Research Article

International Journal of Advanced Computer Research, Vol 10(50)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.2020.1048094

Awareness of data privacy on social networks by students at Qassim University

Abdullah Alabdulatif* **and Fahad Alturise**
Assistant Professor, Computer Department, College of Sciences and Arts, Qassim University, Al-Rass, Saudi Arabia

Received: 29-June-2020; Revised: 05-September-2020; Accepted: 08-September-2020

Abstract
In the socialization paradigm, digitalization is the primary function. Social Networking Sites (SNS) are a means of achieving advanced communication. For the last few decades, SNS have become the most widely used media of socialization and connectivity between people. SNS utilize personal information sharing, which raises privacy concerns in users due to the sensitive, confidential data which is necessarily gathered. This paper investigates awareness regarding the information privacy of students of Qassim University who use SNS. The research comprises a survey exploration to study how the students of Qassim University interact with SNS in terms of privacy. The literature review explores the theoretical privacy concerns with respect to SNS, including measuring awareness of privacy settings for their accounts in SNS. Also covered is student reaction to privacy violations. Data were collected using a questionnaire which sampled 913 respondents, who were selected from various levels and departments using random sampling methods. The analysis revealed that the majority of the users in every SNS are concerned about their privacy and personal information, and 69.4% contacted the government about privacy violations. This paper aims to investigate awareness regarding information privacy in the students of Qassim University using SNS.

Keywords
Social networking sites, Qassim university, Privacy, Privacy settings, Privacy violations.

1.Introduction
Around the world, people are interconnected with each other through SNS. Billions of the world's populations benefit from instant communication using simple and quick social media applications through safe and reliable profiles [1]. SNS allow users to form a profile of their choice, i.e. fully or semi-accessible by other users within a restricted framework [2]. Social media and SNS, like Facebook, have records of confidential and personal information, including birthdates, e-mails, phone numbers, political outlooks, physical addresses, and photographs. Moreover, pictures can be of significant events, ceremonies, or occasions.

The overall biography inside a user's profile holds detailed, private information on social media, which could adversely affect individuals if it was compromised.

Some of the negative social media uses include limiting employment opportunities [3,4] identity theft, and fraudulent actions [5].

Regarding online confidentiality, three different types of information privacy are distinguished [6], namely (i) informational privacy (ii) social privacy and (iii) personal privacy. Based on recent studies, the second type, social privacy, is mainly focused on social media profile privacy settings, which play a vital role in facilitating the mechanism of social media connectivity.

During early 2020, online social networks grew very quickly, which directly impacted their usage within Saudi Arabia. Out of the 33 million population of Saudi Arabia, by June 2020, more than 18 million are active Twitter users, and 20 million are active Facebook and Instagram users [7]. It can be clearly seen on social media that all active users, not only from Saudi Arabia but from the rest of the world, are also regularly posting and sharing detailed personal, confidential information that gives rise to serious online privacy issues [8].

*Author for correspondence

The lack of empirical research which is theory-driven regarding the importance of social media privacy in the Middle East makes this present study valuable to both academic and industrial communities for awareness purposes [9]. Detailed studies aim to identify and assess various security awareness about social networks [8].

In this study, the main aim is to investigate awareness regarding information privacy using SNS in the students of Qassim University. The primary objectives include (i) Identify the privacy functions of SNS and the related concerns about them (ii) explore motivations to reveal the data on SNS and be aware of personal privacy data (3) determine the awareness of information privacy during the use of SNS by the students of Qassim University.

2.Literature review

In this fast-growing world, SNS engage users to communicate, in the virtual community, with other network users. SNS users connect with other users through sharing and posting personal information. Despite the personal information involved, new videos and images are shared in an instant. This sharing can be performed in-profile as well as in real-time conversations using chat functionalities [10]. In this scenario, each user has the ability to create online friends in the matching network and to share common interests or collaborations. Note that all SNS are associated with a major goal to make its nomenclature different than other sites, and they vary depending on the site [11]. The SNS networks give access and the freedom to users to openly communicate with new contacts in the network, but also to reach out to people from their offline group of friends.

Interaction among users has been significantly impacted by the advanced, ongoing development of information and communication technologies. This phenomenon is dominant, particularly in the case of people who use mobile devices for communication purposes. Since it is not clear to mobile web users where their personal information is stored, and who can use it, it is important to protect mobile web user data and brief users on data privacy. Confidentiality in these paradigms has become a real challenge.

In early 2019, SNS networks grew in Saudi Arabia, where, out of 33 million people, around 18 million are Twitter users, 20 million are Facebook users, and the remaining five million use Instagram, Snap chat, etc. [7]. It can be clearly seen, in social media, that all active users, not only from Saudi Arabia but also from the rest of the world, continually post and share detailed personal, confidential information. This sharing gives rise to serious online privacy issues in three different categories, namely privacy, social privacy, and personal privacy. Details mainly focusing on social media privacy settings [12], and the surrounding concerns, are discussed in the following sections. Literature regarding privacy shows that sharing the personal data of customers relies upon data sensitivity, whereas the willingness to share it is associated with individual inherent risk.

