunities and options for individuals and students to share and exchange their information with each other (Yat, 2012). Web 2.0 technology allows users to interact and collaborate with one another in virtual social

community called social networks or social media. By this rapid growth in Web 2.0 technologies, the concept of social networks has changed. Web 2.0 make it possible to create such manageable online social networks that allows users to share and disseminate information more easily and fast than any other time in the history of the Internet (OReilly, 2007). By SNSs, users can interact, collaborate, keep in touch with one another and be updated with the latest news about their friends oblivious for geographic location and time (Yat, 2012); to explore themselves, relationships, and share cultural artifacts (Agarwal & Mital, 2009).

The use of SNSs especially among students and adolescents has been radically increased in the past few years due to its extreme popularity (Ellison, 2008). There are some pros and cons of SNSs regarding students' achievement. The pros of using SNSs regarding students' achievement are: collaboration for education; development of creativity; finding good people; free business promotion expertise; ease of communication and development of domains. On the other hand, students have to face some problems of using SNSs in their academic environment that may be: accessibility of information, everything is public, multitasking or lack of concentration, negative publicity, time consuming, and living in the virtual world (e.g. virtual world addicted) (Srivastava, 2012).

Almost all online activities require users to establish their identity each time. They use a new application, usually by filling out an online form and providing sensitive personal information. Individuals leave a lot of their Personal Identifiable Information (PII) on the internet while using internet and Online Social Networking applications (Cavoukian, 2008).

SNSs permit their users to create profile about themselves to connect with the internet. Users post a lot of their personal information onto those profiles to attract the people of their interests (Hinduja & Patchin, 2008). The profile include information such as name, birth date,

address, and various other pieces of personally identifiable information (PII) (Dwyer et al., 2007; Gross & Acquisti, 2005). Users create digital identities on SNSs to identify themselves. These identities differ from each SNS to SNS to which they belong. The personal information they put onto their profiles may be public (e.g., artistic or professional profiles) or private (e.g., restricted between friends or family members). This personal information may be pictures (e.g., on Flickr, Facebook, MySpace), opinions (e.g., on Twitter, blogs, forums), videos (e.g., on YouTube), and a variety of information on personal home pages. Such postings may contain sensitive information, such as birth dates, home addresses, and personal phone numbers (De Paula, 2009).

Department of the Navy (2012) stated that it is very hard to identify the exact PII of individuals, it may be sensitive for someone and on the other hand it may not be so sensitive for any other as it varies person to person, organization to organization and the way wherein it has been using.

A survey has been conducted by the Ellison (2008) to determine the behavior towards the disclosure of personal information via SNSs among adolescents and undergraduates. The survey reported that it is common for all age groups to include their first name and personal photo at their profile. Most Net Generation SNS users disclose e-mail address or instant messaging (IM) screen name, last name, and full date of birth on their profiles but older respondents are more likely to reveal personal information. Madden (2012) and Ellison (2008) explores that females are more cautious about revealing their personal information that identifies them directly such as last name, cell phone number, and address or home phone number than males.

Pew Internet and American Life Project study on teens and social media discovered that adolescence decision on revealing their personal information though SNSs depends upon the context in which it is going to be exchanged (Duggan & Brenner, 2012).

PII first arose as an issue in 1960s when the computer allowed public bureaucracies and private companies to process personal data (Solove, 2001). The privacy problem about disclosure of personal information on SNSs has been becoming the hottest issue since the inception of internet and arising much public concern and discussion. With the escalating usage of SNSs, we cannot ignore this issue because SNSs contains abundance of personal information which may cause commercial interest and illegal usage of the information. This online published information can be easily abused by stalkers and crooks, bullies, or even friends and personals information of SNS users also provide opportunities to third parties to take advantages from it and use it without taking permission from owner of that information for their different business purposes such as online advertising, customer segmentation, data mining, direct communication and online advertising (Barnes, 2006; Gross & Acquisti, 2005; Naryshkin, 2010).

When someone shares information in an online environment, several consequences exist. Among the top consequences are identity theft and stalking. A huge amount of personal information about users is stored by the online social networks (Perez, 2008) which might be used not only by truthful users but third parties with rather adverse purposes as well (Acquisti & Gross, 2006).

