

Social Network Analysis & Information Disclosure: A Case Study

Shilpi Sharma, J. S. Sodhi

Abstract—The advent of social networking technologies has been met with mixed reactions in academic and corporate circles around the world. This study explored the influence of social network in current era, the relation being maintained between the Social networking site and its user by the extent of use, benefits and latest technologies. The study followed a descriptive research design wherein a questionnaire was used as the main research tool. The data collected was analyzed using SPSS 16. Data was gathered from 1205 users and analyzed in accordance with the objectives of the study. The analysis of the results seem to suggest that the majority of users were mainly using Facebook, despite of concerns raised about the disclosure of personal information on social network sites, users continue to disclose huge quantity of personal information, they find that reading privacy policy is time consuming and changes made can result into improper settings.

Keywords—Social Networking Sites, Privacy Policy, Disclosure of Personal Information.

I. INTRODUCTION

INTERNET revolutionized computers and communications around the world and paved the way for many technological evolutions to follow. It provided a platform to connect with people and with the advent of social networking sites, it became even easier to search, communicate and stay connected. Also with internet services now available on mobile phones, connecting through networking sites has become just a finger tap away; hence the popularity of ‘check-in’ feature, wherein a user can get his current position identified using GPS and then post the location on SNS. This feature is used mainly when the users are travelling and want to keep their friends posted about new expeditions. Social networking sites are now used by the hundreds of millions of people around this world. References [1], [12], [14] state “Web based services that allow individuals to construct a public or semipublic profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within a system”. In social networking sites, the users create a personalized account known as profile that includes the information like date of birth, hobbies, preferences, education status, relationship status and personal interest etc. and add each other to their corresponding social network [27], [37], [40]. It is a website that provides a place for people of same or different community to share their

personal views and activities with family members, friends and colleagues and post information based on their interest, suggestions and discussions on a particular topic or randomly at international platform [10]. The users can restrict the inspection of their profiles from other people not part of their network or keep open for everyone [49]. Earlier research [12], [14], [18], [19] suggests that the main motivation to use online social networking sites is to communicate and to maintain relationships. Few researchers found that different interaction rituals are performed on an SNS for reconstructing the established social networks [51]. Popular activities include updating personal information, sharing photos, getting updates on the activities by friends, sending messages privately or posting public testimonials [17], [18], [34], [54]. Due to huge popularity of SNS’s, they are also being used for marketing and advertising [22]. Such in their impact, which even information posted on these sites is being used in computer forensics for legal and criminal investigations. With growing usage, come many benefits but also many concerns.

There is an ongoing debate that whether social networking sites actually bring people closer or take them away from each other by isolating them. The real risks are believed to arise when users disclose identifiable information about themselves to people whom they do not trust [3], [14], [18], [21], [53].

References [16], [17], [19], [23] show student’s awareness on the privacy issues and the available privacy protections provided by Facebook are not reliable. They observed that majority of the respondents are aware of the consequences of providing personal information but are comfortable in posting and do not take any initiative to protect the information. Participant’s personal information can be accessed by three groups of stakeholders in SNSs; the network, the hosting site, and the third parties and the information are knowingly or unknowingly revealed by the participant [3], [26].

Furthermore, many companies and organizations use social media sites as the medium for marketing campaigns. Social media are regarded as an opportunity for self-presentation and interaction with many respondents around the globe by [33], [47]. Facebook provides data access and privacy control but user’s information is not sufficiently protected, which thus results in information leakage, [3], [42]-[44] privacy in general is hard to measure and examined

In this study, we have mainly considered information disclosure in terms of profile i.e. what users divulge in their profile, where they disclose personal information on their walls irrespective of knowing about information theft. How much time the respondents spent in SNSs and which information do they think must not be shared. The respondents

Shilpi Sharma is with the ASET, Amity University, Uttar Pradesh (Noida), India (e-mail: ssharma22@amity.edu).

Dr JS Sodhi is with the AKC Data Systems Pvt. Ltd. (e-mail: jsodhi@akc.in).

have to differentiate between the two privacy perspectives, protection and disclosure [29]. We also aimed to identify what influences users to disclose their information.

This paper shows how social networking sites influence the users without knowing the detail issues of leakage of information which may lead security issues. The purpose of this research paper is to provide countermeasures by raising awareness. It also discusses and warns the community to be more vigilant about the outcome of information leakage. Further the researchers must develop a new framework that can be beneficial to the society.

II. RESEARCH OBJECTIVES

The target is to collect data and analyze how much information is disclosed by the respondents in their profiles and what are the influence factors.

III. RESEARCH QUESTIONS

- RQ1. Which is the most popular Social Networking Site among the users?
- RQ2. What is the purpose of using Social Networking Sites?
- RQ3. What are the activities that users perform on Social Networking Sites?
- RQ4. What is the frequency of using Social Networking Sites?

Specific Objectives of the Study Were-

- B. To find out the role of Social Networking Sites in creating awareness among the users.
- C. To find which is the most popular Social Networking Sites among the users.
- D. To find, what is the frequency of usage of Social Networking Sites.
- E. To find out to what extent users share their personal information.
- F. To find, why the users disclose personal information's on Social Networking Sites.
- G. To find out the consent of users at the time of registration before concur on terms and conditions on Social Networking Sites.
- H. To find whether users can easily update privacy settings on Social Networking Sites.
- I. To find whether the users are willing to pay extra money for security.

IV. SCOPE

This research is confined to the residents of Delhi and NCR, India.

