

Analysis and Evaluation of Privacy Issues in Online Social Networks

Rabia Riaz¹, Sanam Shahla Rizvi², Hammad Masood Minhas³, Sana Shokat⁴

¹Department of CS & IT, University of Azad Jammu and Kashmir, Muzaffarabad, 13100, Pakistan

²Raptor Interactive (Pty) Ltd, Eco Boulevard, Witch Hazel Ave, Centurion 0157, South Africa

³Department of CS & IT, University of Azad Jammu and Kashmir, Muzaffarabad, 13100, Pakistan

⁴Department of CS & IT, University of Azad Jammu and Kashmir, Muzaffarabad, 13100, Pakistan

ABSTRACT

Online social networks (OSNs) are increasingly becoming popular tools for social interactions despite the prevailing ambivalence towards them. The issue of privacy is a key concern due to increasing popularity and immense growth in the volume of online data exchange between OSN users. There is a need to realize and deal with the social consequences of confession of unwanted information to unintended audiences. Despite of information disclosure, the issue is more problematic due to a lack of privacy knowledge and related privacy risks on behalf of the users. The core idea of this research is to come up with comprehensive guidelines for protection against unintended information disclosure via OSNs. Although the users can tweak privacy settings related to different information items/categories, authors hypothesize that the complexity of managing privacy settings, accompanied by increasingly negligent default settings, leads to unintended information disclosure.

Keywords: Information and Communication Technologies, Online Social Networks, Social Inclusion and Cohesion Enabling Approaches, Privacy, Facebook, Trust Management

Author's Contribution

^{1,2,3,4}Manuscript writing, Planning of Research, Data Collection, Data analysis & interpretation, Conception, synthesis, planning of research & Discussion

Address of Correspondence

Rabia Riaz
[rabiaiqbal18@gmail.com/](mailto:rabiaiqbal18@gmail.com)
rabia.riaz@ajku.edu.pk

Article info.

Received: Feb 23, 2019
Accepted: Dec 07, 2019
Published: December 30, 2019

Cite this article: Riaz R, Rizvi SS, Minhas HM, Shokat S. Analysis and Evaluation of Privacy Issues in Online Social Networks. *J. Inf. commun. technol. robot. appl.* 2019; 10(2):59-69

Funding Source: Nil
Conflict of Interest: Nil

INTRODUCTION

An online social network (OSN) is an online platform that people use to build social links or relationships with other people. They create social networks so that they can share common activities, similar personal or career interests, real-life associations, or background. Online social networking is a great source of interaction. In computer networks, OSNs describes the perfect demonstration of graphs, where nodes are showing users and edges represent relationships between them. The

majority of the people spend a lot of their time on OSNs.

A set of privacy policies that force the system to protect personal information can also be defined as a willingness to share information and their reaction to unintended parties viewing or using this information [1],[2]. Privacy is a major concern that is discussed by the researchers. Authors should understand privacy is an umbrella term for a group of related yet distinct things. Privacy is about respecting the desires of individuals were

compatible with the aims of the larger community. Privacy is not merely an individual right, it is an important component of any flourishing community. OSNs have various merits and demerits. If you have a huge number of friends in these sites than there are strangers too which can snoop user information and can cause some common privacy issues among younger's including harassment, identity theft etc. It has been perceived that young users don't bother about privacy risks due to which several threats are associated with posting their personal details on OSNs.

One of the most important threats that the users have to face is identity theft. These issues also give birth to several social evils such as financial and terrorism risk, physical and sexual extortion etc [3]. On the internet the top most visited social networking site is Facebook which had 1.5 billion monthly active users. As this site is available for every user so its openness also creates some major issues regarding security. Privacy is essential in an extensive range of applications that pursue to protect the user's information related to their location and other details too. As it's a diverse concept so no single definition of privacy can include all the characteristics related to it [4]. There is no privacy standard for controlling the user's personal information settings as it varies from site to site.

The main focus of this study is to scale the level of understanding of the privacy settings of Facebook and exposure to privacy risks due to negligent default settings. This study is restricted to Facebook because it is the most commonly used OSN site in the state of Azad Jammu & Kashmir (AJK) Muzaffarabad and it is easy to use.

In this paper, a detailed literature review is presented in the next section. Later the material and methods used to complete all aspects of study along with hypothesis are discussed. Results are debated in detail before concluding the study in last section.

RESEARCH METHODOLOGY

In the last few years, the numbers of users of OSNs had widely proliferated because of the boom of IT and its availability to the common person. Nowadays, a huge number of internet users are using OSNs to communicate with their family and friends and share their photos, videos, and their thoughts[5].

Every OSN asks users to provide their e-mail id, address, D.O.B, etc to complete their profile. This information leads to create a threat state for that particular user whose personal information can be breached by unknown persons [6].It is observed in [7] that majority of the users in USA, Australia, Brazil, and Belgium were below the age 24, which shows youth is more inclined toward social interaction show careless behavior which causes them to fall in the risky state, so researchers are highly focused on youth to educate them [9].Elderly users are more aware of posting personal information details such as date of birth, friend list and school information on their social network accounts than younger users. Older internet users are more worried about the privacy of personal information than younger users. Some of the younger users publish their own information without the knowledge of the dangers that may occur from the misuse of their data.

