Asian Journal of Information Science and Technology
ISSN: 2231-6108 (P) Vol.8 No.1, 2018, pp.33-38

DOI: https://doi.org/10.51983/ajist-2018.8.1.168

Social Networking Websites and Privacy Concern: A User Study

Krishanu Dey[1] and Parikshit Mondal[2]
[1]Ph.D. Scholar, Librarian, Ramakrishna Mission Vidyamandira, Calcutta, India
[2]Assistant Professors Dept. of Library and Information Science, University of Calcutta
E-mail: krishanudey.15@gmail.com , parikshit.cu@gmail.com
(Received 15 December 2017; Revised 4 January 2018; Accepted 24 Janaury 2018; Available online 3 February 2018)

Abstract **- With the advent of the online digital mode of communication the traditional communication tools are losing their grounds. The increasing popularity of the Social Networking websites has paved new ways of online communication. But the social networking sites have also eroded some privacy related ethical questions in the mind of the researchers. This paper aims to identify the privacy related issues related to the social networking websites. As a representative of the social networking websites Facebook has been studied along with its usage standards and policies. To fulfill the aim of the study some relevant literatures are studied and an online survey has been conducted. The study reveals, though most of the people are concerned about the privacy issues while using the social networking sites, they hardly practice the safety norms in the actuality.**
Keywords: **Social Networking Sites, Digital Privacy, Facebook**

I. INTRODUCTION

At present the digital media has evolved as a victorious competitor of the traditional media of communication. The internet being the prime conveyer of the digital communication has arisen and different online social networking websites (SNS) like Facebook, Twitter, LinkedIn, Orkut are gaining their hold upon the world of digital communication. Through these SNSs a person may design his public profile and communicate with alike or known netizens. To design a public profile one must share some information about himself/herself. He/She may disclose his/her age, sex, locality, profession, qualification, etc. the shared information enables them to connect with others and create an online group or community. To safeguard the privacy and safety of the users almost every SNS has a set of policies and settings.

II. LITERATURE REVIEW

Townsend (2016) has sated some ethical guidelines for conducting research on the SNSs. In the e-newspaper The Guardian an article named '2016: the year Facebook became the bad guy' (2016) some case studies have showed the profound influence of Facebook in the ethical and political spheres of the society. Khan (2015) has pointed out the ethical dilemmas concerning the wide use of SNSs. He has also forecasted some probable impacts of using the SNS. Turculet (2014) has described three ethical concerns, i.e. privacy, anonymity and trust in the light modern philosophical thought and has proposed some solutions to avoid any issue concerning the three ethical themes. Williams (2014) has discussed the lack of standardization of SNS use from a sociological aspect. Kasturi (2014) has deciphered some common features and the role of the SNSs in the present day society. Marturano (2011) has sorted the main ethical points of view from which the SNSs can be judged appropriately.

III. OBJECTIVES OF THE STUDY

This study intends to get acquaintance on the following concerns:

1. To identify the probable threats to the online privacy of the SNS users.
2. To identify the level of user awareness regarding privacy issues related to the SNSs.

IV. METHODOLOGY

The relevant literatures are studied to discover the theoretical background of the study. Facebook has been selected as a representative of the popular social networking sites. An online questionnaire has been prepared using Google Forms application and the same has been shared with 120 Facebook users during December, 2017. The responses are summarized with the help of MS Excel and some findings are disclosed.

V. SCOPE AND COVERAGE OF THE STUDY

Though the study aims to study the common privacy concerns of the SNS users the scope has been limited to the study of the Facebook only. Some relevant literatures published in-between 2011 to 2016 have been consulted for pursuing the study. The people both of national and international nativity participated in the survey.