2.1Privacy

Different authors and researchers define confidentiality differently. The author [13] defined privacy as the protection of personal information from misuse by others, and the allowance of only certain authorized entities to access personal information. The author [14] described privacy as a set of policies that force systems to protect private information. Privacy also applies to user location and other details relating to the user [15]. Based on various studies with wide-ranging aspects, the concept of privacy is found to be diverse, having no single definition which incorporates all aspects.

2.2Privacy concerns

In this digital age, personal information has been found to be the most critical form of retained data. There are also moral issues around privacy, like psychological, philosophical, lawful subjects, and sociological subjects. From a broad-ranging view, privacy purpose is also contemplated in the view of various perspectives [16]. In SNS, privacy is considered a subset of data privacy. For active social media users, privacy is psychological based on protecting their personal, confidential data against offline scams. Various researches show a range of perspectives in the information technology (IT) domain based on two functions. The first is explained as privacy is explained as the ‘claim of individuals, groups, or institutions to define for themselves when, where, how, and to what degree of personal information about the user is shared with third parties [17]. The second is explained as “the product-based aspect regarding the monetary use of an individual’s data for exchange and commercialization. In this process, third parties are always ready to analyse, gather, and vend individual user information [18].

Privacy management is most widely considered to be the control of self-revelation of individual as well as private data. In the self-revelation process, an

individual is willing to share their personal data with other people [19]. The level to which the data is exposed by each user to others is identified through privacy management. In this process, the two basic elements of sharing data are (i) willingness to share data and (ii) user awareness [20]. Data classification characterizes the degree to which users are willing to share their information, whereas the sensitivity of data is considered to be the usage of personal information for commercial purposes [21]. Literature regarding privacy shows that sharing a customer's personal data relies upon data sensitivity, whereas the willingness to share it is associated with inherent individual risk [17].

2.3Motivation to reveal data on SNS

In SNS the size of the website is a critical element that specifies contact lists as well as users. It is user eagerness that motivates users to share their information with their online list of contacts. Each user procures the network to reinforce their feelings based on the reactions of an enlarged SNS network size [17]. The data holder uses certain settings to constrain the sharing of personal details [22].

2.4Awareness of personal privacy data

While registering on a SNS, personal information is required as input, which creates worry in almost every user. Different studies have indicated the strong concerns of users regarding privacy [23] [8]. In the base of communication experience, awareness is defined as new concept acknowledgment and its transformation [24]. Some people are looking for news and exposure in a communication network chain for trending to present their thoughts on different aspects [25]. For social recognition, while visiting social networks, individual awareness can move users toward various applications and exercises. The person forms a bridge between their past and future plans in comparative circumstances [26].

SNS are considered to be responsible for managing user's data security, and whenever the user feels unsafe regarding their respective data, after knowing it has been manhandled, the user becomes dissatisfied with its commitments. Detailed extensive examinations and findings reveal that individuals have experienced privacy invasion [17]. For this purpose, almost all SNS have high levels of flexibility in their privacy settings; however, it is never an exact science. Privacy flexibility is offered to protect one's profile from friends, the public, and semi-friends or acquaintances. In some cases, settings provide further options within each topic, which offer checkboxes for various options to expose or disclose data to certain people or groups of people.

2.5Privacy and financial incentives

Incentive measurements are regularly implemented by SNS to provide individual user data. In the case of shopping coupons and transactions, clients are drawn in and encouraged to reveal information [27]. The enforcement element is a minor advantage that can be viewed where SNS collect all private data to facilitate users' privacy. According to growing user enthusiasm, financial incentives improve user-perceived behaviour in sharing personal information [28]. In this regard, SNS developers maintain a constant code of conduct based on proclamations issued regarding data collection, data storage, and essential user routes to understand the policy and develop trust [29]. Only SNS networks with transparent security approaches are trusted, as opposed to those which don't focus on security. Users are eager to provide data to sites with adequate defensive measures. User concerns and confidence regarding privacy and information can be improved by explicit privacy management and privacy policies in which the user is urged to share data [30].

User personal information can be exploited to the extent as prescribed in privacy policies based on legal notices. This information includes name, marital status, address, date of birth, financial records, contact information, credit card information, and medical history, etc. Generally, all privacy policies thoroughly explain comprehensive related information regarding how much and how user information will be used. Furthermore, they provide disclosure around how the data are collected, stored, and tracked. It explains the rule which users need to know about the data uses by the website. In recent years, people often use SNS as anonymous and unethical users to ensure data security and confidentiality. Therefore, the privacy policy is vital to such websites [31].

3.Methodology

This study aims to investigate awareness regarding information privacy by students of Qassim University who use SNS based on research questions responded to in a survey. Previous studies show that questionnaire-based survey studies on information privacy are indicated to be the most useful method of data collection. Some studies include free format questions [32], and selective interviews [33], to get additional data. A few questionnaires have been on

paper, but most were web-based [1] [34] [17]. For this study, web-based was chosen because most, if not all, study respondents can manage an online questionnaire.