The online environment may be dangerous for users, regardless of age, because of the possible leakage of personal information details[9],[10].For example; Facebook knows a huge amount about its users. A fully filled-out Facebook profile contains about 40 pieces of recognizable personal information, including name; birthday; political and religious views; online and offline contact information; gender, gender preference, and relationship status; favorite books, movies, educational and employment history and finally pictures. Facebook also offers multiple tools for users for finding out and adding potential contacts [11].

With the help of filled information by the user, a clear snapshot can be taken about user like who are you and whom you know. This information might be negatively used by others and can cause serious damages to one's life. This risk can be minimized if people read and understand policies and terms of privacy and security given by OSN sites[12],[13].Whether the information sharing policies are clearly stated, people still remain unaware due to their careless behavior. Even if they have read them willingly or unwillingly, they cannot understand how it affects their lives[14].It is being observed; users engaged themselves in danger due to their own non-seriousness[11].

Safeguarding personal information; privacy has become an essential issue among OSN providers and

online masses. The majority of the social network providers have created several techniques to limit the threats and risks to the users' privacy [15],[16]. These risks include the leak of personal information which may lead to illegal acts such as identity theft. The procedure of selecting privacy settings should also be straight-forward to offer users a clear idea of the data that will be shared with others [9],[17].

Privacy and security attacks are based on stakeholders of OSNs [18]. The stakeholders are both the users of OSNs and OSN itself. The users share a huge amount of their information leading from personal to their professional information [19]. This leads to the misuse of their information among others [20]. On the other hand, OSNs delivering services to the users handling their personal information and management of user activities in network are purely responsible for accurate functioning of their terms of services and also maintaining profitable business model [21],[22].

As with the large-scale OSNs, it is crucial to come up with an overview of trust relationship among users rather than simply knowing how much a user A trusts a user B. Statistical results of the social network status, such as average trust level and the structure of trust social network, to some extent indicates the quality of a social community [23]. If a large section of the accounts were distrusted entities (spam users for example), then content in the network might not be reliable or valuable and regular users would become inactive. So, there is a need for a trust assessment framework at a network level [24].

Connectivity through numerous applications of online social networks like Instagram, Facebook, WhatsApp, Twitter etc., has become the common platform of every Internet user to go through a public domain for staying connected, sharing their views, maintaining social relationships, and broadcasting user generated multimedia contents. Analysis of the traffic flow of applications is going to be very important because of the rapid growth of online social networks to comprehend the behavior of social network applications for the effects of latency and data rates considering the growing nature of actively connected users. Now a day's internet is available all over the world at affordable prices. Due to its low cost, the internet is acting as a catalyst for the ease of online social networks access [25].

Another important and interesting research challenge is to provide recommendation techniques for multimedia data in one or more social media environments [26]. While considering SNA (Social Network Analysis) perspective, there is a key role of multimedia data: understanding and representing user data (multimedia) interaction mechanisms and characteristics of multimedia items can be useful to check user behavior especially in designing human-centric (multimedia applications and services). Secret data transmission through public channels without drawing suspicion is called Steganography whereas disclosure of hidden communication by analyzing the media on public channels is called steganalysis. To minimize the distortion caused by modification on a cover object, the syndrome trellis coding (STC) has been designed to work with predefined embedding costs for all cover elements. The embedding costs are used to quantify the effects when modifying the cover elements [27].

The availability of huge amounts of data from Location-based social networks, such as Facebook, Foursquare and Gowalla is the factor of the increasing popularity of online event marketing [28]. An important and crucial issue is how to make use of the users' social behaviors analysis for online event marketing. Due to the increase in World Wide Web, community mining is also increasing in the equivalent pattern. A lot of research has been done for mining the unique communities of web pages. Byword community, means that the collection of objects share with common properties. Researchers worked on the detection of hidden activities and they have done a worthy analysis in this scenario [29]. They identified the problem in three steps:

1. Information flow through the network using the affected dataset
2. Noticing non-obvious connections between actors
3. Identification of nodes (directly or indirectly) connected to other nodes

Results showed that hidden activities can be mapped by using different data mining algorithms like regression. Their work identified a conceptual framework for detection and analyzing hidden groups and their activities.

Many researchers have raised their attention towards the accuracy of privacy studies [30-32]. They have raised their voices about privacy surveys, some researchers

purposely attempt to obscure their interest in privacy when running studies, and several others have pointed out the inconsistency between reported privacy concerns and user actions.

METHODOLOGY AND HYPOTHESIS

The underlying study has focused on Facebook because; it is most widely used all over the world and also in Azad Jammu and Kashmir (AJK), it is easier to use and is more interactive than other OSN's. The survey questionnaire was designed based on Facebook interface and terminologies. The questionnaire had 14 different variables related to demographic information, usage capacity and knowledge of users. The questionnaire includes both quantitative and qualitative data. Quantitative data includes age of respondents, number of friends, number of accepted unknown requests etc. While qualitative data includes user part of the information they share, knowledge of privacy, trust on OSN etc.

