International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 16, Issue 1, 2022

Social Media Users and Cybersecurity Awareness: An International Perspective

Dr., Fahad. Z. Alshammari[1] Dr, Waleed. M. Eyadat [2], [1,2]Department of Curriculum and Instructions, Kuwait University, P.O. Box: 13281, Kuwait 71953,
Email: , [1]Fahad.alshammari@ku.edu.kw, [2]waleedeyadat85@gmail.com

The aim of the present study was to investigate privacy awareness on social media platforms among 817 undergraduate students from different departments in college of education at Kuwait University. The main objective of the research study was to promote students' knowledge of their use of privacy setting, privacy security, and awareness of social media risks through their actions when using social network platforms. For the purpose of this study, the researchers applied a descriptive analytical approach that used data gathered through a set of questionnaires. The findings revealed the following: (1). The majority of students were concerned about their privacy when using social media while claiming to be somewhat aware of the privacy risks, and privacy settings, of SNSs. (2). Furthermore, the results indicated that the majority of participants revealed their personal information, such as their hometown, date of birth, and phone number. (3). A significant difference related to self-disclosure and information sharing in students based on their gender.

Keywords: *Privacy awareness, Privacy concern, Personal Information Disclosure, Cybersecurity.*

1 Introduction

Social media platforms including Twitter, YouTube, Snapchat, and Instagram have certain practical benefits, such as allowing users to create and share their own profile (Zheleva et al., 2012), share their personal information, and engage in interesting common spaces with friends (Shabnoor & Tajinder, 2016) to simply socialize and share knowledge (Gaál et al., 2015). Due to the massive growth of mobile device usage, combined with the explosive growth of social media platforms, social media and such platforms have gained high popularity among internet users of all ages for a wide variety of purposes (Alalawi & Al-Jenaibi, 2016). Currently, the number of social media users is remarkable. According to "The 2020 Global digital overview statistic", more than 4.5 billion people now use the internet, and 3.8 billion of them use social media.

This proliferation of shared personal data presents a variety of risks for individuals and increases the need for data protection awareness and security measures (Hazari & Brown, 2014). Numerous studies have consistently concluded that the overwhelming majority of people are 'concerned' or 'very concerned' about threats to their privacy while online (e.g., Ali et al., 2019;
Choi & Sung, 2018; Din et al., 2018). For example, "The 2020 Pew Research Center", reported that 79% of Americans were concerned about their privacy while on the internet, and 64% said that they have little or no control over their data being collected. This can be attributed to many critical reasons including a lack of understanding about data privacy laws, a lack of privacy settings, a lack of policymaking (Michota & Katsikas, 2018), a lack of privacy literacy, and a lack of privacy awareness (Trepte et al., 2015).

In Kuwait, online social platforms are becoming increasingly popular, especially among students and young populations. They allow individuals to communicate with others, share ideas, and post personal information (Hamade, 2013). Statistics of social media usage reports have shown that there were 4.25 million social media users in Kuwait (Digital 2021 reports). Due to this massive amount of information being exchanged and available online, concerns surrounding users' privacy have created new challenges (Hazari & Brown, 2014) and highlight dangerous consequences, such as blackmailing, stalking, and identify theft. (Aldhafferi et al. ,2013).

Furthermore, there is a lack of empirical research investigating this phenomenon of social platforms in Kuwait. Hence, to fill this knowledge gap, this study contributes to the discussion and nascent body of research in three steps. First, we explore the notion of privacy awareness and privacy concerns in the specific context of Kuwait's higher education institutions. Second, we analyze privacy awareness in relation to the disclosure of personal information. Third, we analyze privacy awareness in terms of security and policies among active users. To achieve the greatest accuracy possible, a preliminary questionnaire was pilot tested with a group of 100 students from the same college, who were not included in the final sample of the study, by crafting an online survey during

the first semester of 2021 to gauge students' security awareness through their actions when using social network platforms. Participants in this pilot test shared at least one type of information about themselves on SNSs but did not alter their settings to protect their privacy. Our observations indicate that users of online social networks may not be aware of how much they actually reveal online. Therefore, increasing students' awareness is essential to protecting their privacy when using social media. We hope that our survey provides a clear and comprehensive academic and practical understanding of privacy awareness among Kuwaiti undergraduate students.