VI. PRIVACY VIOLATIONS

People often share personal information to create their public profile. The intention behind sharing this information is to help others to identify the people they may know. But, if this information is used without the consent of the sharer and the intention is to harm the concerned person, then the instance may be referred to as an ethical blunder. Often the advertisers attempt to go for a behavioral study of a user by

following his/her website search or shared contents. These may increase the relevancy of the advertisements before the particular user but on the other hand these may result into an unethical encroachment in the privacy of the concerned user. Due to this concern most of the SNSs design their own privacy policy to safeguard the shared information available with them.

A. Spamming

In SNSs the advertisers often send promotional advertisements to the users without thinking the relevancy of those to the people. These huge numbers of unwanted spams cover the relevant information and the users miss much necessary information due to the unwanted spams. The issue is ethically not acceptable to the users.

B. Information misuse

Whenever people share some information on SNSs they think that the information will remain private but it is not the fact. Once content is shared it becomes the property of the SNS. Even if after sharing a content one person intends to remove the same from the SNS it may not be possible for him because by that time the content may have been stored and shared by many people.

C.Manipulation of information

It is quite difficult to authenticate the contents shared in SNS. A user may claim any virtue for him or accuse any vice against others. In this case the information goes viral and accepted by others without validating the facts. These attempts may disgrace others or ruin the credibility of the sharer.

D. Anonymous contents

In SNSs often some contents are shared by anonymous sources. The source being unidentifiable the reliability of the information becomes fuzzy. The users get confused and mislead. The information cannot be verified and no one can be blamed for the effects the information may bring forth.

VII. RESULTS AND ANALYSIS

The participants are grouped gender wise and studied to understand their level of concern regarding the privacy issues.

The participants are grouped according to their age to understand their level of concern regarding the privacy issues. We can easily observe from Figure 2 among 120 participants 45% belong to the age group of 20-29 years, 40% belong to the age group of 30-39 years, 5% belong to the age group of 40-49 years, 5% belong to the age group of 50-59 years, 3% belong to the age group of 60-69 years and 2% belong to the age group of 70-79 years.

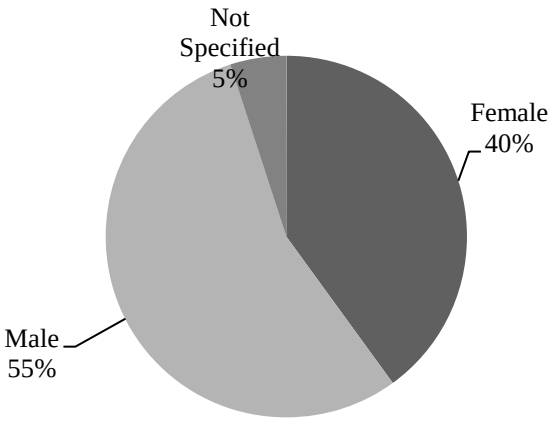

Fig. 1 Depicts among 120 participants 55% are male 40% are female and 5% did not specify their gender.

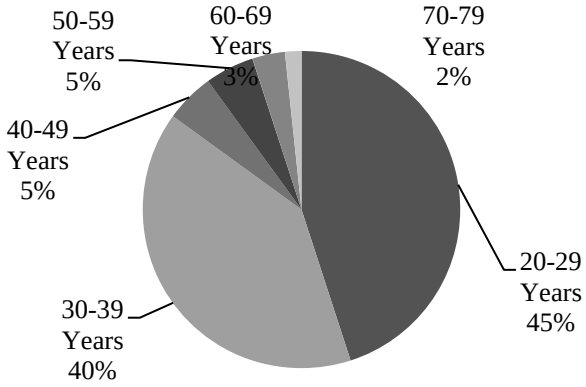

Fig. 2 Age group

The participants are grouped according to their digital proficiency to understand their level of concern regarding the privacy issues.