The sample was taken from total enrolled students in the University of Azad Jammu & Kashmir (AJ&K), Muzaffarabad Campus, using Thomas Yamane sample size calculation formula [33]. According to his formula, if the population size is known then there is no need of mean and standard deviation. According to him sample size can be calculated with Eq. (1).

$$n = \frac{N}{1 + N * (e)^2}$$

Where n is corrected sample size, N is total population size, and e represents margin of error or alpha level or confidence interval, for example, e = 0.05 with the Confidence Interval (CI) of 95%. In this study, total population N at the time of survey was 6414, alpha level e was set to 0.05, which makes sample size n=376.6 ~ 377.

The targeted respondents were educated audiences of the University of AJ&K. The questionnaire was distributed among students of different departments like, Computer Sciences & Information Technology, Economics, Statistics, Botany, Geology, Law, Zoology, Fine Arts, Mathematics, Chemistry, Physics etc. Gender wise division of respondents is presented in Table 1. They were divided into four categories according to their educational qualification i.e. BS, MS, MPhil and PhD as

shown in Table 2. Total of 600 samples were distributed among respondents in the university, out of which 418 were received filled properly and complete. In remaining 182 samples, some samples were not accurately filled, while others were never received back from respondents.

Table 1: Number of respondents based on gender

Gender	Number of respondents	
	Frequency	Percent
Male	218	52.15%
Female	200	47.85%
Total	418	100%

Table 2. Distribution of respondent according to qualification

Academic qualification	Number of respondents	
	Frequency	Percent
Bachelors	251	41.83%
Masters	119	19.83%
M.Phil.	28	4.67%
Ph.D.	20	3.33%
Total	418	100%

For this study, the hypotheses for analyzing the results are as follows:

1. Gender will affect the number of friends in User's profile.
2. Highly qualified people will have more social interactions.
3. Gender will affect the acceptance of unknown friend request.
4. People who use account frequently are more privacy conscious.
5. Education level will influence privacy knowledge.
6. The number of friends will have a positive impact on usage of account.
7. Old age people give least time to OSNs.

The quantitative data collected from the respondents was first entered in MS Access later it was exported to MS Excel for cleaning and checking missing values from the dataset. Finally, cleaned data was analyzed using SPSS version 14.0[34]. Initially, 50 samples were tested and analyzed to check the feasibility of the study. Based on its results and after making necessary changes, finally collected data was analyzed by using cross tabs,

frequencies and Chi-Square test [35]. Apart from that, frequency of few main questions is taken along with its graphs. The results are analyzed using descriptive analysis procedure. Chi-Square is the sum of the squared difference between observed (o_i) and the expected (e_i) data, divided by e_i (Eq. (2)). Furthermore 95% CI was calculated using Eq. (3). Variables whose Chi-Square value is 0.05 or less than 0.05 are significantly proving the feasibility. The hypotheses are proven with the help of Chi-Square.

$$\chi^2 = \sum_i^n (o_i - e_i)^2 / e_i \quad (2)$$

$$\hat{P} \pm 1.96 \sqrt{\hat{P}(1 - \hat{P})/n} \quad (3)$$

In this proposed study, numbers of constraints were faced during designing, testing, surveying and analyzing results. In designing phase, this has been observed that it is difficult to cover all aspects of privacy issues in a single questionnaire. So authors focused on main and critical points of the underlying system. The main objective of this study is to analyze and restrain the privacy concerns of the users among provided privacy policies.

RESEARCH FINDINGS AND ANALYSIS

In this study few hypothesis have been developed that actually prove the social behavior of the respondents based on their age, qualification, visited FB accounts, number of friends, privacy knowledge and trust on Facebook. Predefines hypothesis are tested and results are explained individually in this section so that a clear picture can be depicted.

Gender Wise Number of Friends in Profile

In OSN, people who have more number of friends in their friends list are consider to be more social as compare to others. Previous findings and observations showed that user giving more time to OSNs have more number of friends. Gender wise distribution shows that female users belonging from any area preferred to have a shorter friend list.

Here the hypothesis is approved by the Chi-Square value of 0.000 that is highly significant. This hypothesis can be concluded as gender has a dominant impact on number of friends in OSN user's profile. Fig. 1 shows that

female users prefer to have less number of friends than male users. Generally it is observed that male respondent pays least attention to their profile security. Results show that only 5.96 percent male respondents lie in category of 0-100 friends in their profile but the trend gradually increases as the category of friend's increase as 23.85 percent lies in category of 500-1000 and 18.35 percent lies in category of 1000 or above number of friends. Numbers strongly showed that male users prefers less restricted profile, so everyone from their friends or relatives can easily access them from inside and outside their friends graph.