The questionnaire was developed based on closed-ended questions utilizing some available questionnaires, which underpinned the development. The resulting questionnaire has been reviewed by professional colleagues in the computer field for confirmation and effectiveness. Furthermore, a statistical consultant and English and Arabic language experts were also involved to ensure clarity, proper language structure, and the elimination of language ambiguities. Overall, the pilot test was performed on seven participants, which resulted in minor modifications.

In this survey, two different sets of questionnaires were set where *Table 1* responded to demographic information, and *Table 2* attended to various matters of information regarding privacy. The primary goal was to question respondents' perspectives about privacy and confidentiality matters on Social Networks such as privacy setting, privacy controls, and included general, personal viewpoints about privacy awareness. The overall questionnaire questions were selected based on four different groups, namely (i) Questions 1-4 in *Table 2* gather general information related to social networks and daily time spend (ii) Questions 5-7 investigate user attitudes and the way information is used for disclosure and data privacy control (iii) Questions 8-10 determine user awareness and understanding of the privacy policies and terms of use of Social Networks.

The survey participants had access to ten discreet questions and four demographic queries. All participants were guided to select one or more answer(s) based on the type of query within a set frame of answers.

3.1Results of data collection

Data were collected by sharing a link with students of Qassim university in various colleges in the Kingdom of Saudi Arabia. All the participants were provided with information sheets and Arabic language questionnaires. This survey link was active for seven days. In this survey, a total of 933 respondents participated from whom responses were gathered and later used for analysis.

3.2Demographic characteristics

Out of the 913 respondents, 398 (43.6%) were from arts and humanities colleges, and 453 (49.6%) were from science colleges, with just 62 (6.9%) from medical science colleges. For gender, 289 (31.7%) were male, and 624 (68.3%) were female. Most study undergraduate degrees 794 (87%), and 64 (7.1%) are in the foundation program at university, with 55 (6%) in postgraduate degrees. Age-wise, 779 (85.3%) were between 18 and 24 years old, and 107 (11.7%) were between 25 and 29 years old. Just 27 (3%) were over 30 years old. *Table 1* presents the summary of demographic profile of the respondents, while Table 2 shows the survey questions response.

Table 1 Demographic profile of respondents

Variables	Answers	Responses	
		Frequency	**Percent**
Age	18-24	779	85.3%
	25-29	107	11.7%
	More than 30	27	3%
Gender	Male	289	31.7%
	Female	624	68.3%
Education levels	Foundation	64	7.1%
	Undergraduate	794	87%
	Postgraduate	55	6%
Field of study	Arts and Humanities	398	43.6%
	Sciences	453	49.6%
	Medical sciences	62	6.9%

Table 2 Questions and answers in the survey

Survey questions	Answer options
1. What social network(s) do respondents use?	Facebook, Twitter, Instagram, Snapchat, WhatsApp, other
2. How long have respondents used social media?	< 1 year, 1 - 2 years, 3 - 4 years, > 4 years
3. How did most respondents access Social media?	Smartphone, laptop, tablet, desktop
4. On average, how many hours per day is spent on social network(s)?	< 1 hour, 1 - 2 hours, 3 - 4 hours, > 4 hours
5. Why do respondents use social media?	Mix with friends, meet new people with similar hobbies, express my opinion or share my knowledge, I use different social media platforms for different purposes, not sure.
6. How often does the respondent post, share, or comment publicly on own and/or other SN pages?	Never, occasionally, sometimes, often, frequently.
7. Which of the following privacy control mechanisms is the respondent currently using?	Control how others can find me, block spam, control who can message, restrict visibility of my profile, restrict photo tagging, set alarm if unknown login occurs, I don't use any mechanism.
8. When joining a social network, which answer best describes the respondent?	Never read the terms of service but agreed to join, only sometimes read the terms yet still agree to join, always read the terms still agree to join, always read the terms and do not join if disagree
9. Regarding social network privacy policies, which answer best describes the respondent?	Not aware; don't read and can't find them, aware but never read them, aware; sometimes read them but have no concern with privacy, aware; read, and take info. privacy seriously and act adequately.
10. If others try to uncover the respondent's private information from the user's social network pages, how difficult would be?	Very difficult, somewhat difficult, not too difficult, not at all difficult.

3.3Information about social networks

The results showed that WhatsApp was the dominant SNS used with a response rate of 89% (813). Facebook, which is now an old SNS, had the lowest percentage of users at 3.9% (36). Snapchat is the newest social network between the other four networks, with a response rate of 74.8% (683). 77% (703) of respondents use Twitter. 62% (566) of students use Instagram. Finally, about 6.5% (59) of participants use other social media. Table 3 represents the findings and the rankings of the SNSs by the survey participants.

The analysis displayed in *Figure 1* shows that 86.9% of the respondents have used social media from more than four years, 10% have used it for between three and four years, 1.6% have used it from one to two years, whereas 1.3% has used it for less than a year. All the students use social media through different devices.

Table 4 illustrates that 99% of the users use smartphones, 28.9% are using laptops, 12.4% use tablets, and only 5.1% are using a desktop for social media.

Figure 2 shows daily usages are 43.5% of the students spend more than four hours on social media, 36.5% use it for three to four hours, 14.5% spend over one to two hours on it, and 5.5% spend less than an hour on social media.