Zhang, Sun, Zhu, and Fang (2010) examined that there were two types of attacks on online social graphs: forging nodes/identities and forging social links/connections. Forging a node (e.g., identity theft) has become a fundamental problem in SNSs and is also the foundation of many other security problems. Identity theft has become modern day cyber crises, which possibly affect those individuals who use internet or online social networks(Anderson, Durbin, & Salinger, 2008; Lai, Li, & Hsieh, 2012). Individuals especially adolescents have to face different types of cyber-attacks while using SNSs that includes identity theft, defamation, stalking, injuries to personal

dignity, cyber-bullying (De Paula, 2009), communication intrusion , phishing, information leakage (Hogben, 2007), unwanted exposure, distortion, badmouthing and reputational (Weiss, 2009).

To prevent from becoming victims of identity theft or cyber stalking is to educate individuals. "It is very important that individuals of all ages be educated about what personally identifiable information is and what they should and should not share via online social networks" (Flinn, 2009b, p. 24). Barnes (2006, p. 41) stated a very comprehensive sentence in this regards, "Awareness is key to solving the solution". Mitseva, Imine, and Prasad (2006) explore the importance of educating individuals by using different proper methods of accessing the Internet in different public areas such as hospitals, hotels and airports. Additionally there must be some privacy laws to educating individuals, to solve that problem.

Barnes (2006) stated three different ways/solutions to protect privacy in online SNSs— social solutions, technical solutions, and legal solutions. Parents, schools, and social networking sites are also working on various social solutions to the privacy problem. Experts agree that the first step in building protections for teenage bloggers starts with parents. The social solutions to the privacy paradox begin at home. Parents need to be much more involved with their kids' computer use than they are. "In many cases, schools are being forced to respond to real world problems which only came to their attention because this information was so publicly accessible on the Web." Some schools have banned blogs and asked students to take their information off the network (Koontz, 2008; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). Currently, commercial social networking companies are reacting to the problem of teens online. In addition to social awareness, social networking sites are exploring technological solutions to better protect their users.

Research Design and Procedure

Quantitative research approach was used to determine the personal information sharing behavior of university students. A structured survey questionnaire will be solicited to collect the data from the respondents.

The population of this study was consist of currently enrolled masters' students of Faculty of Economics and Management Sciences, University of the Punjab, Lahore. The required sample was determined using equal sized stratified simple random sampling technique. The strata was decided on the basis of departments of this faculty.

The list of the departments of Faculty of Economics and Management Sciences, University of the Punjab is as under with respect to currently enrolled masters' students and calculated sample size (with 95% confidence level and 5% marginal error):

Table 1

Population and Sample Size

Sr. No.	Name of the Department	Population	Sample Size
1.	Institute of Business Administration (IBA)	135	50
2.	Department of Economics	225	50
3.	Institute of Business & Information Technology (IBIT)	122	50
4.	Department of Information Management	120	50
5.	Institute of Administrative Sciences	110	50
	Total	712	250

Structured survey questionnaire (Appendix A) was used to collect the data which was adapted from a study conducted by Flinn (2009) on college students. Several survey questions was modified according to the needs of university students and local scenario; as the original survey was developed for American college students. This survey was conducted on Pakistani university students and there was a cultural, economic, religious and social differences between these two populations.

Although many of the questions on the survey were validated as they had been taken from the study on college students of Frostburg State University. But it was important and necessary to validate the entire survey. The entire survey, including the adapted study questions and the new questions, was presented before the experts of the field for further improvement; and to a group of university students for useful suggestions and improvements. The Cronbach's Alpha of the instrument was 0.89.

The questionnaire was personally administered. The researcher was available at the time of data collection from the students to guide and assist them in case of any ambiguity and vagueness in the questions. Data thus collected was analyzed using Statistical Package for Social Sciences (SPSS) version 22.

Results and Discussion

Demographic Information

The distribution of the respondents by gender is in favor of females with 64.3 percent compared to 35.7 percent for males.

Table 2
Respondents by Gender

Gender	Frequency	Percent
Male	74	35.7%
Female	133	64.3%
Total	207	100.0%

The department-wise distribution of respondents was tabulated in Table 3 and the distribution of respondents by marital status showed that majority of them (74.9%) were single while 25.1% were married.