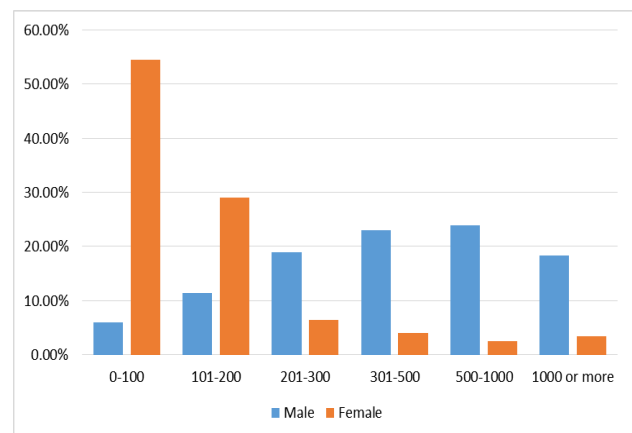


Figure 1. Gender wise number of friends in Facebook

In females, numbers of users decreases as the size of friends list increases. The reasons justify above statement because of their privacy consciousness 54.50 percent of female respondents lie in the category of 0-100 number of friends and only 3.50 percent lies in the category of 1000 or above number of friends from all over the data. This is because female users restrain themselves from being more social as compared to male. They prefer to be connected only with family and friends.

Highly Qualified People Will Have More Social Interactions

The findings indicate that high qualified users pay least time to their social networks, see Fig. 2. In contrast to hypothesis, practically it is observed that with the passage of time, age of user's increases and the daily routine work is also grown higher so they spend least time to their social networks.

Figure 2 clearly shows that bachelor's level users visit Facebook account more on daily basis then Masters,

M.Phil, and Ph.D. level users. 41.9 percent bachelors, 18.9 percent Masters, 5.5 percent M.Phil, and 3.8 percent PhDs visit account on daily basis. Observations of this study shows that with an increase in qualification level, the frequency of account visits is decreasing. We can say that the obtained results that account for visit frequency and qualification have a negative relationship. Bachelor's level users give more time to social networks like Facebook which is commonly used in Muzaffarabad AJ&K as compared to highly qualified users. As authors have seen an increase in the qualification of the user means they pay least time to social networks.

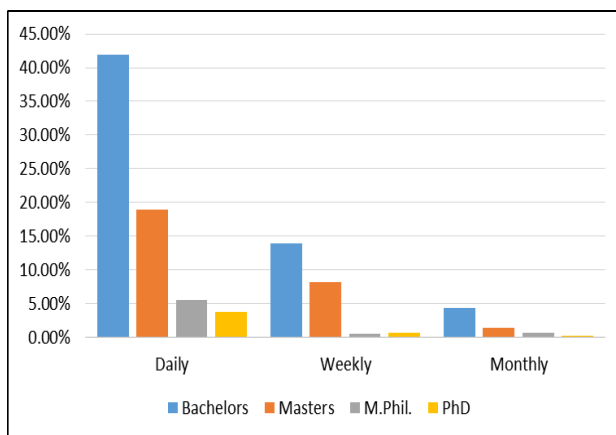


Figure 2. Academic qualification and frequency of accessing social network

Gender Will Affect The Acceptance of Unknown Friend Request

This hypothesis is designed to see the relationship between gender and acceptance of unknown friend requests, regardless of user age and qualification. Comparatively this has been observed that male kept their profile open and less restricted. So number of friends will be high because many people can send them request and they do not hesitate in accepting those requests. The first hypothesis also supports that male users have more numbers of friends in their friends list.

Table 3. shows that only 9 female respondents out of 200 accept unknown friend requests, therefore their friends list was shorter than male respondents. On the other side, male respondent also behaves in similar pattern but they are also more open to accept friend requests from unknown users.

Table 3. Gender Wise Acceptance of Unknown Friend Request			
Gender	Accept Unknown request		
	Yes	No	Total
Male	53	165	218
	24.30%	75.70%	100%
Female	9	191	200
	4.50%	95.50%	100%

People Who Use Account Frequently are More Privacy Conscious

This hypothesis explains that those users who use Facebook regularly probably are more conscious or very keen about privacy on their timeline. Privacy generally refers to the security of the profile. If a user gives more time to Facebook or OSNs, probably he or she will have more knowledge about the privacy terms and conditions that are given by Facebook management. Generally, if they spend 2 hours per day, on average, to their profile then they will make their profile very secure by getting updates from the friends available in his or her friend list.

Fig. 3 shows the relationship between time to social network and profile security. It refers to those respondents who think about the security of their profile. A user gives his/her response in Yes or No and time to social network was scaled as daily weekly and monthly. It shows that 51% of the respondents who are using their profile daily think that their profile is not secure as per their expectations.