In addition, *Table 5* confirms that 77.5% of the students spend time on social media to connect with friends, 28.3% try to connect with new people, 54.9% use it for multiple purposes, whereas 35.9% use it for sharing and expressing their personal views with other people.

Furthermore, *Figure 3* illustrates that more than 300 people sometimes share their opinion with the public, while about 300 rarely share on social media.

Table 3 Chosen social media by respondents

Social media	Frequency	Percent
Facebook	36	3.9%
Twitter	703	77%
Instagram	566	62%
Snapchat	683	74.8%
WhatsApp	813	89%
Other	59	6.5%

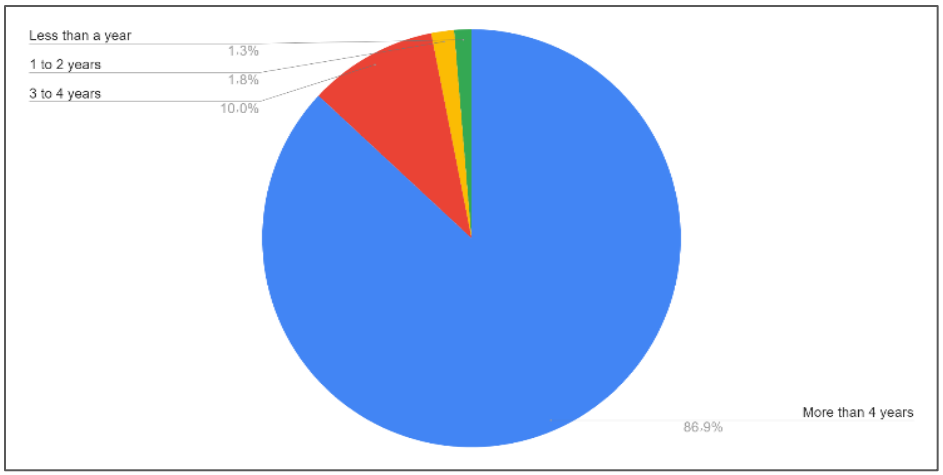

Figure 1 For how long have you been using social media?

Table 4 By what means do you access social media?

Device type	Frequency	Percent
Smartphone	904	99%
Laptop	264	28.9%
Tablet	113	12.4%
Desktop	47	5.1%

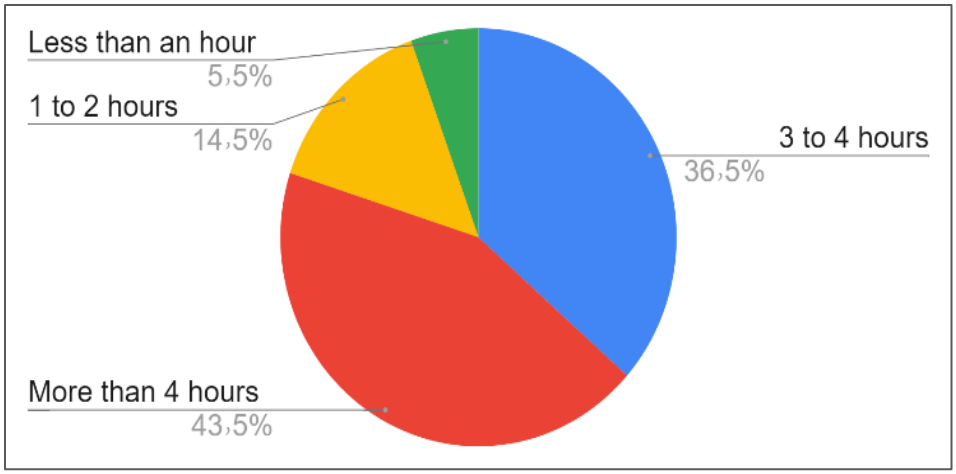

Figure 2 How many hours of social media per day?

Table 5 The goals of using social media

Social media	Frequency	Percent
To connect with friends	708	77.5%
To connect with new people who have similar interests	258	28.3%
I use different social media platforms for different purposes	501	54.9%
To express my opinion or share my knowledge on a topic	328	35.9%
Not sure	71	7.8%

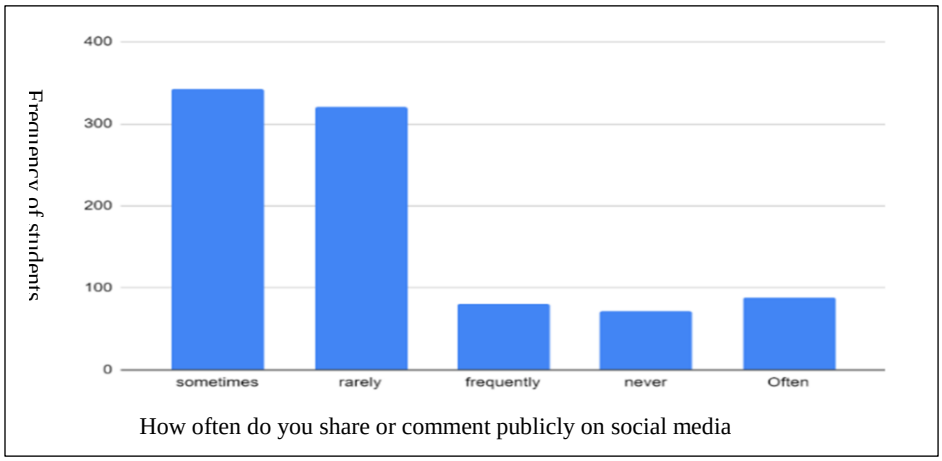

Figure 3 How often do you share or comment publicly on social media?