Table 3
Respondents by Department wise (N = 207)

Departments	Frequency	Percent
Institute of Business Administration (IBA)	44	21.3%
Department of Economics	38	18.4%
Institute of Business & Information Technology (IBIT)	41	19.8%
Department of Information Management	40	19.3%
Institute of Administrative Sciences	44	21.3%

The distribution of the respondents by age group shows that a large majority (54.1%) falls in the age-group of 19-24 while 45.4% are '25-30' years. A very small number (0.5%) is in the age group of 'up to 18'.
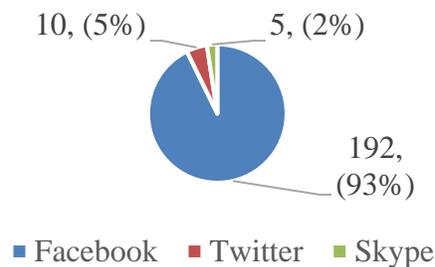
Table 5
Respondents by Age Group (N = 207)

Age Group	Frequency	Percent
up to 18	1	0.5%
19-24	112	54.1%
25-30	94	45.4%

Personal information sharing via Online Social Networks (OSNs)

The students were asked about mostly used OSNs. Majority of the respondents (92.8%) replied that they frequently used Facebook. Out of the total respondents (207), only 15 used Twitter, Skype and/or other social media like WhatsApp (Figure 1).

Figure 1: Most Frequently Used Online Social Networks

10, (5%)   5, (2%)

192, (93%)

■ Facebook   ■ Twitter   ■ Skype

Most of the students (59.9%) used OSNs several times a day, while 72 (34.8%) used about once a day. Only 11 (5.3%) replied that they spent few time 1-2 days a week or every few weeks in using OSNs (Table 6).

Table 6
Frequency of using Online Social Networks (N = 207)

Use of OSNs by students	Frequency	Percent
Several times a day	124	59.9%
About once a day	72	34.8%
1-2 days a week	8	3.9%
Every few weeks less often	3	1.4%

The results revealed that mostly university students spent their most of the time to use OSNs either for educational purpose or infotainment. With the consistent of the previous studies' findings Barkhuus and Tashiro (2010); (Brennan, 2006; Cheung et al., 2011; Duggan & Brenner, 2012; Flinn, 2009b; Hinduja & Patchin, 2008) the use of social networking sites among students were increasing and used these Web 2.0 technologies several times a day.

Figure 2: Mostly Used Devices for using Online Social Networks

A desktop computer A laptop computer A smart phone/digital device
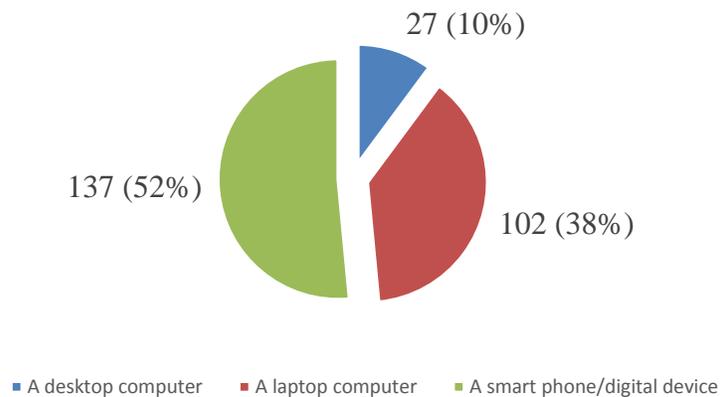
Majority of the students (52%) used smart phones or other digital devices to use OSNs, 102 (38%) used laptop computers while only 27 (10%) used desktop computer for this purpose. Mostly students used smartphones due to the ease of access to these devices and to set an image to other students.

Types of Personal Information Shared

The students were also asked about their personal information shared via OSNs. Almost all the respondents (206) replied that they shared their first name, 197 shared last name, 154 shared their college name. Whereas, of the total respondents, 165 responded that they don't share their home phone number, 158 don't disclose their class schedule and 138 don't reveal their height/weight onto OSNs (see Table 7).