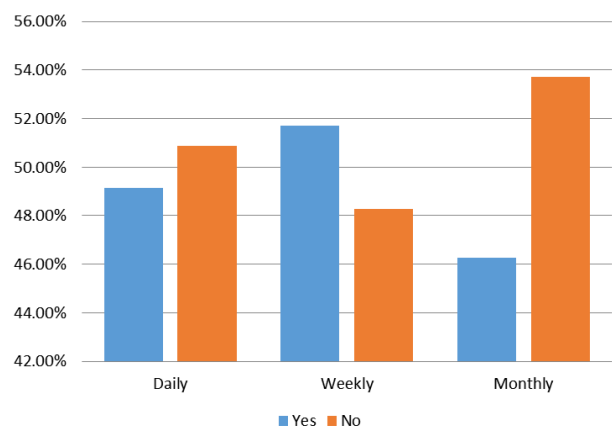


Figure 3. Relationship between time to social network and profile security

Similarly, weekly basis users consider their profiles

are more secure under the available conditions. Lastly, monthly users consider their profiles are not secure but overall statistics shows that 50.5 percent users feel insecure on Facebook under the given conditions provided by Facebook. But 49.5 percent users think that they are secure under given conditions. So the mathematical difference is only 1 percent in values which can be ignored in general analysis.

Education Level Will Influence Privacy Knowledge

In this hypothesis the knowledge of the respondent about privacy settings provided by Facebook is analyzed. Privacy knowledge covers privacy terms and condition provided by Facebook which the user has to accept before making his or her profile on Facebook.

Results show that bachelor level users have more knowledge as compared to other qualification levels. Results show that 7.4 percent lies at high category of knowledge in bachelor level whereas from Ph.D. level only 0.2 percent people lie in category of high knowledge. It is also perceived that increase in qualification caused decrease in the concern of the respondent's about privacy terms and conditions provided by Facebook.

The knowledge of respondent's was obtained by taking the sum of the scores with options provided to user as a query of privacy knowledge. Later knowledge bands were developed by dividing scores into three categories: low, medium and high in SPSS. Bachelors level respondents, who are ranked on low level in qualification, but they spend more time than highly qualified people, so this can be concluded that professional qualification doesn't matter in order to maximize privacy knowledge. It may acts as little provision but a user may be ranked at high level only if he or she spends more time at Facebook.

This research developed the hypothesis that high qualified people have more knowledge about privacy of the Facebook, but the statistics show different results. As shown in Fig. 4 education level has no effect on the privacy knowledge of users. So from the above findings, we will reject null hypothesis and accept alternative hypothesis that is high qualification can't influence privacy knowledge of the respondent.

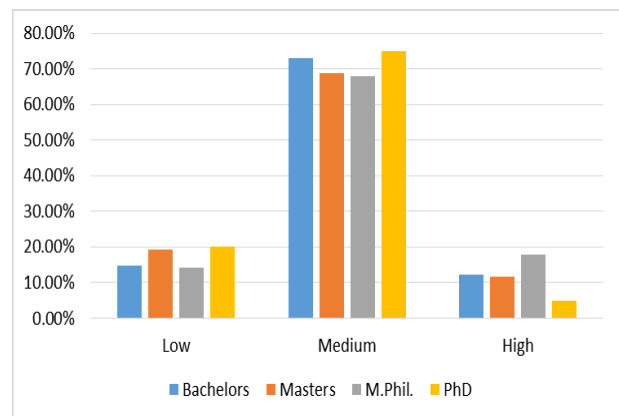


Figure 4. Academic qualification and privacy knowledge of respondent

Number of Friends Will Have Positive Impact on Usage of Account

The hypothesis states that OSN users with more number of friends on his/her social network account may give more time to his or her profile. As the number of friends increases, the usage of account will also increase because user's social network expands with more number of friends. This theory was tested under this hypothesis to satisfy the results. There is a positive relation between social interaction and account usage.

Results show that respondents who generally spend more time to Facebook have more friends, the analysis shows that 12.2 percent out of 70 percent users who used accounts on daily basis have more number of friends compare to those who used Facebook for limited time i.e. monthly. These results clearly satisfy our hypothesis that if a user spend more time at Facebook then he or she will have more social interaction with people and their number of friends will be high. Thus we accepted our null hypothesis, that is, more time to social networks will raise the numbers of friends in someone's profile.

Number of friends is taken along X-axis and number of respondents along Y-axis in Fig. 5. Lines show that if user spends more time at Facebook he or she will have more friends in any provided category from 0-100 to 1000 and above. It can be clearly seen that as the number of friends' increases, more users use OSN on daily basis. 500-1000 category line in the graph proves this hypothesis.