Regarding privacy, *Figure 4* illustrates that 88.1% are concerned about their privacy, and sharing depends on what they themselves set, whereas 1.5% use the default settings, 3.3% ask a technical person to help, and 7.1% rely on friends and family members.

Details of the control over personal information, sharing of photos, tagging and spam messages are shown in *Table 6*, where 44.1% have control over searching, and 34.1% of users avoid spam messages, 36.5% control inbox messaging, 39.9% restrict profile viewing, 15.2% block tagging, and 33.4% set an alarm when a login is detected from any other source.

Figure 5 shows when any new user logs in whether they study the terms and conditions or ignore them. It can be clearly seen that more than 300 students agree that when they log in as new user, they ignore the terms and conditions and don't even read them. Only less than 100 people study the full details while logging in to social networks.

From *Figure 6*, it can be clearly seen that the majority of the users don't read terms and conditions while joining social networks. Analysis (as shown in *Figure 6*) reveals that about 34.4% are aware of privacy concerns but still ignore the terms, whereas 32.7% of the students take all the terms and conditions regarding privacy seriously, and read them all, while only 12.6% ignore the terms and conditions about privacy.

However, *Figure 7* shows that if anyone tries to disclose user information, about 33.8% of them believe it has a high impact, whereas 36.8% show it is somewhat difficult, and 22.5% ignore it. All the significant users avoid even ads coming up in front of them.

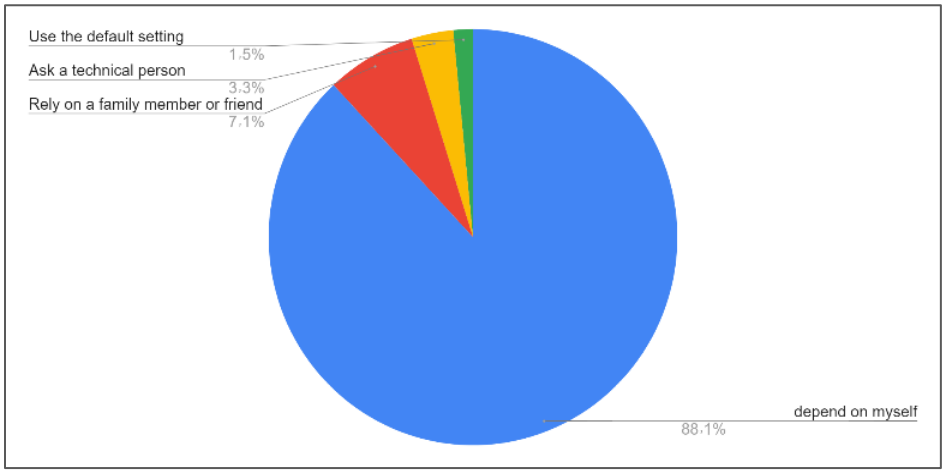

Figure 4 Do you adjust the privacy settings for your account(s) on social media?

Table 6 Which privacy controls do you use?

Social media	Frequency	Percent
Control how others can find me.	403	44.1%
Block spam users.	311	34.1%
Control who can message.	333	36.5%
Restrict visibility of my profile.	364	39.9%
Restrict photo tagging.	139	15.2%
Set alarm if login occurs from unknown.	305	33.4%
I don't use any mechanism.	241	26.4%

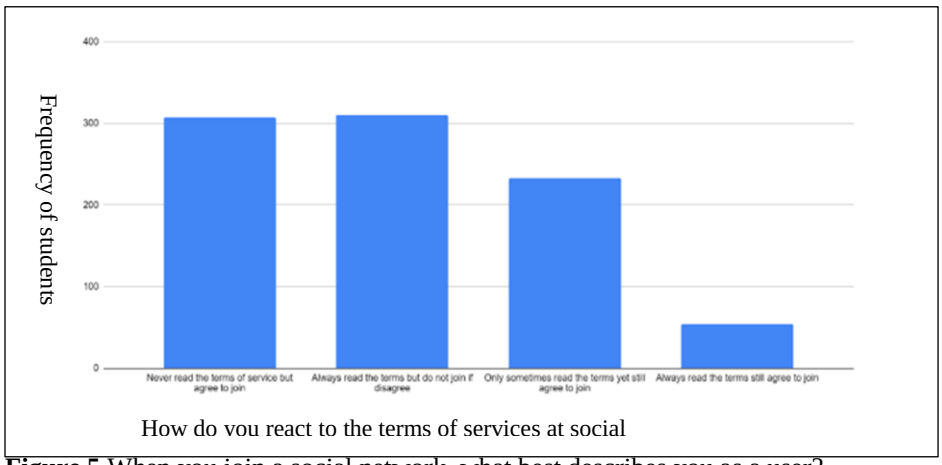

Figure 5 When you join a social network, what best describes you as a user?