TABLE I
SAMPLING DATA ANALYZING DETAILS

Sampling Technique	Convenient Sampling
Sample Unit	Students, Academicians, Corporate persons
Sample Frame	SNS's users and non-users in Delhi and NCR, India
Sample Size	1205

V. METHODOLOGY

For the collection of primary data questionnaire method was adapted designed by 6 academicians and 4 industrialists. The empirical data was gathered with a web questionnaire that was prepared on the basis of the objective of the proposed study and was distributed randomly among the target population under the study. Variables were measured with categorical, scale, and non-metric variables. Also some open questions were used for feedback. The questionnaire consisted of four main parts:

1. Background information
2. Users personal information and friends on SNSs
3. Users privacy setting
4. User's security concerns.

780 respondents were asked to answer the questionnaire via a link provided through e-mail. These users had also the possibility to send the invitation forward. Using the snowball effect total of 1205 acceptable responses was received.

VI. EMPIRICAL STUDY

Total number of 1205 people responded to the online questionnaire. Of this 37% were male and 63 % were females. Majority of the 748 (62%) respondents fall between the age group of 20-40 years, 415 respondents (i.e. 34%) fall between 12-19 years, 35 respondents (i.e. 3%) are between 41-50 years whereas 7 (i.e. 1%) of the respondents are 50 years + who used SNSs. Most of the respondents (72%) were students and academicians and only 28% were professionals [29]-[31].

Fig. 1 shows that the most commonly used SNSs is Facebook [25], as the data depicts that 573 respondents (47.55%) are using Facebook, 271 respondents (i.e. 22.49%) are using Twitter, 227 respondents (i.e. 18.84%) are using LinkedIn, 62 respondents (i.e.5.14%) are using MySpace, 31 respondents (i.e. 2.57%) are using Flickr, 23 respondents (i.e. 1.91%) are using Orkut and 18 respondents (i.e. 1.49%) are using other Social Networking Sites.

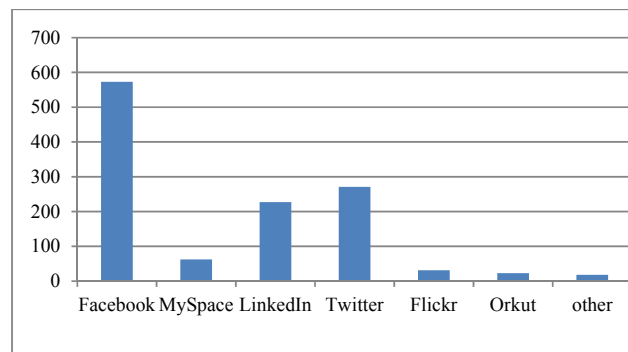


Fig. 1 Use of Social Networking Sites

Fig. 2 (a) presents the frequency of accessing SNSs, among the respondents from Delhi and NCR, India. The data depicts that 670 (i.e.55.60%) respondents are using SNSs daily, 369 (i.e. 30.62%) respondent's access SNSs thrice a week, 119 respondent's (i.e. 9.87%) access once a week whereas 47

respondents (i.e. 3.90%) are accessing their SNSs once in a month.

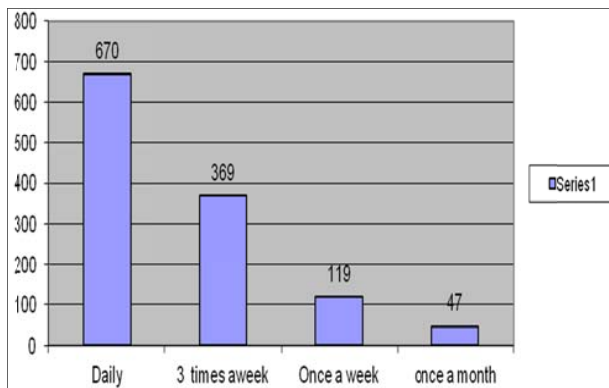


Fig. 2 (a) Accessing Social networking Sites

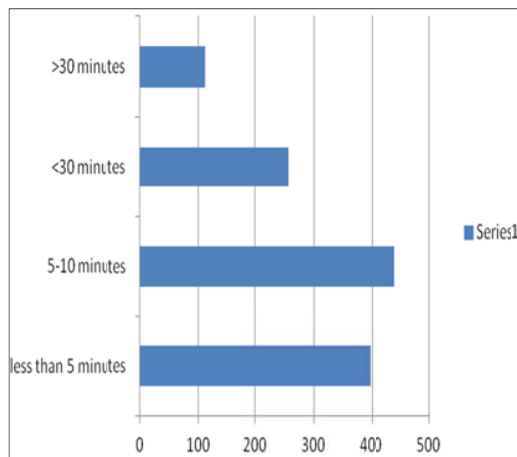


Fig. 2 (b) Session time spent in SNSs

Fig. 2 (b) presents the average time spent by the respondent on their favorite social networking sites. Per session varies from five minutes to thirty minutes. 440 (i.e.36.51%) respondents spend 5 to 10 minutes, less than 5 minutes by 397(i.e. 32.94%) users, 257 respondent's (i.e. 21.32%) access for less than 30 minutes whereas 111 respondents (i.e. 9.21%) spends more than half an hour per session in SNSs.

Fig. 3 reveals that 547 respondents (i.e. 45.39%) use SNSs because of friends as their main interest, 245 respondents (i.e. 20.33%) users have interest towards entertainment and food, 136 respondents (i.e. 11.28%) love to access Social Networking Sites because of music, 82 respondents (i.e. 6.80%) did blogging, 54 (4.48%) respondents access due to romance whereas 38 (i.e. 3.15%) have other reason like news, advertisements etc. to use SNSs [17].

Fig. 4 shows that 655 (i.e. 54.35%) respondents state that they have more than 200 friends, 252 respondents (i.e. 20.91%) have more than 500 friends, 146 (i.e.12.11%) respondents have more than 100 friends, 88 (i.e. 7.30%) and 64 (i.e.5.31%) respondents have friends ranging from 10 to 99 as the number of friends connections in their Social

Networking Sites.