2 Literature review

2.1 Online personal data security awareness

Data such as names, birthdays, e-mail addresses, and phone numbers are examples of personal data that are used to identify a user or a person (Rao et al., 2014). In this research, we refer to personal data that is embedded in online profiles used to communicate ideas, share photos and videos, celebrate birthdays, and seek information. We believe that this identifiable information must be considered personal data and must be controlled by users themselves. Given the increasing significance of online data privacy, a concern that ought to receive maximum attention is how to protect this massive amount of information that has become available online and how these data about active users are used (Hazari & Brown, 2014).

A review of the literature on digital privacy concerns about personal data indicates that real privacy risks are believed to arise when private information is shared by others and when users often disclose personal identifiable information (Gruzd & Hernández-García, 2018; Hazari & Brown, 2014; Magolis & Briggs, 2016; Weber, 2015; Yang, 2013). Specific issues of social networks have played important roles in social lives (Abdullahi et al., 2012) and have been the subjects of extensive research efforts in the past decade (Michota & Katsikas, 2018). Privacy, trust, and security are closely intertwined. Privacy preservations and security provisions rely on trust (Lee et al., 2016). Laws and legislation should foster a better understanding with more control over a user's personal data through easy and flexible methods (Michota & Katsikas, 2018). However, some issues related to privacy and security remain unsolvable. For example, The 2019 Pew Research Center's "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information" found that 63% of Americans say they understand very little or nothing about the laws and regulations that are in place to protect their data privacy. At the same time, only 9% of American adults say they always read a company's privacy policy before agreeing to its terms and conditions, while 36% say they never read a privacy policy before agreeing to it. This can be attributed to many reasons, one of which is that the level of privacy protection offered by legislation is insufficient (Ziegeldorf et al., 2014) and lacks comprehensive legal protections for personal data.

Pensa (2018) argued that even with the adoption of legal and other protections by SNSs, violations of privacy remain a concern; individuals often willingly reveal and share personal identifying information about themselves but are not aware of who can access it. In a comparative analysis of information disclosure on social media platforms, Peterson and Siek (2009) found that participants were generally not concerned with the information they disclosed online and were not aware of how this information could be used against them by malicious third parties.

Privacy features are technical implementations of privacy controls on websites. Such functions can be used by users to adjust the visibility of their profile or of certain information (Kuczerawy & Coudert, 2010), enabling them to decide what to share on social platforms. Social media platform operators have provided many security features for preserving the privacy of their users (Gupta, 2015), but it is not clear whether users are actually making use of their privacy settings. According to the European Union Agency for Network and Information Security (2014), privacy settings are ignored by a large majority of social network users. This ignorance is caused by limitations of awareness and understanding among developers and data controllers as well as a lack of technical implementation tools, which, in turn, affects self-disclosure and presents unique privacy concerns regarding one's privacy and facilitates privacy threats related to SNSs. Kisilevich and Mansmann. (2010) investigated deferent aspects of information revealed by more than 30 million user profiles, collected from Runet, to explore the security and privacy measures of SNSs. The results indicated that most Runet social media platforms do not implement adequate security measures to prevent automatic profile extraction. Aldhafferi et al. (2013) examined the personal information privacy settings of online social networks and their suitability for mobile internet devices. They found that several risks surrounding the posting of personal information include embarrassment, blackmailing, stalking, and even identity theft.

Online social media platforms are becoming increasingly popular in Kuwaiti society, with their usage rising rapidly for communication and sharing information (Hamade, 2013). However, the COVID-19 pandemic brought about social changes and accelerated the transformation of the communication sector, creating new challenges with privacy implications (OECD,2020) In the context of the pandemic, a privacy algorithm has recently been identified as an important factor in data breaches. In the Arab Times Cybercrime newspaper of October 11, 2020, a report by Trend Micro, the global leader in developing cybersecurity solutions, indicated that Kuwait was exposed to 1,305 cyberattacks related to COVID-19 during the first half of 2020. Aware of these risks and the value of social media platforms to Kuwaiti users, the Kuwaiti government has been at the forefront of privacy protection.