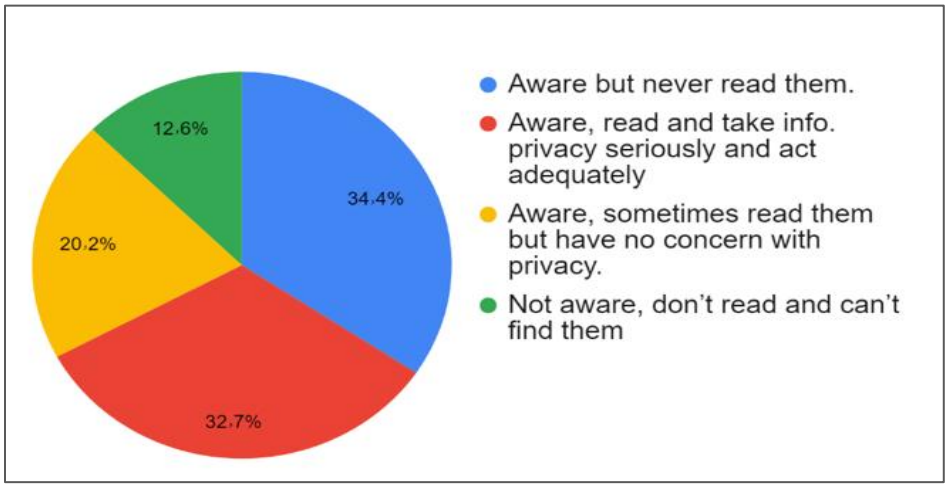

Figure 6 With regard to the privacy policies of social networks, which answer describes you as a user?

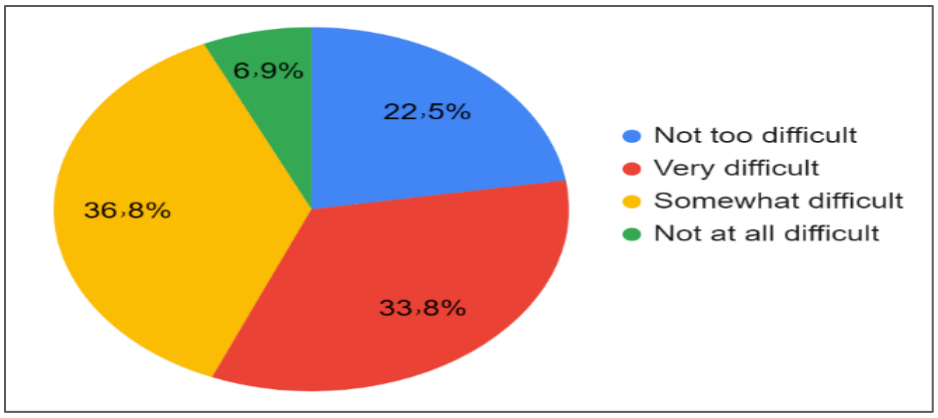

Figure 7 If others try to learn or disclose your user information on social media pages, what is the impact?

4.Discussion

Table 1: shows the demographic information of the participant students from Qassim university, and we can see that most of them (68.3%) were female, while the education levels were distributed among them as foundation (7.1%), undergraduate (78%), and postgraduate (6%). Also, almost half of the respondents (49.6%) study in the science field, (43.6%) study in the arts and humanities field and the remainder study medical science.

The general findings of this study suggest that all the Qassim University students from various departments, different colleges and levels use SNS and are using various types of social media. Moreover, the students at Qassim University are using two or more different social media platforms. Table 3 explains that the students use the most common SNS available in Saudi Arabia as follows, decreasing: WhatsApp, Twitter, Snapchat, Instagram, and Facebook. Most of them use WhatsApp, and the least used social media network was Facebook. Whereas, some of them used other types of SNS. Concerning these results, a study conducted in Qassim University in Saudi Arabia also discovered that WhatsApp and Twitter were the most used social networks between students. On the other hand, Facebook was the least used social network between students of Qassim University.

Figure 1 shows the time spent on social media by students, and it can be observed that close to half of them (43.5%) used SNS platforms for more than four hours a day, while, only a few (5.5) students spent less than an hour using SNS platforms. Regarding how long students have been part of SNS, most of them (86.9%) started to be a member of one the SNS platforms for more than four years, while only (1.3%) joined the SNS platforms less than one year ago. Smartphones are the most popular devices (99%) used to access and browse the SNS platforms by the students of Qassim University. While desktop devices were not preferred tools to access SNS platforms. A number of students use different types of devices to access and browse the SNS platforms. Concerning these results, a study found that as most of the students in Qassim university use smartphones to access and browse the SNS, which are easy to use and available near the user most of the time, that led them to spend more time on SNS platforms and join more types of SNS platforms for different purposes.