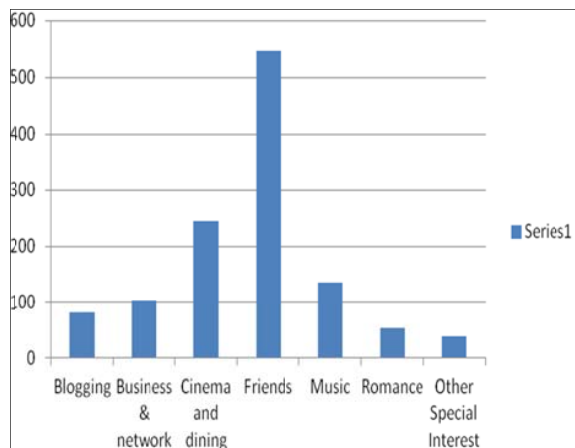


Fig. 3 Respondents curiosity towards SNS

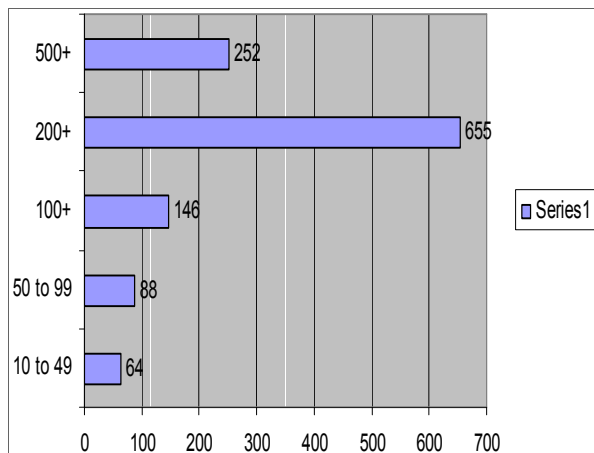


Fig. 4 Number of friends in SNSs

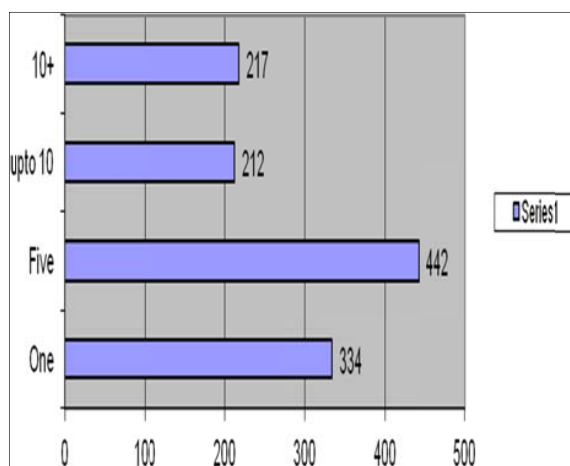


Fig. 5 Number of community groups

Fig. 5 reveals that 334 (i.e.27.71%) members have only one community, 442 (i.e. 36.68%) members have five

communities, 212 (i.e. 17.59%) respondents have up to 10 groups and 217 (18%) users have more than 10 community groups in a Social Networking Sites.

Table II reveals the information and data that are considered to be personal by the respondents of Social Networking Sites.

TABLE II
MOST RARELY DISCLOSED PERSONAL INFORMATION

Information	No. of Respondents	Percentage (%)
Your fingerprints	200	16.60
Financial Information	187	15.52
Your home address	159	13.20
Your mobile no.	129	10.71
Medical information	124	10.29
Your national identity	113	9.38
Your national identity	113	9.38
Your photos	117	9.71
Who your friends are	98	8.13
Your work history	78	6.47
TOTAL	1205	100

In online social networks the respondents must enter profile, work place, education, arts and entertainment and other basic information like gender, e-mail, hobbies etc. After knowing about their interest, and interaction, the malicious user filters such profile information which helps in accessing their private details. The members of the Facebook are asked to enter the profile information manually and it depends on the respondents, to enter his/ her details or avoid revealing the details. The profile is said to be public if the information about the member is made public and it is private if the information is not revealed [38], [41], [45].

Fig. 6 shows why the respondents disclose their personal information on an open platform of social networking sites where 674 (i.e. 55.93%) users like to connect with others, 240 (i.e.19.91%) respondents enter to access certain services, 123 (i.e. 10.20%) does it for fun whereas 111 (i.e.9.21%) respondents feels that they save time at the next visit and 57 (i.e. 4%) fills information for some other reason.

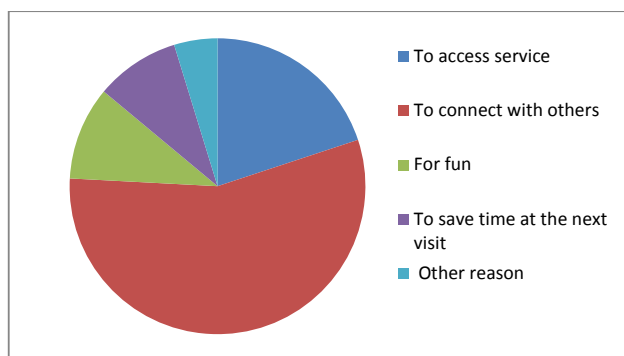


Fig. 6 Reason to disclose Personal information on SNSs

Fig. 7 reveals that 769 (i.e. 63.81%) respondents agrees that the data on social networking is somewhat secure, 213 (i.e. 17.67%) respondents agrees that data is not at all secure, according to 136 i.e.11.28%) respondents it is very secure

whereas 87 (i.e.7.21%) respondents have no idea whether their data is secured or not.