Types of personal information Shared on OSNs: Gender wise cross tabulation

The results of Table 8 showed that 84 female students didn't share their personal cell numbers; 113 didn't share their home phone numbers; 109 didn't disclose their heights and weights related information; 101 didn't unveil their class schedule and 103 didn't show their IM screen number onto OSNs. It is a general fact that females always feel hesitation and reservation to share aforementioned personal information (Table 8) via OSNs due to the cultural & social constraints and religious factors as compared to males.

Table 7
Types of Personal Information Shared (N=207)

Sr. #		n	Yes	No	Don't know
a.	Your first name	207	206	1	0
b.	Your middle name	198	62	136	0
c.	Your last name	198	197	1	0
d.	Your college name	207	154	53	0
e.	Your cell/mobile phone number	207	85	109	13
f.	Your home phone number	207	42	165	0
g.	College you attend	207	124	83	0
h.	Your birthday	203	153	50	0
i.	Your height/ weight	207	60	138	9
j.	Your class schedule	207	17	158	32
k.	Your IM screen name	207	10	143	54
l.	Your email address	207	144	63	0
m.	Your blog/link to your blog	207	72	119	16
n.	Your hometown address	207	65	111	31

Table 8
Types of personal information Shared on OSNs: Gender wise cross tabulation

| | | Gender | | Total |
		Male	Female	
Cell/mobile phone number shared on OSNs	Yes	40	45	85
	No	25	84	109
	Don't know	9	4	13
Home phone number shared on OSNs	Yes	22	20	42
	No	55	113	165
	Don't know	0	0	0
Height/ Weight shared on OSNs	Yes	42	18	60
	No	29	109	138
	Don't know	3	6	9
Class schedule shared on OSNs	Yes	10	7	17
	No	57	101	158
	Don't know	7	25	32
Instant Messenger (IM) screen number shared on OSNs	Yes	3	7	10
	No	40	103	143
	Don't know	31	23	54

The findings of this study are similar the findings with the studies of Brennan (2006), Duffy and Bruns (2006), Krishnamurthy and Wills (2008), Hoy and Milne (2010) and Agarwal and Mital (2009) who revealed that females felt shy to share their personal information like mobile numbers and class schedules on OSNs.

Use of Fake Information on OSNs

The respondents were asked about the usage of fake information instead of real information shared via OSNs. The majority of the respondents (34.8%) used very little; while 44 (21.3%) mostly used fake information on OSNs. Of the total respondents, 55 (26.6%) replied that they never used fake information on OSNs. The inferences shows that majority of the students don't want to show the real information onto OSNs due to orient their dual personality in front of others rather than actual situations. Sometimes due to prevent themselves from the consequences of using

real information on OSNs like cyber stalking, information theft or other cybercrimes, they don't disclose their real information.

Figure 3: Use of Fake Information on OSNs
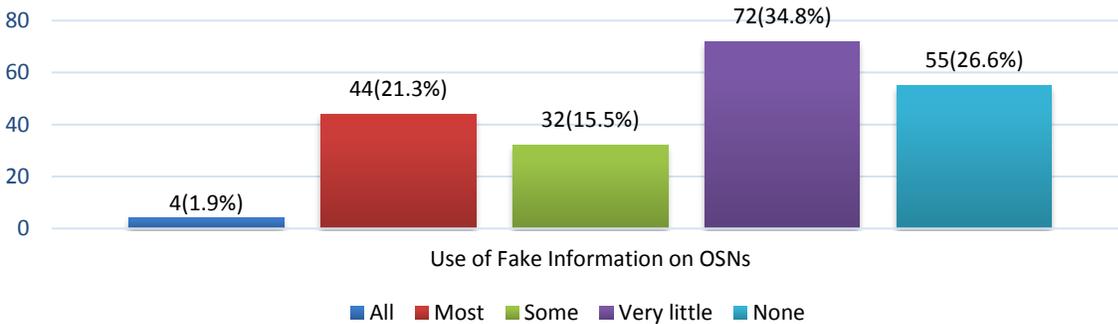
Mostly posted/ Uploaded on OSNs

Majority of the students (99, 47.8%) rarely, while (82, 39.6%) sometimes upgrade their profiles created at any OSNs and only 11 (5.3%) never upgrade their profiles. The findings are against the common perception and it might be due to the miss understanding of the statements by the respondents or may be the students don't want to share this information with others.