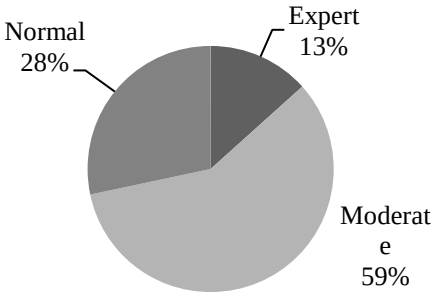

Fig.3 Usage of Social networking

Figure 3 shows that among 120 participants 59% are moderate, 28% are normal and 13% are expert. The participants are grouped according to the frequency of changing their Facebook passwords at regular intervals.

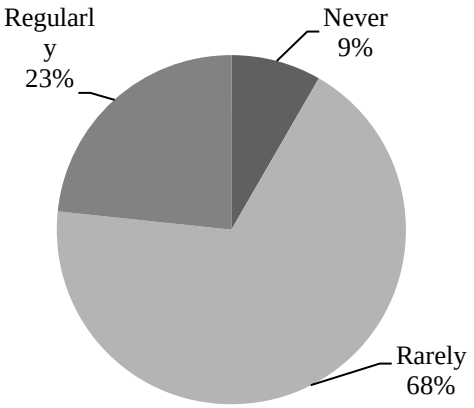

Fig. 4 Frequency of usage

Figure 4 depicts among 120 participants 68% change their passwords rarely, 23% change their passwords regularly and 9% never changed their passwords.

The participants are grouped according to the awareness of them regarding the use of robust passwords.

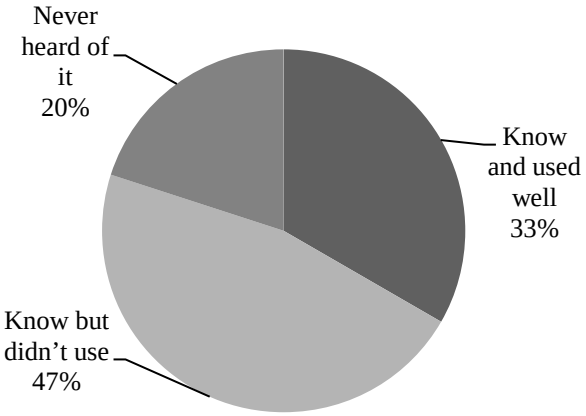

Fig. 5 Robust Password

Figure 5 exhibits that among 120 participants 47% participants know but don't use robust passwords, 33% participants know and have used the robust passwords, 20% participants never hear of the robust passwords.

The participants are grouped according to the frequency of updating their Facebook app.

From the Figure-6 it can be said easily that among 120 participants 58% update their Facebook app regularly, 34% update the app once or twice and 8% don't update the app at all.

The participants are grouped according to the personal contents disclosed by them on Facebook.