In a recent study by Lohar,et,al (2021), called "*Irish attitudes to privacy in COVID-19 times"*, has found that 61%, of its respondents were willing to share their personal data including their locations,

contacts, and medical dates on social media. This increase in global data privacy concerns increases the minimum level of data protection awareness and security measures. Regarding its focus on cybersecurity, Kuwait has recognized the importance of protecting individual privacy to prevent the collection and abuse of personal data online by enforcing cybercrime as a federal law to protect the privacy of individuals. Furthermore, the current law No. 63 was designed to ensure individual data protection, personal identity protection, and confidentiality. (State of Kuwait, Ministry of Interior, 2016).

This law is essential for better security and better individual data protection and demonstrates how cyberspace governance and security remain the central domains for international conflict have become growing problems worldwide. Hence, improved awareness of personal data security and privacy protection for users are needed. To date, privacy concerns due to a lack of awareness of security threats in the context of social media are still critical issues and can become a risk to adolescents more often than most adults realize. This reflects the complexity of online social interactions and requires more efforts and increased research. The solutions therefore entail increasing Kuwaiti students' awareness of the use of privacy settings and creating policies to better manage the information they disclose.

2.2 Personal information disclosure on social media platforms

Personal information disclosure is the act of revealing personal information to others (Kim et al., 2015). Personal information disclosure involves submitting sensitive information to other users on an SNS regardless of context (Gruzd & Hernández-García, 2018). Theoretically, it has been argued that people are willing to voluntarily share information about their daily lives while posting their photos and locations, which can be seen as a behavioral intention (Lo, 2010). Prior studies have shown that Facebook members disclose a considerable amount of private information but are not aware of their privacy options (Aljohani et al., 2016; Tatjana et al., 2010; Tessem & Nyre, 2013; Tuunainen et al., 2009). For example, when users first sign up with Facebook, they will be constantly reminded by the platform to update their profile with more personal information, such as date of birth, hometown, and workplace.

Tuunainen et al. (2009) investigated users' awareness of privacy on Facebook, and their results indicated that respondents who seem to be active users of Facebook disclose a considerable amount of private information. Contrary to users' own beliefs, they are not sufficiently aware of the visibility of their information to people they do not necessarily know. In addition, more than 80% of the sample revealed their personal information, such as their hometown, date of birth, e-mail address and education information. A similar investigation by Tatjana et al. (2010) examined the type of personal and contact information young people disclose through their profiles on Facebook. They found that most people, regardless of gender, enter their full name, facial picture, hometown,

and e-mail address into their profile. Consequently, the more they disclose, the greater the risk of what they themselves consider breaches of their privacy.

Tessem and Nyre, (2013), noted that frequent social media users are more inclined to share their location and other personal information than others. This highlight important concerns surrounding users' privacy (Cañares, 2018), which introduce new threats to users due to their attractiveness and the massive amount of information they share (Salih & Mohammed, 2018).

Previous studies have examined gender differences and the influences of specific behaviors entail directed self-disclosures and information sharing (Idemudia et al., 2017; Rowley et al., 2016). Their results suggest that males are more likely than females to post their personal information when using social media Kandari and Al-Hajri (2016) investigated the influence of gender differences among Instagram users engaged in Kuwaiti higher education. The findings indicated that males are more likely than females to post their personal information on Instagram and to have unprotected Instagram accounts. In general, the literature about the motivations of SNS use has observed that females are more interested in using SNSs merely for personal reasons and to search for information, whereas men are more likely to look at other people's profiles with the intention to make new friends (Herring & Kapidzic, 2015; Kim et al., 2020; Rollero et al., 2019). Women are also much more careful than men about the information they share online. Kuo (2015) investigated gender differences in Facebook's privacy settings among college students in Taiwan and found that females were more concerned about sharing their personal information than males and selected higher levels of privacy. A similar study by Rafique (2017) investigated the personal information sharing behaviors of university students via online social networks and found that females were more conscious of disclosing their personal information on OSNs than males, although social media contexts involve a mix of both genders, which has implications for how both men and women self-present.