Figure 4: Mostly posted/ Uploaded on OSNs
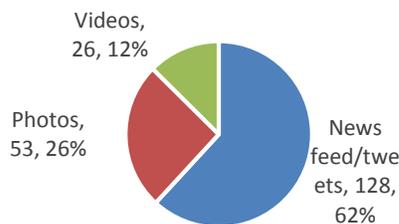
Majority of the students (128, 62%) shared and/or posted news feeds/tweets, 53 (26%) photos and 26 (12%) uploaded videos on OSNs (Fig. 4). One of the basic purpose behind using OSNs is to update ones timelines to aware others or friends/followers about oneself. Therefore the students posted newsfeed and tweets onto their timelines.

Practice of labeling different photos and videos on OSNs

The students were asked about their practice of labeling different posted and/or uploaded photos and videos on OSNs (Table 9). The results showed that mostly students (112, 54.1%) labeled it with their own names while 159 (76.8%) didn't label it with a friends' names (Table 9).

The findings of the study are consistent with the results of the previous studies Facebook (2013), Yat (2012) and Subrahmanyam et al. (2001).

Table 9

Practice of labeling different photos and videos on OSNs

Sr. No.	Photo/ Video on OSNs (Facebook, Twitter, etc.) and…	Yes	No	Don't know
a.	labeled it with your name	112 (54.1%)	91(44.0%)	4 (1.9%)
b.	labeled it with a friend's name	44 (21.3%)	159 (76.8%)	4 (1.9%)
c.	labeled it with the name of place it was taken	58 (28.0%)	124 (59.9%)	25 (12.1%)

Perception about sharing personal information posted on OSNs

The students were asked about their perception about sharing personal information posted on OSNs. All the statements got mean scores of more than 2.50 which means that these participants moderately think that their personal information are shared by the OSNs or with other companies but their feeling is weak (see Table 10).

The findings unveiled that the university students thought their information on OSNs might be used by other people, other organizations or by the employees of OSNs. Anderson et al. (2008) also found that the users of the OSNs always threatened about the disclosure of their personal information to any other nefarious persons or organizations.

Table 10
Perception about sharing personal information posted on OSNs

Sr. No.		N	Mean	SD
a.	To what extent do you think about your personal information being shared by OSNs (Facebook, Twitter, etc.)	207	2.97	.913
b.	To what extent do you think that OSNs (Facebook, Twitter, etc.) share your personal information with other companies?	207	2.89	.954
c.	To what extent do you think that other individuals use any information you provided on OSNs (Facebook, Twitter, etc.)	207	2.65	.873
d.	To what extent do you think about your personal information provided on OSNSs (Facebook, Twitter, etc.) being shared by employees of OSNs (Facebook, Twitter, etc.)?	207	2.59	.995

Scale: 1 = Not at all, 2 = Slightly, 3 = Moderately, 4 = Very Extremely, SD = Standard Deviation

Personal information shared by the respondents on OSNs

The students were also asked about revealing their personal information via OSNs. Majority of the students (176) had their own profile online that others could see; 138 wrote or commented about other people's profile page; 136 allowed anyone to see their profile; 120 included their phone numbers and 103 included a picture of themselves on their profiles.

Table 11
Personal information shared by the respondents on OSNs

Sr. No.	Statements	Yes	No	Don't know
a.	Do you have your own profile online that others can see?	176	27	4
b.	Do you allow anyone to see your profile?	136	71	0
c.	Do you include a picture of yourself on your profile?	103	104	0
d.	Do you include your email address on your profile?	95	95	17
e.	Do you include your instant messenger address on your profile?	63	144	0
f.	Do you include your phone number on your profile?	120	87	0
g.	Do you include your home address on your profile?	58	145	4
h.	Do you include information about your interests and/or hobbies on your profile?	116	87	4
i.	Do you include information about your personality on your profile?	64	132	11
j.	Do you write or comment about other people's profile pages?	138	56	13
k.	Do you spend time personalizing your profile page?	73	99	35

Of the total respondents, 145 didn't include their home address; 144 did not want to include their instant messenger address and 132 did not like to include information about their personality on their profiles (see Table 10).