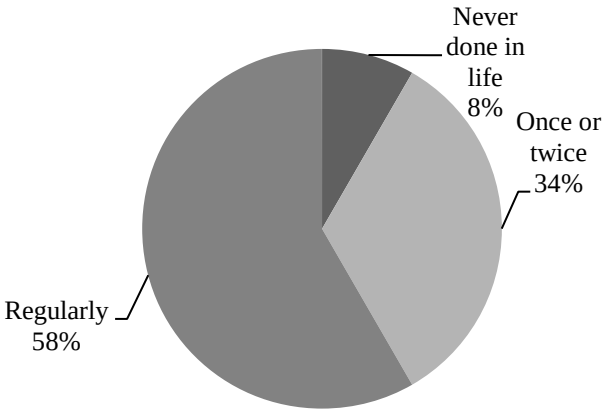

Fig. 6 updating the app frequency

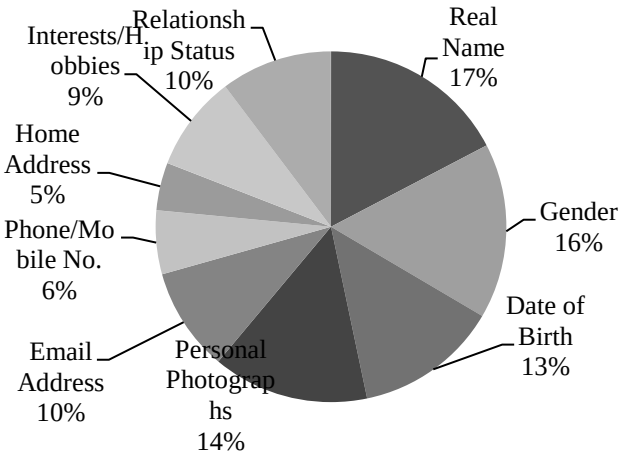

Fig. 7 Disclosing real names

Figure 7 shows that among 120 participants 118 respondents have disclosed their real names, 110 respondents have disclosed their gender, 98 respondents have disclosed personal photographs, 90 respondents have disclosed date of birth, 70 respondents have disclosed their relationship status, 65 respondents have disclosed email address, 60 respondents have disclosed their interests and hobbies, 40 respondents have disclosed their contact numbers, 30 respondents have disclosed their home address.

The participants are grouped according to their awareness of Facebook privacy policies.

Figure-8 clearly represents that among 120 participants 70% are aware of Facebook privacy policy and 30% are not.

The participants are grouped according to their trust towards the privacy protection on Facebook.

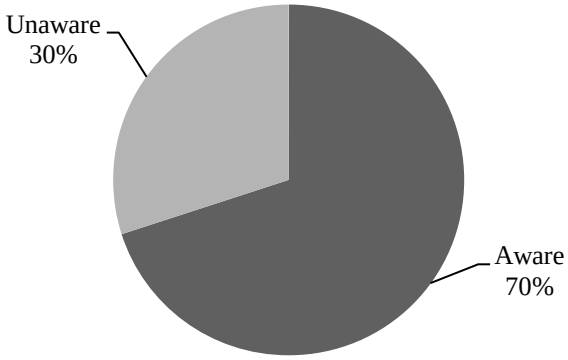

Fig. 8 Awareness of Privacy Policy

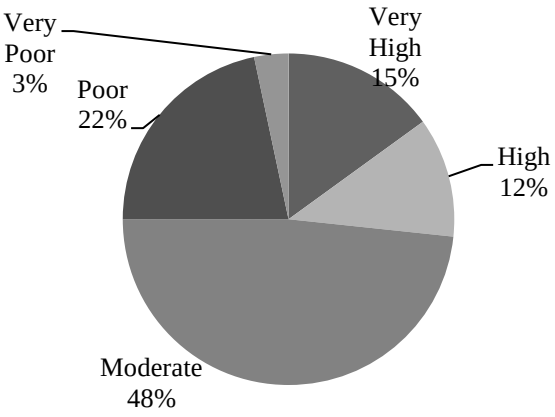

Fig. 9 Trust in privacy protection

As we can observe from Figure-9 among 120 participants 48% trusts Facebook privacy protection policy moderately whereas 22% have shown poor trust, 15% have shown very high trust, 12% have shown high trust and 3% have shown very poor trust.

The participants are grouped according to their experiences of privacy breach on Facebook.

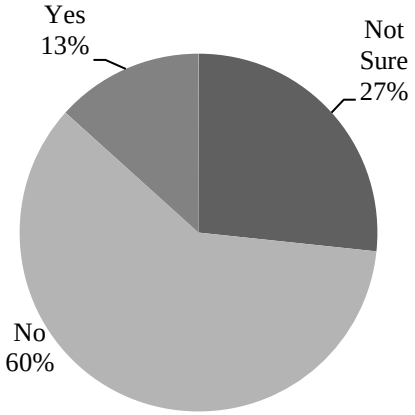

Fig. 10 Privacy Breach experience

The study observes from Figure-10 that among 120 participants 60% have not faced any privacy breach, 27% are not sure whereas 13% have encountered privacy breach.

The participants are grouped according to their willingness to disclose their personal information on Facebook.