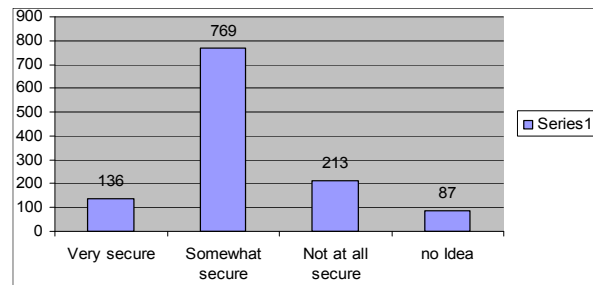


Fig. 7 Data security assessment in SNS

Table III shows what preventive measures the user generally adapts to protect his identity in Social Networking Sites. Where 300 (i.e. 24.89%) responds that they disclose only to trusted people, 324 (i.e. 26.88%) reveals to give minimum information, 112 (i.e.9.29%) responds never disclose personal identity numbers like password, pin no. bank account number etc. 26 (i.e.2.15%) deletes the cookie, 123 (i.e. 10.20%) respondents provide wrong information, 112 (i.e. 9.29%) prefers to use cash instead of recorded transaction whereas 23 (i.e.1.90%) respondents prefer to check that the site has safety logo and the transaction is protected, 13 (i.e.1.07%) users has anti-spy software, 93 (i.e. 7.71%) respondents changes the default browser setting, 49 (i.e. 4.06%) respondents maintain awareness through search engine and 30 (i.e. 2.48%) respondents are least interested about.

TABLE III
PREVENTIVE MEASURES TAKEN BY USERS FOR IDENTIFY PROTECTION ON SNS

To secure Identity	Number of Respondents	Percentage (%)
Give the minimum required information	324	26.89
Disclose information only to people/organization you trust	300	24.90
Provide wrong information	123	10.21
Never disclose password, bank a/c no. or pin no.	112	9.29
Use cash instead of recorded transaction	112	9.29
Change the security of your browser to increase privacy	93	7.72
Use a search engine to maintain awareness of which information circulates about you on internet	49	4.07
Don't do anything	30	2.49
Delete cookie	26	2.16
Check that the transaction is protected or the site has safety logo	23	1.91
Use anti -spy software	13	1.08
TOTAL	1205	100

Fig. 8 shows the interest of respondents to assure whether prior approval is required for processing any personal information, as 790 (i.e. 65.56%) agrees in all cases, 140 (i.e. 11.61%) users says only when asked on internet, 86 (i.e. 7.13%) respondents says not required, 59 (i.e.4.89%) agrees to sensitive information whereas 130 (i.e. 10.78%) respondents

don't know, if required.

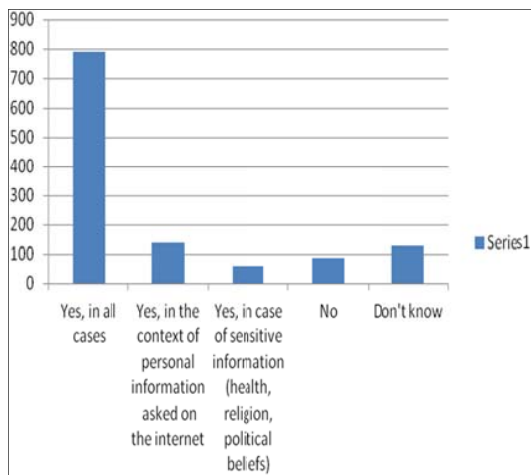


Fig. 8 Proportion of seeking approval by SNS to its users before using their data

In Fig. 9, when the respondents were asked if they would like to pay for accessing their personal information, 205 (17.01%) respondents said yes whereas 1000 (i.e. 82.98%) respondents didn't agreed to pay for the same.

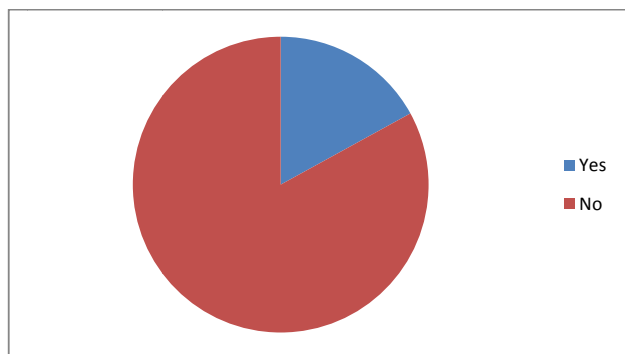


Fig. 9 Personal Information should be accessible on Payment

Fig. 10 shows that 718 (i.e. 59.58%) respondents suggests they themselves must take care of the information being posted whereas 427 (i.e. 35.43%) respondents feels the SNSs administrators, 41 (i.e. 3.40%) feels it should be outsourced to some third party whereas 19 (i.e. 1.57%) respondents don't know who and how their information should be protected.

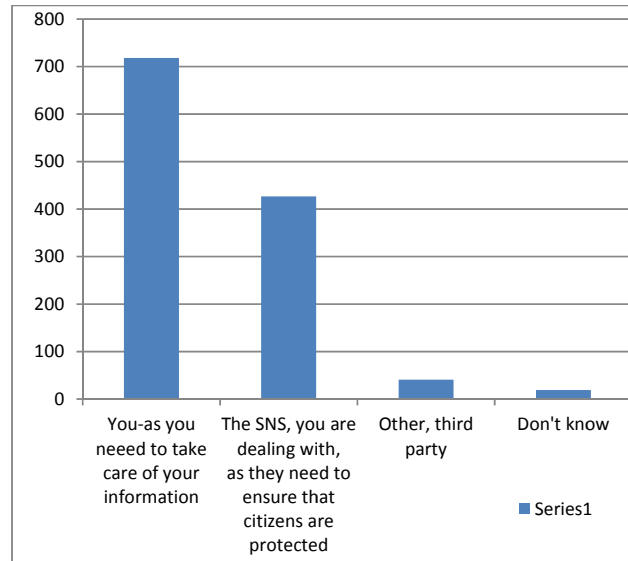


Fig. 10 Who will take care of data protection

Fig. 11 shows that 730 (i.e.60.58%) respondents are concerned about entering their name in search engine whereas 390 (i.e. 32.36%) users are not concerned and 85 (i.e. 7.05%) respondents don't care.