Conclusion and Recommendations

This study explores the personal information sharing behavior of university students via OSNs. A side effect of using online social network is beginning to emerge: people are losing their privacy. People are embracing Web 2.0 sites, such as Facebook, twitter and WhatsApp, and placing sensitive information online, such as their name, phone numbers, addresses, etc. Students share an enormous amount of personally identifiable information, in a variety of situations. The top three items of personally identifiable information that the university students shared was their first name, last name, the college they attend, and their hometown/city. Flinn (2009a) also depicted that the students shared their last name, their college and home town name on OSNs.

Students mostly used a laptop, cell phone, or digital device to use OSNs than other technologies. When uploading photos to web 2.0 such as Facebook, WhatsApp majority of the university students found it was okay to label the photos with their name, their friends' names, and the location that the photo was taken. While photo uploading and labeling is popular, many of the students did not engage in uploading and labeling videos to online websites. Race was a factor for the amount of personally identifiable information students shared with regard to photos. Females were more conscious to share their personal information on OSNs than male students.

The individual falls into various age groups and in addition, he owned one, or more, of the following items: a laptop, a cell phone, and/or a digital device. Finally, he used the Internet for one or more of the following activities: uploading photos, tweets, and/or update their status onto their

timelines. Mostly students had their own profile online that others could see but didn't have instant messenger address on your profile.

This study has revealed multiple opportunities for future research. Although there are many points of interest exposed by this study, three surface as viable research studies for the future: personally identifiable information and videos, students willing to share incriminating photos of themselves or others, and parallel studies at multiple universities.

It would be worthwhile to investigate why students are inclined to share such information despite the possible future consequences such as losing a friendship, having charges files against them, or losing a job opportunity.

References

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on the Facebook.* Paper presented at the Privacy enhancing technologies.

Agarwal, S., & Mital, M. (2009). An Exploratory Study of Indian University Students' Use of Social Networking Web Sites: Implications for the Workplace. *Business Communication Quarterly, 72*(1), 105-110.

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *The Journal of Economic Perspectives, 22*(2), 171-192.

Barkhuus, L., & Tashiro, J. (2010). *Student socialization in the age of facebook.* Paper presented at the Proceedings of the 28th international conference on Human factors in computing systems.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9), 11-15.

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

Brennan, M. (2006). Understanding Online Social Network Services and Risks to Youth. *CEOP: Child Exploitation and Online Protection Centre (CEOP), available at: http://www. ceop. gov. uk/downloads/documents/social_network_serv_report_011206. pdf.*

Castells, M. (2001). Virtual communities or network society. *The Internet galaxy: reflections on the Internet, business, and society*, 116-136.

Cavoukian, A. (2008). *Privacy and Digital Identity: Implications For The Internet.* Paper presented at the Proceedings from Identity in the Information Society Workshop, Lake Maggiore, Italy.

Cheung, C. M. K., Chiu, P.-Y., & Lee, M. K. O. (2011). Online social networks: Why do students use facebook? *Computers in Human Behavior, 27*(4), 1337-1343. doi:http://dx.doi.org/10.1016/j.chb.2010.07.028

De Paula, A. M. (2009). *Security aspects and future trends of social networks.* Paper presented at the Proceedings of The Fourth International Conference on Forensic Computer Science (ICOFCS).

Department of the Navy. (2012). What is Personally Identifiable Information (PII)? *Chief Information Officer: The DON IT Resource.* Retrieved from http://www.doncio.navy.mil/ContentView.aspx?id=2428

Duffy, P. D., & Bruns, A. (2006). The use of blogs, wikis and RSS in education: A conversation of possibilities.

Duggan, M., & Brenner, J. (2012). *The Demographics of Social Media Users — 2012*. Retrieved from Washington, D.C. 20036:

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). *Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace.* Paper presented at the Proceedings of AMCIS.

Ellison, N. (2008). Social networking sites. *ECAR Research Study, 8*.

Facebook. (2013). Facebook: Key Facts. Retrieved from http://newsroom.fb.com/Key-Facts

Flinn, M. B. (2009a). *Personal Information Sharing Behaviors of College Students via the Internet and Online Social Networks: A Case Study.* (Doctor of Science), Robert Morris University, Pittsburgh, USA.