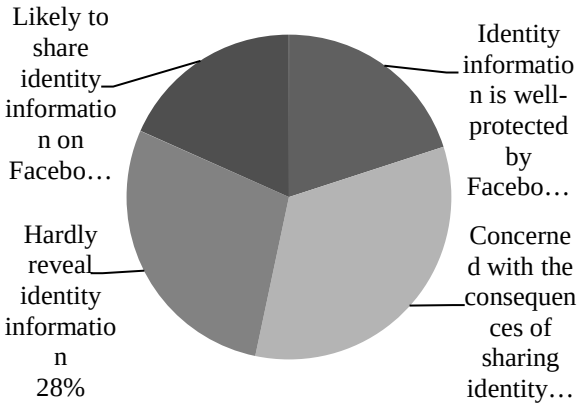

Fig. 11 Concern about the consequences of sharing identity

Figure-11 represents among 120 participants 34% are concerned with the consequences of sharing identity information, 28% are hardly revealing identity information, 20% believe identity information is well-protected by Facebook and 18% don't hesitate to share identity information on Facebook.

The participants are grouped according to their knowledge of probable consequences of privacy while using Facebook.

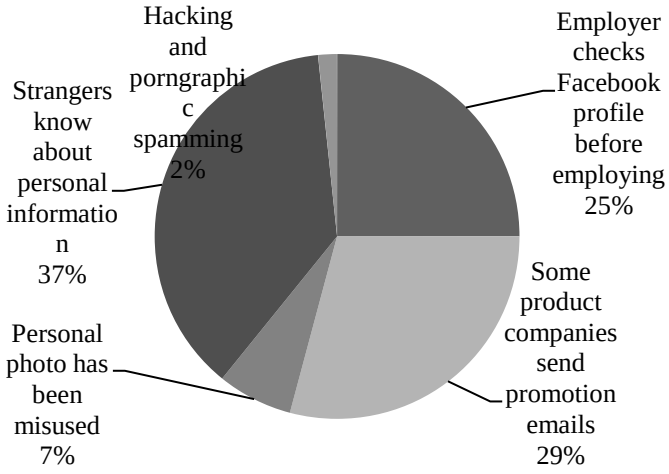

Fig. 12 user belief on Confidentiality of information

Figure-12 depicts that among 120 participants 37% think that strangers may know about their personal information, 29% think that some product companies may send promotional emails, 25% think that employers may check their profile before employing them, 7% think that their personal photographs may be misused and 2% apprehend hacking and pornographic spamming.

The participants are grouped according to their probable action after observing privacy breach on Facebook.

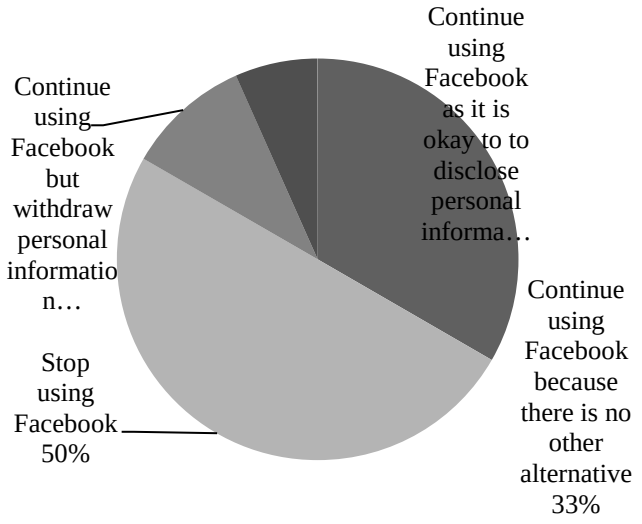

Fig. 13 Continuing usage of Facebook

Figure-13 shows among 120 participants 50% Facebook, 10% would continue using Facebook but withdraw personal information and 7% would continue would stop using Facebook, 33% would continue using Facebook because there is no other SNS as good as using Facebook as it seems alright to disclose personal information on Facebook.