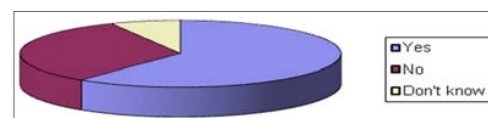


Fig. 11 Concern of typing user name in search engine

Fig. 12 reveals the disclosure of data or information is risky as 352 (i.e. 29.21%) respondents agrees that their information being used by SNSs without their knowledge, 469 (i.e. 38.92%) respondents acknowledged that their data is shared with third parties without agreement, 123 respondents (i.e. 10.21%) are themselves being the victim of fraud, also 123 respondents (i.e. 10.21%) information is shared in different contexts other than where they disclosed, 19 respondents (i.e. 1.58%) are victim of online theft, 119 respondents (i.e. 9.88%) had their data being shared for commercial offers or any other contexts.

Fig. 13 reveals whether the user read terms and conditions while registering in social networking sites, 430 (i.e. 35.68%) respondents don't read the terms and conditions, 299 respondents (i.e. 24.81%) ignores, 254 (21.08%) respondents do not understands and 199 (16.51%) respondents read them carefully whereas 23 (1.91%) respondents are not concerned about the same.

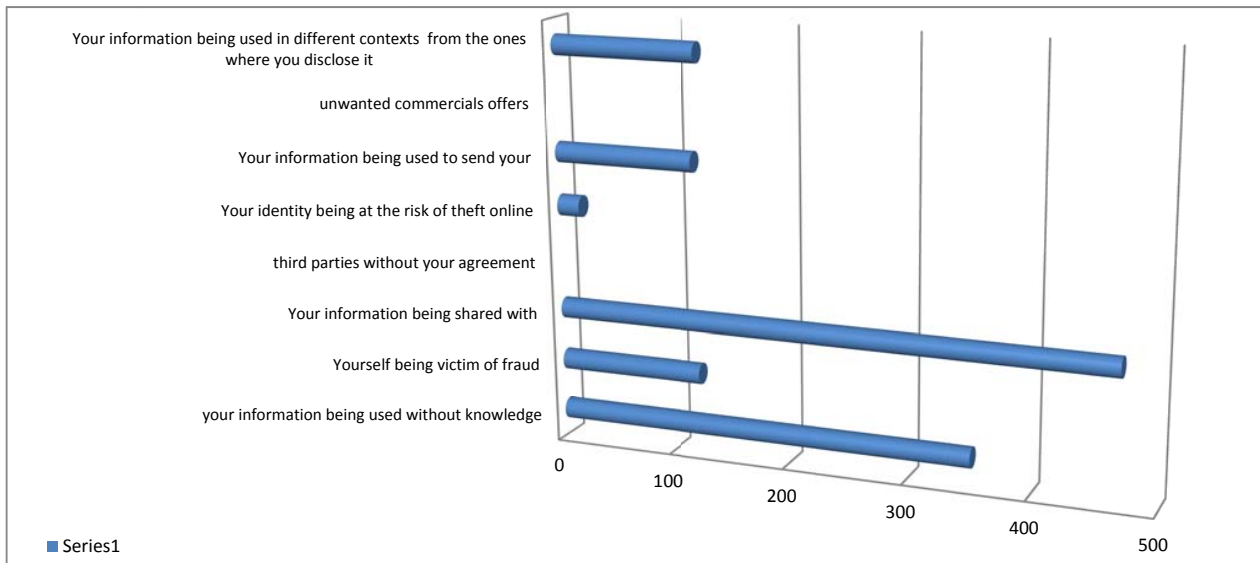


Fig. 12 The risk associated with information disclosure

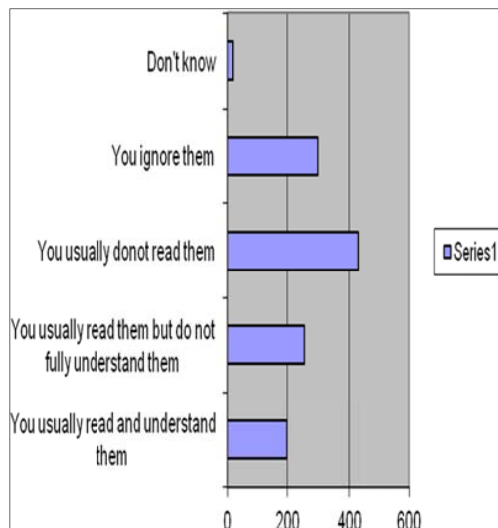


Fig. 13 Response towards consent on terms and conditions

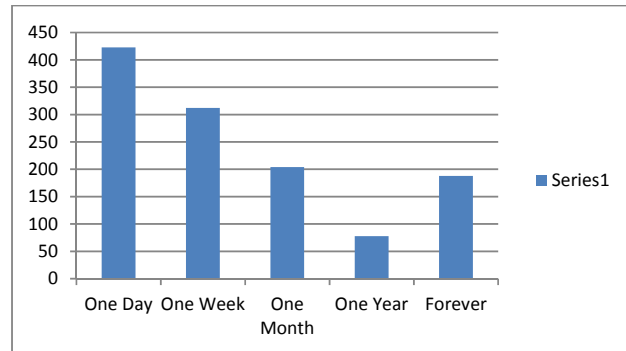


Fig. 14 Addiction to SNSs

Fig. 14 shows how much inclination the user has towards Social Networking Sites, if they are being asked not to access their SNSs for some duration, 423 respondents (i.e. 35.10%) for a single day, 312 respondents (i.e. 25.89%) can stay away for a week and 204 (i.e. 16.93%) for a month and 78 (i.e. 6.47%) respondents for a year and 188 respondents (i.e. 15.60%) forever.