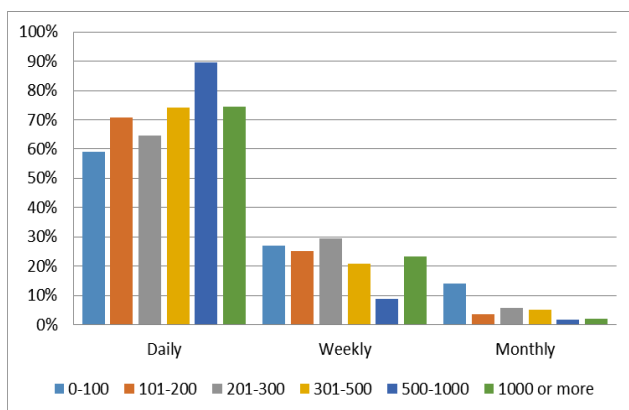


Figure 5. Time to social network with number of friends on Facebook

Old Age People Give Least Time To OSNs

This hypothesis examines the relationship between people of different age groups and their times spend on Facebook. It is observed that the respondents who are in young age groups give more time to social networks i.e. Facebook, twitter, Instagram, etc. There is also a positive relationship between age of the respondent and their time to social network. Fig. 6 shows age bands from 17-25, 26-35 and 36-45 and above in SPSS. Authors found that approximately 62 percent of respondents using their account on daily basis and they all lies in lowest age groups which indicates the youth lies in 17-25 age group excessively using Facebook account. However on daily basis usage of old age people as compared to youth age groups, begins from 36-45 are approximately 2 percent users out of 70 percent. This clearly defines that old age people pays least attentions towards social network i.e. Facebook. Fig. 6 clearly reflects our hypothesis that old age people pay least time to Facebook.

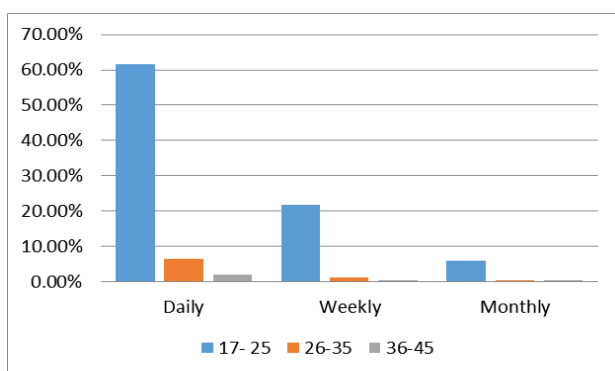


Figure 6. Time to social network with respect to age groups

Chi-Square Table of Hypothesis

We have Chi-Square values to test our hypothesis and declare them as either accepted or rejected. Table 4 shows the Chi-Square values for that all the hypothesis. Hypothesis whose Chi-Square value is less than 0.05 are accepted while hypothesis whose Chi-Square value is greater than 0.05 are rejected and alternate hypothesis will be accepted.

Table 4. Pearson Chi-Square values with respect to hypothesis

Hypothesis	Pearson Chi Square value	Decision
Gender wise number of friends in profile	0.00	Accepted
Highly qualified people will have more social interactions	0.24	Rejected
Gender will affect the acceptance of unknown friend request	0.00	Accepted
People who use account frequently are more privacy conscious	0.87	Rejected
Education level will influence privacy knowledge	0.79	Rejected
Number of friends will have positive impact on usage of account	0.00	Accepted
Old age people give least time to OSNs	0.58	Rejected

Area Based Comparisons

In this study, all the hypothesis were also tested to check the impact of area of residence of respondents. In this proposed study, area was divided into three categories as: Advance (Islamabad), Developing (Muzaffarabad) and underdeveloped (Hattian Balla) based on availability of Internet and easy access to OSN. Area wise sample were distributed to check different levels of privacy among different area residents and also the impact of technology. In area wise distribution, knowledge of respondents in terms of privacy was also observed as a key concern.

In this study, Muzaffarabad was chosen as main city in which actual survey was taken. For this comparison purpose 418 samples were taken from Muzaffarabad, 50 samples from Quaid-e-Azam University Islamabad and 50

from Hattian Balla (Rural) Campus of UAJK. Table 5 summarizes the outcome in percentage format. Hattiaian Campus only has bachelor level education available with a very less female population. The hypothesis based results of area wise comparison are

- There is a clear difference between male and females number of friends regardless of their area of residence.
- Qualification has a positive impact on social interactions without having area wise any impact. The usage of social network of different qualification levels is almost equal in all three areas.
- Females in all these areas do not accept anonymous friend's request, thus supporting our claim that gender effects acceptance of unknown friend request.
- People don't trust on social network either they are from developed, developing or under developed areas
- Maximum users from all three area's have medium level of privacy knowledge.
- People use their account on daily basis having lots of number of friends regardless of their area of residence.
- Interestingly, this is observed people from Hattian and Islamabad, users with age group ranging from 25 to 45 give least time to social networks

Table 5. Area based summary in percentages				
Area based summary in %ages				
		Muzaffar-abad	Hattian	Islam-abad
Gender	Male	53	78	34
	Female	47	22	66
Age	17- 25	89.5	98	80
	26-35	8.1	0	20
	36-45	2.4	2	0
Academic Qualifi- cation	Bachelors	60.0	96	26
	Masters	28.5	4	34
	M.Phil.	6.7	0	40
	PhD	4.8	0	0
No. of Friends on Facebook	0-100	29.2	22	48
	101-200	19.9	18	18
	201-300	12.2	14	16
	301-500	13.9	14	16
	500-1000	13.6	16	0
	1000 or	11.2	16	2

	more			
Visit Account	Daily	70.1	44	70
	Weekly	23.2	48	22
	Monthly	6.7	8	8
Accept Friends Request	Yes	14.8	36	32
	No	85.2	64	66
Change Privacy Setting	never	25.6	40	18
	Rarely	63.2	58	78
	Regularly	11.2	2	4
Profile Secure	Yes	49.5	40	46
	No	50.5	60	54
Information Shared on Facebook	Basic Information	47.1	42	30
	Personal Information	9.8	94	6
	Contact Information	11.2	94	14
	Education & work	32.1	70	32
	Family & Relationship	5.0	0	2
	Life Events	20.3	84	10