VIII. OBSERVATIONS

1. Male users of Facebook are more concern with the privacy than their female counterparts. (ref. Figure-1)
2. Facebook users aged between 20-29 years are more concerned about their online privacy than the people belonging to the other age groups. (ref. Figure-2)
3. Most participants claim to be moderate in terms of digital proficiency. (ref. Figure-3)
4. Maximum Facebook users rarely change their passwords at regular intervals. (ref. Figure-4)
5. Most people know but don't use robust passwords. (ref. Figure-5)
6. Most people tend to update Facebook app regularly. (ref. Figure-6)
7. Among many type of identity information maximum people have disclosed their real names on Facebook. (ref. Figure-7)
8. Maximum participants are aware of Facebook privacy policy. (ref. Figure-8)
9. Among all the participants maximum people trust the Facebook Privacy Policy moderately. (ref. Figure-9)
10. Maximum participants have not faced any privacy related issues while using Facebook. (ref. Figure-10)
11. Most of the participants are concerned about the consequences of sharing identity information. (ref. Figure-11)
12. Maximum participants think that if they disclose their personal information then the information may be used for commercial or advertising purposes. (ref. Figure-12)
13. Most of the participants have reported that they would stop using Facebook in case of any privacy breach. (ref. Figure-13)

IX. SUGGESTIONS

1. Users shall try to use robust passwords for accessing their Facebook account. There is a provision in Facebook privacy setting which enables a user to add an extra security layer to his/her account by sending a security code to the registered mobile number for logging in.
2. The Facebook Friends or people who will be able to view the shared information shall be familiar to each other.
3. The Facebook app shall be updated at a regular interval to ensure better security.
4. Users shall minutely review the tagged information or advertisements before sharing the same on their timeline.
5. The unknown people shall be blocked from viewing the Facebook Friend list or posting anything on the timeline of the users.
6. Users shall log out from Facebook after using the same on any unfamiliar device and remote log out facility is also available.
7. The Facebook privacy settings allow a user to be notified whenever his/her account is logged in on a device which is not used by him/her for accessing the Facebook earlier.
8. Facebook users may restrict other search engines from showing their profile by customizing their privacy settings.
9. Users shall always keep the backup data of their Facebook activity to be safe from being hacked.

X. CONCLUSION

The discussion shows that with numerous benefits of digital communication the SNSs have brought many serious concerns for their users. Among the issues some may be dealt with the legal procedures but others being matters of morality are not legally applicable. With so many threats to the privacy and safety the digital media should have become more restricted sphere. But if restrictions block the freedom, which we enjoy most while using internet, the condition will be catastrophic. Instead of restricting the use with policy and standards the users may be made aware of the consequences of privacy breach. The users should be very careful in choosing contents for sharing and selecting people who will be able to access those contents.

REFERENCES

[1] A.Marturano,"The Ethics of Online Social Networks – An Introduction". *International Review of Information Ethics*, Vol. 16, pp. 3-5, 2011.

[2] M.Turculet, "Ethical issues concerning Online Social Networks", *Procedia - Social and Behavioral Sciences*, Vol. 149, pp. 967-972, 2014.

[3] S.Kasturi and P.Vardhan, “Social Media: key issues and new challenges: A study of Nalgonda district”, *Global Media Journal*, Vol. 5, No. 1, pp. 1-12, 2014.
[4] H.Williams, “The Lack of Ethical Standards of Online Social Networking”, 2014,
[5] A.A.Khan, “Ethical Issues in Social Networking”, October 10, 2015,. [Online]Available:https://www.researchgate.net/publication/Ethical_Issues_in_Social_Net working
[6] “2016: the year Facebook became the bad guy”, *The Guardian*, December 12, 2016.
[7] L.Townsend and C.Wallace, “Social Media Research: A Guide to Ethics”, 2016