Fig. 15 shows that 785 (i.e. 65.15%) respondents agreed of experiencing data loss directly or indirectly as they know through media, 217 respondents (i.e. 18.01%) have heard from others, 112 (i.e. 9.29%) respondents have lost their data and 91 respondents (i.e. 7.55%) ensured that their family members or friends lost data in last 12 months.

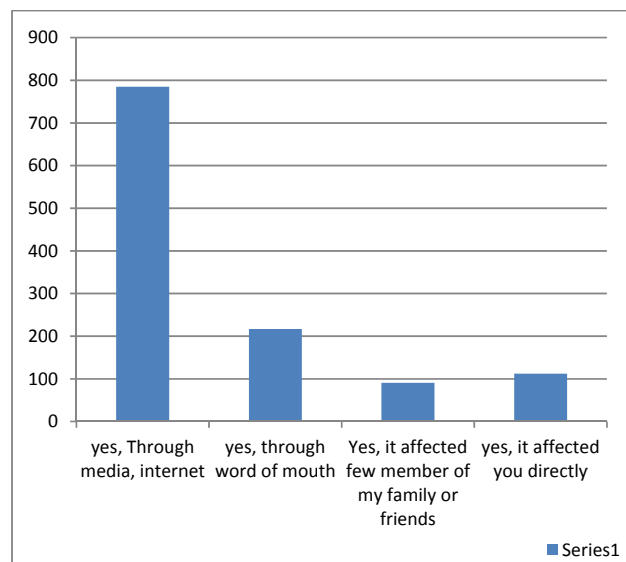


Fig. 15 Respondents' data loss

The study of [3] shows that only a small number of users change the default privacy references which are set to maximize the visibility of user's profiles. Anyhow privacy features has no meaning if the end user does not use them. The reason not taking any initiative to change privacy setting as user find learning and reading privacy policies are time consuming and are very confusing, or the users lack confidence and fear that they will mess up the settings [24].

In today's digital era, information is extensively stored in the form of digital images, audio and video files. Security is an important criterion for data exchange and an important concern for most organizations to protect our personal data from hackers by implementing encryption techniques [43].

Table IV shows the eagerness of users to change default privacy setting in social networking site where 937 agrees, 227 disagrees and 41 respondents never thought to change.

TABLE IV
ALTERATION MADE IN DEFAULT PRIVACY SETTING

Ever tried to change Privacy Setting	No. of Respondents	Percentage (%)
Yes	937	77.76
No	227	18.84
Don't ever thought	41	3.40
TOTAL	1205	100

VII. DISCUSSION

Research results presented in the previous section seem to suggest that Facebook is the most popular SNSs used by all categories of respondents followed by Twitter and LinkedIn. Whereas the earlier finding confirms the result that Facebook and MySpace are most popular social networking sites [11].

Our study shows, that the users of Social Networking Sites discloses a large amount of information about themselves to their weak and strong connections, in spite of having significant awareness that they must disclose only to the people they know.

There occur discrepancies between privacy concerns and actual privacy settings [6], [8] Analysis of profiles found that SNS users provide a large amount of personal information on public profiles. [4] Found that only a small percentage had changed the default privacy settings. Reference [48] analyzed that only 27% were set to private. In 2007, [35], [38] downloaded the Facebook profiles of a whole class of a private American university and found that only one third was set to private.

Reference [32] concludes social networking sites are the greatest social technological phenomenon's of the 21st century. Most users are unaware of the several threats that are present with users profile page. As the popularity of social networking sites continues to grow, so do the security risks associated with them [28].

Also privacy policy seems to be important but the users do not read the privacy policies [5], [50]. Only a small percentage of users read the privacy policies before accepting them [12], [15], [55].

The study found that the main purpose of using SNSs is to find information, the newsfeed and updates of their friends.

They disclose information in order to connect with their friends. They post many kinds of information freely related to personal behavior, experimentation and their own sentiments. [9], [21], [39] concluded that most important reason is to get in contact with new people (31%). The second reason was to keep in touch with their friends (21%), whereas the third was general socializing (14%) from open questions to 1,200 SNS users.

Reference [7] analysis indicates that it is essential to provide users with the suitable tools that allow them to recognize the context in which their information exists and select appropriate levels of information allocation and perform protections on their personal information.

The study shows that the user's information is used by the host or third parties for marketing or other beneficiary task without users intimacy [2], [12].

The respondents are cautious about the information being displayed or searched by their colleagues or known friends [12], [14], [15], [20].

The study found that the users are not ready to pay for security of their private data in social networking sites. References [3], [52] agree that users will be more careful if they pay additional fee amount for their access in social media.

The study shows that there must be prior approval or consent of user before sharing personal information [5], [52].

The study shows that the theft or data loss is very common as it is known to major community. In paper [1] researchers concludes that information loss or damages in many organizations is by their employees. Employee's social networking behavior, accidental or intentional, provides an opportunity for advanced persistent threats attackers to realize their social engineering techniques.