CONCLUSION AND FUTURE WORK

The purpose of this study was to examine the relationship between privacy in OSN with respect to academic qualification, gender, and age of the respondents. Privacy index was developed with the help of six important variables such as control tagging, control posts on your timeline, control who can find you from on and off the Facebook and how to lemmatize friends request. The descriptive analysis along with cross tabs showed that privacy is most sensitive variable these days.

This study examined that highly qualified users have less privacy knowledge compared to bachelor level users, apart from that it is also observed that users spending more time to Facebook have more privacy knowledge. It also finds that as age increases user pay least time to OSNs. Gender is also very important variable which showed that female users prefer to have restricted profile, accepted least number of friend's request and allows new requests senders in their friends list after proper authentication.

The users other than IT related academic background have moderate knowledge, which showed

that related subject have positive impact on the users privacy taste. This research clearly demonstrated that privacy is a big issue in social networks especially in Facebook. Previous literature showed that people are taking keen interest in using OSNs such as Facebook, twitter, LinkedIn, WhatsApp etc. But the security of user's profile is also a very important issue. Literature described that the users themselves feel insecure on OSNs while being online or offline.

It is very important for a user to read and understand the privacy policies illustrated by OSNs in their own language before creating their profiles. This will help them to be more aware about the privacy. From the study, it is also observed that many users have knowledge about privacy and its issues but they don't apply proper limitations to their profiles. This careless behavior causes them to fall in danger in future. The study also clearly demonstrated that females are more sensitive about their privacy.

In this proposed study, there also have been applied different machine learning classifiers in order to find some new directions and make this research more qualitative. The goal of machine learning classifiers was to predict the privacy level of OSNs among the students of university of AJ&K based on the gender, qualification and region. But due to certain limitations, the desired results cannot be obtained. This could be a valuable research in future. There can be applied advance techniques like regression, feature selection, prediction methods etc to obtain favorable results. These techniques will be helpful in predicting awareness and increase level of privacy knowledge of users of certain regions about OSNs.

REFERENCES

1. Q. Ni, E. Bertino, J. Lobo, C. Brodie, C.M. Karat, J. Karat, and A. Trombeta, "Privacy-aware role-based access control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 3, pp. 24, 2010, DOI. 10.1145/1805974.1805980.
2. R. Carthy, "Will IRSeeK have a chilling effect on IRC chat?," Available online: <http://techcrunch.com/2007/11/30/will-irseek-have-a-chilling-effect-on-irc-chat/>, (accessed March 01, 2018).
3. Singh, and A. Singh, "Review of cyber threats in social networking websites," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, 2017.
4. Bunnig, and C.H. Cap, "Ad hoc privacy management in ubiquitous computing environments," in *Proc. Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services*, 2009, pp. 20-25.
5. Sailunaz, K, & Alhajj, R. "Emotion and sentiment analysis from Twitter text". *Journal of Computational Science*, 36, 101003, 2019.
6. W. Binden, M. Jormae, Z. Zain, and J. Ibrahim, "Employing information security awareness to minimize over-exposure of average internet user on social networks," *International Journal of Scientific and Research Publications*, vol. 4, no. 1, pp. 1-6, 2014.
7. Vanderhoven, Ellen and Schellens, Tammy and Valcke, Martin, "Educating teens about the risks on social network sites. An intervention study in secondary education = Enseñar a los adolescentes los riesgos de las redes sociales: Una propuesta de intervención en Secundaria," *Comunicar*, vol. 22, no. 43, pp. 123-132, 2014, DOI. <http://dx.doi.org/10.3916/C43-2014-12>.
8. Błachnio, A, & Przepiorka, A. "Be aware! If you start using Facebook problematically you will feel lonely: Phubbing, loneliness, self-esteem, and Facebook intrusion. A cross-sectional study". *Social Science Computer Review*, 37(2), 270-278, 2019.
9. N. Aldhafferi, C. Watson, and A.S.M. Sanjeev, "Personal information privacy settings of online social networks and their suitability for mobile internet devices," *International Journal of Security, Privacy and Trust Management (IJSPTM)*, vol. 2, no. 2, 2013.
10. Pensa, Ruggero G., Gianpiero Di Blasi, and Livio Bioglio. "Network-aware privacy risk estimation in online social networks." *Social Network Analysis and Mining* 9, no. 1 (2019): 15.
11. Z. Asif, and M. Khan, "Users' perceptions on facebook's privacy policies," *ARPN Journal of Systems and Software*, vol. 2, no. 3, pp. 119-121, 2012.
12. M. Chewae, S. Hayikader, M.H. Hasan, and J. Ibrahim, "How much privacy we still have on social network?," *International Journal of Scientific and Research Publications*, vol. 5, no. 1, 2015.
13. Zheng, Xu, Zhipeng Cai, Guangchun Luo, Ling Tian, and Xiao Bai. "Privacy-preserved community discovery in online social networks." *Future Generation Computer Systems* 93: 1002-1009, 2019.
14. Srivastava, and G. Geethakumari, "Measuring privacy leaks in online social networks," in *Proc. IEEE Advances in Computing, Communications and Informatics*, 2013, pp. 2095-2100.
15. Sahoo, S. R, & Gupta, B. B. "Classification of various attacks and their defence mechanism in online social networks: a survey". *Enterprise Information Systems*, 13(6), 832-864, 2019.
16. Wenninger, H., Krasnova, H., & Buxmann, P. "Understanding the role of social networking sites in the subjective well-being of users: a diary study". *European Journal of Information Systems*, 28(2), 126-148, 2019.
17. Y. Liu, K.P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: user expectations vs. reality," in *Proc. ACM SIGCOMM conference on Internet measurement*, 2011, pp. 61-70.