Trust plays a crucial role within interpersonal relationships and social media. (Grabner, and Bitter, 2013). It is the willingness of a user to rely on a site and to provide personal information (Sonja & Sofie, 2015). However, the depth and reciprocity of these relationships has not been sufficiently evaluated (Håkansson & Witmer, 2015). The relative importance of trust depends on certain factors that influence people's personal information sharing behaviors or self-disclosures, e.g., social trust, trust, enjoyment, and motivation (Sharif et al., 2021). Abramova et al (2017) conducted a systematic literature review by examining 50 studies to identify the factors behind self-disclosure on SNSs. They found that users are mainly driven by several factors including building new relationships, enjoyment, and entertainment. Ampong et al. (2018) found that privacy awareness, privacy concerns, and privacy invasions are significant predictors of self-disclosures. Waldman (2016) investigated privacy sharing and trust on Facebook and found that trust exists between friends and

that the trust that exists between users and the platform is a significant factor that increases a person's willingness to share information on social media. Clearly, the more an individual is surrounded by friends that are careless about their privacy, the greater the likelihood the privacy of that individual is likely to be breached (Pensa, 2018).

Trust can exist among friends, but trust can also reasonably exist among strangers (Lo, 2010). Evidence suggests that issues of privacy arise when access to information is extended beyond one's circle of friends (e.g., Al-Rahmi & Othman, 2013; Ampong et al., 2018; Håkansson & Witmer, 2015; Koranteng et al., 2019; Sarikakis & Winter, 2017). The dangerous consequences of this act were further illustrated by Aldhafferi et al. (2013), who identified several dangers of user vulnerability on SNSs including embarrassment, blackmailing, stalking, and identify theft. This demonstrates that worries about negative consequences are real and should be added to other concerns since they pose additional challenges; privacy breaches have become an issue of grown public concern (van den Hoven et al., 2019). Therefore, social media is a forum that requires improvements in self-protection and privacy awareness.

2.3 Purpose of the study

In recent years, the state of Kuwait's information and communication landscape has changed dramatically, characterized in particular by the emergence of smartphones and the increasing penetration of social media. Websites such as Twitter, YouTube, Snapchat, and Instagram have gained high popularity among Kuwaitis of all ages (Alsurehi & Al Youbi, 2014). According to the 2016 "Consolidated Kuwait National ICT Indicators report", 99% of Kuwaiti households and 96% of all households in the country have access to the internet; 75% use social media to send messages; 65% download music, videos or images; and 63% post to social media with their mobile phones. Meanwhile, malware was considered the biggest security threat, with 61% of organizations affected by it. Despite an exponential growth in the number of users and a massive amount of information exchange, a concern that ought to receive maximum attention is how to protect this large amount of information that has become available online and how the data about active users are used (Hazari & Brown, 2014). This highlights a phenomenon that is relevant in the case of so-called potential privacy risks. These risks include embarrassment, blackmailing, stalking, and even identity theft. Hence, efficient awareness is of vital importance. Many recent studies on privacy concerns focus on analyzing this phenomenon in the United States and Europe, whereas studies in Islamic and Arabic countries have focused on the production, dissemination, procession and effects of information, whether through media or interpersonally in political contests (Muñoz & Bolívar, 2015). To fill this knowledge gap, this study contributes to the nascent body of research by empirically exploring the privacy awareness of Kuwaiti students in the context of their online interactions. Notably, students have been shown to be ignorant of the potential risk of disclosing too much of their personal information and often do not realize who can access the information that

they post on social media. Unfortunately, this often leads to unintended consequences, including such threats as unwanted contact, harassment, stalking, and identity theft (Body & Ellison, 2008). These factors offer researchers an understanding of how the concept of privacy needs is a socially and contextually constructed process (Moreno-Becerra et al., 2016). Therefore, the main purpose of this study is to observe the aftereffects of a subject who takes our survey. This survey is intended to make online social network users aware of their potential privacy risks and to alert them to the possible harmful consequences of such risks. The following research questions guided the study:

RQ: 1- To what extent do preservice teachers' personal information awareness on social media platforms affect their tendency to disclose personal information?
RQ: 2- To what extent do preservice teachers' awareness of security settings and policies for personal data privacy on social media platforms affect their tendency to disclose personal information?
RQ: 3- Are there significant differences based on gender at the level of $\alpha \leq 0.05$ among preservice teachers' privacy awareness on social platforms?