The users are doting of accessing the SNSs as they spend on an average of 3 hours daily, also they cannot miss to access more than a day. Respondents have more than 200 friend connections.

The study reveals that majority population agrees that Social Networking Sites are somewhat secure in context to data protection [46].

The study found that majority of users are not interested to change the default privacy settings as they find it either time consuming, or they might messed up the settings due to incomplete knowledge [13], [36].

VIII. CONCLUSION

This paper investigates privacy issues related to SNSs and presented the results of our qualitatively empirical studies among users. This study was focused on, the use of Social Networking Sites and related privacy awareness to protect users information.

This study employs users of SNSs, and acquired data based on users response. The analyzed data shows that most users' preference is Facebook.

Results show that most of the respondents with their knowledge discloses considerable amount of private information of them and are not aware of the visibility and

leakage of information to unknown people and third party service providers. Also the privacy policy and terms of use are either not known or understood by our respondents. There are many different factors that affect privacy behavior on Social Networking Sites.

REFERENCES

- [1] Abdul Molok, Nurul Nuha and Ahmad, Atif and Chang, Shanton "Information Leakage through online social networking: opening the doorway for advanced persistence threats". The Journal of the Australian Institute of Professional Intelligence Officers (AIPIO), 19 (2). pp. 38-55. (2011)
- [2] Abu Bashar, "Effectiveness of Social Media as a Marketing Tool: An Empirical Study", more International Journal of Marketing, Financial Services & Management Research Vol.1 Issue 11, November 2012
- [3] Acquisti, A., & Gross, R. (2006), "Imagined communities: Awareness, information sharing, and privacy on the Facebook", Proceedings of 6th Workshop on Privacy Enhancing Technologies (pp. 36–58), In P. Golle & G. Danezis (Eds.), Cambridge, UK: Robinson College.
- [4] Acquisti Alessandro, Gross Ralph, "Information revelation and privacy in online social networks", WPES '05 Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp 75-80, 2005
- [5] Ai Ho, Abdou Maiga, Esma Aïmeur, "Privacy protection issues in social networking sites". Conference: The 7th IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009,
- [6] Barnes, Susan B. "A privacy paradox: Social networking in the United States." *First Monday* 11.9 (2006).
- [7] Barrigar, Jennifer. Social network site privacy: A comparative analysis of six sites. Office of the Privacy Commissioner of Canada, 2009.
- [8] blog.reyjunco.com/pdf/Chapter6.pdf
- [9] Barnes, John Arundel. "Who should know what?: social science, privacy, and ethics." (1979).
- [10] Benevenuto F., Rodrigues T., Cha M., and Almeida V., "Characterizing user behavior in online social networks," Proc. of the 9th ACM SIGCOMM Internet Measurement Conference, pp. 49–62, 2009.
- [11] Batagelj, Vladimir, and Andrej Mrvar. "Some analyses of Erdos collaboration graph." *Social networks* 22.2 (2000): 173-186.
- [12] Bosch, T.E. (2009), "Using online social networking for teaching and learning: Facebook use at the University of Cape Town", *Communication*, 35 (2): 185-200.
- [13] Barnes, Susan B. "A privacy paradox: Social networking in the United States." *First Monday* 11.9 (2006).
- [14] Boyd Danah and B. Ellison Nicole, "Social Network Sites: Definition, History, and Scholarship", *Journal of Computer-Mediated Communication* Volume 13, Issue 1, pages 210–230, October 2007
- [15] Boyd D and Eszter Hargittai, "Facebook privacy settings: Who cares?" *First Monday*, Volume 15, Number 8-2 August 2010 <http://firstmonday.org/ojs/index.php/fm/article/view/3086/2589>
- [16] Braman, James, et al. "Preparing Your Digital Legacy: Assessing Awareness of Digital Natives." *The Social Classroom: Integrating Social Network Use in Education: Integrating Social Network Use in Education* (2013): 208.
- [17] Calvi, L., Cassella, M., Nuijten, K. (2010). "Enhancing users' experience: A content analysis of 12 university libraries Facebook profiles", In *ELPUB 2010 International Conference on Electronic Publishing*, Helsinki (Iceland), 16-18 June, pp.258-269.
- [18] Cheung, C. M. K., Chiu, P. Y., Lee, M. K. O. (2010). "Online social networks: Why do students use Facebook?", *Computers in Human Behavior*, Article in Press.
- [19] Claudia Hauff, Geert-Jan Houben, "Deriving Knowledge Profiles from Twitter", in *Proceedings of EC-TEL 2011 (LNCS 6964)*, pp. 139-152.
- [20] Dwyer, Catherine; Hiltz, Starr Roxanne; and Passerini, Katia, "Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace" (2007). *AMCIS 2007 Proceedings*. Paper 339.
- [21] Elisa Lehtinen Vilma, "Maintaining and Extending Social Networks in IRC-galleria", *Helsingin yliopisto - Helsingfors universitet - Helsinki University*, 2007.
- [22] Fabricio Benevenuto, Tiago Rodrigues, Meeyoung Cha, Virgilio Almeida, "Characterizing User Behavior in Online Social Networks", *Proceedings IMC'09 9th ACM SIGCOMM conference on Internet measurement* 2009
- [23] Govani, Tabreez, and Harriet Pashley. "Student awareness of the privacy implications when using Facebook." unpublished paper presented at the "Privacy Poster Fair" at the Carnegie Mellon University School of Library and Information Science 9 (2005).
- [24] Hattori Yuki, Nadamoto A, "Extraction and Categorization of Tip Information from Social Media", *Proceedings of the International Multi Conference of Engineers and Computer Scientists, Hong Kong (IMECS 2013)*
- [25] Helms, R. "Suitably Social: How FMCG brands can best use social media for engaging with their customers", *University of Edinburgh Business School, Masters of Business Administration*. (2010)
- [26] Hew, K.F. (2011). "Students' and teachers' use of Facebook", *Computers in Human Behavior*, 27: 662-676.
- [27] <http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf>.
- [28] <http://www.gilc.nl/privacy/survey/intro.html>
- [29] <http://www.techopedia.com/definition/4956/social-networking-site-sns> 2013
- [30] <https://members.reccenter.stonybrook.edu/PrivacyStatement.aspx>
- [31] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf. 2010
- [32] Herman, Roblyer, M.D., McDaniel, M., Webb, M., J., Witty, J.V. (2010). "Findings on Facebook in higher education: A comparison of college faculty and student uses and perceptions of social networking sites", *Internet and Higher Education*, 13: 134-140.
- [33] Jefferson Lane, "Social Networks Media in Academia", *Journal of Information Science*, vol2, page34-56, 2009.
- [34] J. Tang, T. Lou, and J. Kleinberg, "Inferring social ties across heterogeneous networks," presented at the *Proceedings of the fifth ACM international conference on Web search and data mining*, Seattle, Washington, USA, 2012.
- [35] Joud Albakr, "Awareness of Social Networking Security, 2014" <http://prezi.com/e42yoscdlgo/awareness-of-social-networking-security/>
- [36] Katharina Krombholz, Dieter Merkl, Edgar Weippl, "Fake Identities in Social media: A case Study on the Sustainability of the Facebook Business model", *Journal of Service Science Research* (2012) 4:175-212
- [37] Lehtinen Vilma, Näsänen Jaana, Sarvas Risto, "A little silly and empty-headed: older adults' understandings of social networking sites", *BCS-HCI '09 Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology*, Pages 45-54.
- [38] Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy: An analysis of college student privacy settings in an online social network. *Journal of Computer-Mediated Communication*, 14(1), 79-100.
- [39] Liu Y, Gummandi K, Krishnamurthy B, & Mislov, "Analyzing Facebook privacy settings: User expectations vs reality" in: *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference, IMC'11*, ACM, New York, USA: 61-70
- [40] Mazman, S.G., Usluel, Y.K. (2010). "Modeling educational usage of Facebook", *Computers & Education*, 55: 444-453.
- [41] Nancy p, R.Geetha Ramani, "Knowledge Discovery (Email harvesting, gender Identification & Prediction) in Social Network Data (Facebook 100 Million URL)", *Proceedings of the World Congress on Engineering and Computer Science*, WCECS 2012, San Francisco, USA 2012
- [42] Petter Bae Brandtzaeg, Jan Heim, "Online Communities and Social Computing" *Third International Conference, OCSC 2009, Held as Part of HCI International 2009*, San Diego, CA, USA, July 19-24, 2009. *Proceedings*
- [43] Sharma Shilpi, J. S. Sodhi. "Awareness on Confidentiality in Social Networking Sites", *International Journal of Scientific & Engineering Research*, Volume 4, Issue 4, p.1664-1670, April-2013
- [44] Sivakumar, T., and R. Venkatesan. "A Novel Approach for Image Encryption using Dynamic SCAN Pattern." *IAENG International Journal of Computer Science* 41.2 (2014): 91-101.
- [45] S. Sodhi J., Sharma Shilpi, "Conceptualizing of social Networking Sites", *IJCSI International Journal of Computer Science Issues*, Vol. 9, No 1, Issue 1, p.p 422-428, January 2012.
- [46] Strater K, Lipford HR, "Strategies and struggles with privacy in an online social networking community. In: proceedings of 22nd British HCI Group Annual conference on People and Computers: BCS-HCI, UK 2008, 1:111-119
- [47] Stutzman F, Capra R, & Thompson J (2011), "Factors meditating disclosure in social network sites. *Computers in human behavior* 27(1):590-598. DOI 10.1016/j.chb.2010.10.017
- [48] Stutzman F, Kramer- Duffield J (2010) Friends only: Examining a privacy enhancing behavior in Facebook, In: *proceedings of the 29th*