18. Imrul Kayes, Adriana Iamnitchi, A survey on privacy and security in online social networks. *Online Social Networks and Media Journal*, arXiv:1504.03342 [cs.SI], 2017.
19. Sun, Zewei, Huaizhen Kou, and Wanli Huang. "Privacy-aware friend finding in social network based on thumbs-up data." *EURASIP Journal on Wireless Communications and Networking* 2019, no. 1 (2019): 211.
20. Cheng, Shulin, Bofeng Zhang, Guobing Zou, Mingqing Huang, and Zhu Zhang. "Friend recommendation in social networks based on multi-source information fusion." *International Journal of Machine Learning and Cybernetics* 10, no. 5 (2019): 1003-1024.
21. Bastos, Marco T., and Dan Mercea. "The Brexit botnet and user-generated hyperpartisan news." *Social Science Computer Review* 37, no. 1 (2019): 38-54.
22. Günneç, D., Raghavan, S., & Zhang, R. "Least-Cost Influence Maximization on Social Networks". *INFORMS Journal on Computing*, 2019.
23. K. Zhao, and L. Pan, "A machine learning based trust evaluation framework for online social networks," in *Proc. IEEE Trust, Security and Privacy in Computing and Communications*, 2014, DOI. 978-1-4799-6513-7/14.
24. Wu, Youke, Haiyang Huang, Ningyun Wu, Yue Wang, Md Zakirul Alam Bhuiyan, and Tian Wang. "An incentive-based protection and recovery strategy for secure big data in social networks." *Information Sciences* 508 (2020): 79-91.
25. D. Prakash, and S. Surendran, "detection and analysis of hidden activities in social networks," *International Journal of Computer Applications*, vol. 77, no. 16, 2013.
26. Baydeti, N., Veilumuthu, R., & Vaithilingam, M. (2019). Scalable Models for Redundant Data Flow Analysis in Online Social Networks. *Wireless Personal Communications*, 107(4), 2123-2142.
27. Amato, F., Moscato, V., Picariello, A., & Piccialli, F. (2019). SOS: A multimedia recommender System for Online Social networks. *Future generation computer systems*, 93, 914-923.
28. Hu, Yinghong, Zichi Wang, and Xinpeng Zhang. "Steganography in Social Networks Based on Behavioral Correlation." *IETE Technical Review* (2020): 1-7.
29. Liu, Yuxin, Anfeng Liu, Xiao Liu, and Xiaodi Huang. "A statistical approach to participant selection in location-based social networks for offline event marketing." *Information Sciences* 480 (2019): 90-108.
30. M. Siddula, L. Li, Y. Li, "An empirical study on the privacy preservation of online social networks," *IEEE Access*, vol. 6, pp. 19912-19922, 2018.
31. K. Wong, A. Wong, A. Yeung, W. Fan, S.K. Tang, "Trust and privacy exploitation in online social networks," *IT Professional*, vol. 16, no. 5, 2014.
32. Z. He, Z. Cai, J. Yu, "Latent-data privacy preserving with customized data utility for social network data," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 1, pp. 665-673, 2018.
33. Thomas Yamane, "Formula to determine the sample size," Available online: <https://www.quora.com/What-is-Yamane-sample-calculation> (accessed May 22, 2018).
34. Marcus Hearne, "SPSS 14.0 brief guide," the University of Virginia, Available online: <http://www.tau.ac.il/cc/docs/spss14manuals/SPSS%20Brief%20Guide%2014.0.pdf> (accessed May 22, 2018).
35. E.W. Weisstein, "Chi-Squared test. From MathWorld--A wolfram web resource," Available online: <http://mathworld.wolfram.com/Chi-SquaredTest.html> (accessed May 22, 2018).