As can be seen in Table 5, the first goal of using SNS platforms is to connect with friends (77.5%), which is expected, since students at university have classmates and other friends from previous levels of education. The second goal for using these SNS platforms is connecting with new friends with similar interests (28.3%), which reflect that some of the students are looking at other students in other universities who are studying the same subject or have the same hobbies. The third goal of using SNS found between the students (35.9%) was sharing knowledge and expressing their opinion about a topic. Finally, (7.8%) of the students at Qassim university were not sure about their reasons for joining SNS platform(s). On the interaction in social media by the students to share or comment publicly, *Figure 3* shows that according to the outlooks of the participants, more than 300 students share their opinion or comment in public, while around the same number of students rarely share their opinion or comment publicly. The remaining students are distributed nearly equally between the three categories frequently, often, and never share their opinion or comment publicly.

In the section about account privacy settings, *Figure 4* shows how the students set privacy used in their current accounts on SNS platforms. It shows clearly that most of the students (88.1%) chose their privacy level for their account without consulting anybody; conversely (1.5%) of the students use the default privacy settings. Also, (7.1%) of the students ask members of their families or friends about what they should for privacy control in their current accounts of SNS. Only (3.3%) of students obtain a consultation with technical people about setting their SNS account privacy. The SNS platforms offer a number of privacy control mechanisms to meet the requirements of most users, which include, in this study, control how others find me, block spam, control who can message me, restrict my profile visibility, limit photo tagging, set alarm if login happens from unknown source. The study found that nearly half of the students (44.1%) control the 'how others can find me' mechanism, while only (15.2%) of the students use restrict photo tagging mechanisms. The students use the mechanisms block spam, control who can message, limit visibility of my profile by (34.1%, 36.6%, 39.9%), respectively.

With regard to reading the terms of service agreement of SNS platforms, *Figure 5* shows that when any new user logs in, either they study the terms and conditions or ignore them. It can be clearly seen that more than 300 students agree that when they login as new users, they ignore the terms and conditions and don't even read them. Only less than 100 people study the full details when they login to social networks. This result reflects on whether the privacy policies of the SNS platforms are looked at, where a third of the students (34.4%) don't read terms and conditions while joining social networks, however, they are aware of the privacy factors. While (32.7%) of the students realize the importance of all the terms and conditions regarding privacy and read them in their entirety. Only (12.6%) of the students do not care about the terms and conditions regarding privacy.

The difficulty or ease of hiding user's private information from the user's social network pages is one of the privacy techniques for users of SNS platforms and depend on many parameters such as SNS platform settings and the technology culture of the user. Around a third (33.8%) of the students find hiding a user's private information is very difficult. Whereas (36.8%) of students find it somewhat difficult to maintain their privacy and (22.5%) of students conceal their private information easily.

5.Conclusion

In this paper, awareness of information privacy is investigated based on the students of Qassim University who use SNS. A detailed study was carried out with 913 student responses from various departments and of differing gender, age, and field of study. The study shows that 89% of the students use WhatsApp, 74.8% use Snapchat, 3.9% use Facebook, 77% use Twitter, and 62% use Instagram, while 77.5% of the students use social media for connecting with friends and avoid connecting with new people for security reasons. Moreover, 44.1% of users control whether they can be searched for, 34.1% block spam users, 36.5% control inbox messaging, 39.9% restrict profile visibility, and 33.4% set alarms for logins of their profile. This analysis reveals that the majority of users in every SNS are concerned about their privacy and personal information. All the users ensure that their privacy is maintained, personal information is not shared, and in case of violation of privacy, the government must take action on it.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Aljohani M, Nisbet A, Blincoe K. A survey of social media users privacy settings & information disclosure. The proceedings of Australian information security management conference, cowan university, Perth, Western Australia. 2016 (pp.67-75).

[2] Li K, Wang X, Li K, Che J. Information privacy disclosure on social network sites. Nankai Business Review International. 2016; 3(7):282-300.

[3] Abril PS, Levin A, Del Riego A. Blurred boundaries: social media privacy and the twenty-first-century employee. American Business Law Journal. 2012; 49(1):63-124.

[4] Del Riego A, Sanchez Abril P, Levin A. Your password or your paycheck? a job applicant's murky right to social media privacy. Journal of Internet Law. 2012; 16(3):17-26.

[5] https://www.managingip.com/article/b1kc1mcwg39nps/to-tweet-or-not-to-tweet-advice-on-social-media. Accessed 22 May 2020.

[6] Van Schaik P, Jansen J, Onibokun J, Camp J, Kusev P. Security and privacy in online social networking: risk perceptions and precautionary behaviour. Computers in Human Behavior. 2018; 78:283-97.

[7] https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics. Accessed 22 May 2020.