- international Conference on human factors in Computing Systems CHI'10, ACM, New yorkUSA:1553-1562
- [49] Thelwall, M. (2008). Social networks, gender and friending: An analysis of MySpace member profiles. *Journal of the American Society for Information Science and Technology*, 59(8), 1321–1330.
 - [50] Tommy K H Chan, Xiabing Zheng, Christy M K Cheung, Matthew K O Lee and Zach W Y Lee, "Antecedents and consequences of customer engagement in online brand communities, *Journal of Marketing Analytics* 2, 81-97 (June 2014)
 - [51] V., Viswanath, A., Mislove, M., Cha, & K.P., Gummadi, "On the evolution of user interaction in Facebook", *Proceedings of the 2nd ACM SIGCOMM Workshop on Social Networks*, Barcelona, Spain, August 17, 2009.
 - [52] Wüest, Candid. "The Risks of Social Networking." Symantec http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_risks_of_social_networking.pdf (2010).
 - [53] Xing Xing, Weishi Zhang, Zhichun Jia, Xiuguo Zhang, "Trust-Based Social Item Recommendation: A Case study", *2nd International Conference on Computer Science and Network Technology 2012 IEEE Changchun, China*.1050-1053, 2012
 - [54] Zaideh A. J. Y., "The Use of Social Networking in Education:challenges and Opportunities," *World of Computer Science and Information Technology Journal(WCSIT)*, vol.2,pp.18-21,2012
 - [55] Zainab Asif, Mamuna Khan, "Users Perceptions on Facebook's Privacy policies" *ARNP Journal of Systems and Software*, vol. 2, no. 3, March 2012.