2.4 Significance of the study

The importance of this study stems from the fact that only limited research has investigated privacy awareness of online social platforms among students at the College of Education at Kuwait University. The main objective of the research study is to promote awareness of privacy policies and privacy challenges to increase user privacy awareness and knowledge. Furthermore, it seeks to enhance the use of existing privacy mechanisms among active users. Thus, the study is expected to provide other researchers with critical knowledge about the privacy awareness of online social platforms. This outcome will further inform initiatives related to user privacy awareness at the University of Kuwait.

2.5 Limitations

The following limitations are relevant to the present study:

1. The sample size of this study was restricted to preservice teachers at the College of Education at Kuwait University during the 2021 academic year.
2. Internal and external validity are limited due to the reliability of the instruments used in this study.

3 Methodology

3.1 Research design

In accordance with the purpose of this study and its context, the researchers applied a descriptive analytical approach that used data gathered through a set of questionnaires (Creswell, 1998) to investigate privacy awareness on online social platforms among preservice teachers at the College of Education at Kuwait University during the 2020-2021 academic year. To achieve the research objectives, the researchers designed a multiple-choice questionnaire including 30 items with one score per item. The validity and reliability of the test were checked by a judgment panel, and modifications were made based on the panel's assessment. A total of 6000 social media users were invited to answer this questionnaire online. We used an online survey to examine users' privacy awareness of online social platforms. The questionnaire was available online for two weeks. Using the snowball effect, a total of 817 acceptable responses were received. The inclusion criteria required that participants were students and current social media users. All responses were voluntary and anonymous. The full questionnaire is omitted from this paper but can be requested from the authors.

3.2 Participants and sample

This study included 817 undergraduate students from different departments randomly selected females (62%) and (38%) males from the College of Education at Kuwait University, ranging in age from 18 to 21 years old. Study participation represented 18.13% of the total student population at the College of Education. All participants in this study were homogenous with regard to nationality, native language (Arabic), language proficiency and educational background.

3.3 Instrumentation

The instrument used in this study was developed by the researchers based on an extensive review of related theory and research in the literature (Andrews et al., 2003; Leedy & Ormrod, 2001; Long, and Robinson, 1998). The items in the instrument contained thirty questions within three dimensions investigating the awareness of personal data and information on SNNs, the awareness of privacy settings and privacy policies of SNNs, and the awareness of personal information disclosures on SNNs. The first part inquired about background information, such as gender and the type of social platforms participants actively use. To ensure the validity of the instrument, it was drafted by the researchers and submitted to several content judges who reviewed and determined its face and content validity. These judges (n = 12) also had expertise in the field of educational technology. On the basis of their feedback, items were added, dropped, or reworded as needed, and the instrument was pilot tested with a group of one hundred students who were not included in the final sample of this study. In this phase, the researchers evaluated the extent to which all the items within the instrument converged to the same construct. The items assess a preservice teacher's

privacy awareness level and are rated on a 5-point Likert scale (1, "Always"; 2, "Very Often"; 3, "Sometimes"; 4," Rarely"; and 5, "Never"). The existing instrument was available in digital form to participants at the "SurveyGizom" website, and the time for a response was limited to two weeks. The values related to the internal consistency of the instrument were estimated using the Pearson correlation coefficient. The results are presented in Table 1.

Table 1. Pearson's Correlation Coefficient of Consistency of Sample Responses across the Items on a Multiple-Item Measure (n =100).

N	Pearson Correlation	N	Pearson Correlation	N	Pearson Correlation
1	0.382**	11	0.559 **	21	0.650 **
2	0.473**	12	0.651 **	22	0.717**
3	0.371**	13	0.502**	23	0.729 **
4	0.330 **	14	0.730**	24	0.679**
5	0.540 **	15	0.764 **	25	0.417**
6	0.520 **	16	0.596 **	26	0.635**
7	0.541**	17	0.674 **	27	0.676**
8	0.429**	18	0.425**	28	0.495 **
9	0.570**	19	0.449 **	29	0.455 **
10	0442**	20	0.650**	30	0.437**

According to Table 1, the correlation coefficient of each item was significant at the level of 0.01 and high, ranging from 0.382 to 0.679 for all items. This finding suggests that all the items were highly consistent, and the instrument was valid as a tool for the study. To determine its reliability, Cronbach's alpha coefficients were calculated to evaluate internal consistency, and the results were estimated. The results are presented in Table 2.