Flinn, M. B. (2009b). Personal Information Sharing Behaviors of College Students via the Internet and Online Social Networks: A Case Study. *ProQuest LLC*.

Gross, R., & Acquisti, A. (2005). *Information revelation and privacy in online social networks.* Paper presented at the Proceedings of the 2005 ACM workshop on Privacy in the electronic society.

Hinduja, S., & Patchin, J. W. (2008). Personal information of adolescents on the Internet: A quantitative content analysis of MySpace. *Journal of Adolescence, 31*(1), 125-146. doi:http://dx.doi.org/10.1016/j.adolescence.2007.05.004

Hogben, G. (Ed.) (2007). *Security Issues and Recommendations for Social Networks*: European Network and Information Security Agency.

Howard, B. (2008). Analyzing online social networks. *Communications of the ACM, 51*(11), 14-16.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*(2), 28-45.

Koontz, L. D. (2008). *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*: DIANE Publishing.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of Information Technology, 25*(2), 109-125. Retrieved from http://www.palgrave-journals.com/jit/journal/v25/n2/full/jit20106a.html

Krishnamurthy, B., & Wills, C. (2009). *Privacy diffusion on the web: A longitudinal perspective.* Paper presented at the Proceedings of the 18th international conference on World wide web.

Krishnamurthy, B., & Wills, C. E. (2008). *Characterizing privacy in online social networks.* Paper presented at the Proceedings of the first workshop on Online social networks.

Lai, F., Li, D., & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems, 52*(2), 353-363.

Lenhart, A. (2007). *Teens and social media: The use of social media gains a greater foothold in teen life as they embrace the conversational nature of interactive online media*: Pew Internet & American Life Project.

Lenhart, A., & Madden, M. (2007). *Teens, privacy & online social networks: How teens manage their online identities and personal information in the age of MySpace*: Pew Internet & American Life Project Washington.

Lenhart, A., Rainie, H., & Lewis, O. (2001). *Teenage life online: The rise of the instant-message generation and the Internet's impact on friendships and family relationships*: Pew Internet & American Life Project.

Leskovec, J., Backstrom, L., Kumar, R., & Tomkins, A. (2008). *Microscopic evolution of social networks.* Paper presented at the Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining.

Madden, M. (2012). *Privacy management on social media sites*. Retrieved from Washington, D.C. 20036:

Mitseva, A., Imine, M., & Prasad, N. R. (2006). *Context-aware privacy protection with profile management.* Paper presented at the Proceedings of the 4th international workshop on Wireless mobile applications and services on WLAN hotspots.

Naryshkin, K. (2010). Study on the Leakage of Private User Information Via a Range of Popular Websites.

Olivia. (2011). Difference Between Web 1.0 and Web 2.0 and Web 3.0. Retrieved from http://www.differencebetween.com/difference-between-web-1-0-and-vs-web-2-0-and-vs-web-3-0/

OReilly, T. (2007). What is Web 2.0: Design patterns and business models for the next generation of software. *Communications & strategies*(1), 17.

Perez, J. C. (2008). Can you trust your social network? *PC World, 26*(2), 22.

Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review*, 1393-1462.

Srivastava, P. (2012). Social Networking & Its Impact on Education-System in Contemporary Era. *International Journal of Information Technology, 1*(2).

Subrahmanyam, K., Greenfield, P., Kraut, R., & Gross, E. (2001). The impact of computer use on children's and adolescents' development. *Journal of Applied Developmental Psychology, 22*(1), 7-30.

Tidwell, L. C., & Walther, J. B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human Communication Research, 28*(3), 317-348.

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

Weiss, S. (2009). Privacy threat model for data portability in social network applications. *International journal of information management, 29*(4), 249-254.

Wellman, B., Salaff, J., Dimitrova, D., Garton, L., Gulia, M., & Haythornthwaite, C. (1996). Computer networks as social networks: Collaborative work, telework, and virtual community. *Annual review of sociology*, 213-238.

Yat, S. C. (2012). *Factors affecting Online Self-disclosure of University Facebook Users.* Hong Kong Baptist University Hong Kong.

Zhang, C., Sun, J., Zhu, X., & Fang, Y. (2010). Privacy and security for online social networks: challenges and opportunities. *Network, IEEE, 24*(4), 13-18.