[8] AlSagri HS, AlAboodi SS. Privacy awareness of online social networking in Saudi Arabia. In international conference on cyber situational

awareness, data analytics and assessment 2015 (pp. 1-6). IEEE.
[9] Aljasir S, Woodcock A, Harrison S. Facebook in Saudi Arabia: some aspects of facebook usage by Saudi university students. International Journal of Engineering and Technology. 2013; 5(1):80-4.
[10] Shin DH. The effects of trust, security and privacy in social networking: a security-based approach to understand the pattern of adoption. Interacting with Computers. 2010; 22(5):428-38.
[11] Al Johani M. Personal information disclosure and privacy in social networking sites (Doctoral dissertation, Auckland University of Technology). 2016.
[12] Strater K, Lipford HR. Strategies and struggles with privacy in an online social networking community. People and Computers XXII Culture, Creativity, Interaction. 2008:111-9.
[13] Bunnig C, Cap CH. Ad hoc privacy management in ubiquitous computing environments. In international conference on advances in human-oriented and personalized mechanisms, technologies, and services 2009 (pp. 85-90). IEEE.
[14] Ni Q, Bertino E, Lobo J, Brodie C, Karat CM, Karat J, et al. Privacy-aware role-based access control. ACM Transactions on Information and System Security. 2010; 13(3):1-31.
[15] Taheri S, Hartung S, Hogrefe D. Achieving receiver location privacy in mobile ad hoc networks. In international conference on social computing 2010 (pp. 800-7). IEEE.
[16] Sanchez-Casado N, Navarro JG, Wensley A, Tomaseti-Solano E. Social networking sites as a learning tool. The Learning Organization. 2016.
[17] Bhandari RS, Bansal S. Privacy concerns with social networking sites: an empirical investigation of users in national capital region (NCR), India. South Asian Journal of Management. 2019; 26(3):68-87.
[18] Hong W, Thong JY. Internet privacy concerns: an integrated conceptualization and four empirical studies. Mis Quarterly. 2013; 37(1):275-98.
[19] Hsu CL, Lin JC. An empirical examination of consumer adoption of internet of things services: network externalities and concern for information privacy perspectives. Computers in Human Behavior. 2016; 62:516-27.
[20] Xie E, Teo HH, Wan W. Volunteering personal information on the internet: effects of reputation, privacy notices, and rewards on online consumer behavior. Marketing Letters. 2006; 17(1):61-74.
[21] Youn S. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. Journal of Consumer Affairs. 2009; 43(3):389-418.
[22] Martin KD, Murphy PE. The role of data privacy in marketing. Journal of the Academy of Marketing Science. 2017; 45(2):135-55.
[23] Dhawan S, Singh K, Goel S. Impact of privacy attitude, concern and awareness on use of online social networking. In international conference-confluence the next generation information technology summit (Confluence) 2014 (pp. 14-7). IEEE.
[24] Krasnova H, Günther O, Spiekermann S, Koroleva K. Privacy concerns and identity in online social networks. Identity in the Information Society. 2009; 2(1):39-63.
[25] Gupta B, Chennamaneni A. Understanding online privacy protection behavior of the older adults: an empirical investigation. Journal of Information Technology Management. 2018; 29(3):1-3.
[26] Prince C. Do consumers want to control their personal data? empirical evidence. International Journal of Human-Computer Studies. 2018; 110:21-32.
[27] Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions. Information Systems Research. 2006; 17(1):61-80.
[28] Rotenberg M. Privacy in the modern age: the search for solutions. New Press. 2015.
[29] Al Hasib A. Threats of online social networks. International Journal of Computer Science and Network Security. 2009; 9(11):288-93.
[30] Hargittai E, Marwick A. "What can I really do?" explaining the privacy paradox with online apathy. International Journal of Communication. 2016.
[31] Talib S, Ismail NA, Olowolayemo A, Naser SA, Haron SZ, Yusof AH. Social networks privacy policy awareness among undergraduate students: the case of Twitter. In the international conference on information and communication technology for the muslim world 2014 (pp. 1-5). IEEE.
[32] Aldhafferi N, Watson C, Sajeev AS. Personal information privacy settings of online social networks and their suitability for mobile internet devices. arXiv preprint arXiv:1305.2770. 2013.
[33] O'Brien D, Torres AM. Social networking and online privacy: facebook users' perceptions. Irish Journal of Management. 2012.
[34] Ibrahim S, Tan Q. A study on information privacy issue on social networks. ISeCure-The ISC International Journal of Information Security. 2019; 11(3):19-27.

Abdullah Alabdulatif is Assistant Professor of Computer Department, College of Sciences and Arts, Qassim University. He graduated from Qassim University, Saudi Arabia in 2004. He received a bachelor of computer Science degree. Then entered Newcastle University, UK and received a Master of Computer Security and Resilience degree in 2009 and PhD in Information Security from Nottingham Trent University in 2014. He has 6 research papers in refereed international journals and conferences. He is interesting research in Academic & Research includes Wireless security, IoT security, Blockchain Security.
Email: A.Alabdulatif@qu.edu.sa

Fahad Alturise is currently working as an Assistant Professor in the Computer Department, College of Science and Arts in Ar Rass, Qassim University, Saudi Arabia. He has an experience of twelve years in the field of teaching and research. He holds a PhD in Information Technology from Flinders University. His primary research interests include e-learning, e-services, e-government, IOT, ICT adaption, IT security and Software Engineering. He has published 12 papers in international journals/conference proceedings He was a member of the Australian Computer Society (ACS) for 4 years.
Email: falturise@qu.edu.sa