Tabel.2 Result of Reliability Statistic N=817

	Domain	**Items**	**Cronbach's alpha**
1	Awareness of personal data and information on SNNs	10	.628
2	Awareness of privacy settings and privacy policies of SNNs	7	.602
3	Awareness of personal information disclosures on SNNs	13	.748
	Overall	30	.811

Table 2 shows that the internal consistency and reliability of privacy awareness were examined for the whole scale and subscale. Cronbach's alpha coefficient for all domains was .811 and ranged

from 0.628 to 0.748. These values were considered acceptable and suitable for fulfilling the study objectives.

3.4 Data collection

A descriptive research methodology was used to conduct this study. Data were collected from students via an online survey during the first semester of the 2021 academic year. The researchers and their assistants contacted all participants by a social media platform and explained the nature and goals of the study to assure volunteers of its confidentiality and their anonymity. The participants were also informed that the instrument would take approximately 10-15 minutes to complete. The participants who agreed to participate in the study were given the instrument and were asked to complete it within a two-week timeframe. At the end of the two weeks, the researchers and their assistants collected the instruments.

3.5 Data Analysis

Data were analyzed quantitively using SPSS 21.0, version. We generated descriptive statistics for quantitative items including Mains, and Standard deviations. A 5-point Likert scaling was used in three dimensions with 30 items in total with one score per item. A te-tests were conducted in order to determine the differences in user's privacy setting and personal information disclosure variables with genders. All items were interpreted at a conservative alpha of 0.01. Person's correlations were calculated to examine association between social media platforms and preservice teacher's privacy awareness.

4 Results

4.1 RQ: 1- To what extent do preservice teachers' personal information awareness on social media platforms affect their tendency to disclose personal information?

To explore the first guided research question, participants were asked to indicate whether they have a profile on and actively use five social media platforms, and what their motivations are for being active on any or all of these sites (check all that apply). The purpose of having this question at the start was to identify what kind of social media account the respondents had. All participants in this survey had at least one public profile. The results are given in Fig. 1. Fig:1types of social media platforms

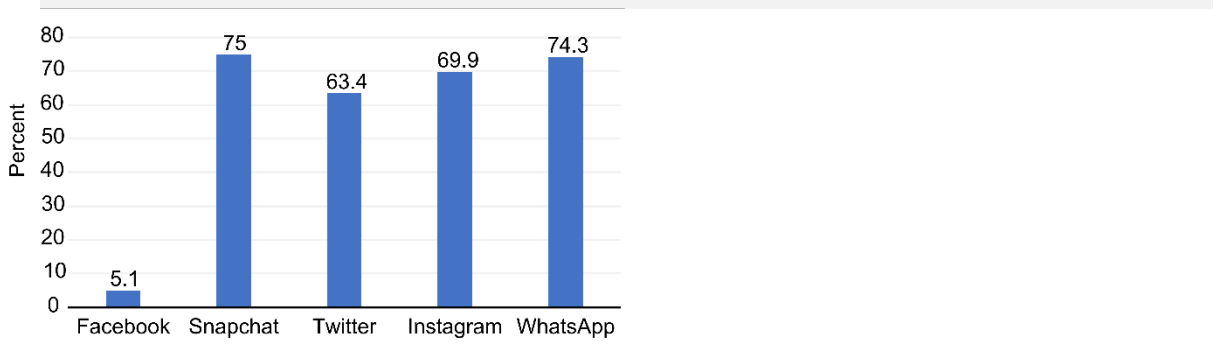

Fig. 1 shows that Snapchat was the dominant social media platform, with a response rate of 75%, whereas Facebook had the lowest percentage of users at 5.1%. These results can be attributed to the fact that users use Snapchat to talk to friends and share photos and videos. These features and the functionality of Snapchat lead to an increase in the engagement of users and, as a result, also lead to an increase in the number of downloads of Snapchat. In comparison, the majority of survey participants in this study chose not to join Facebook for many reasons, including perceived security issues, safety risks, a lack of trust, privacy concerns, and a lack of control. These findings support the existence of contributing reasons for the rejection of Facebook in addition to those that have been directly reported in the literature (e.g., Aloudat et al., 2019). One question was specifically designed to determine the reason behind a user becoming a member of a platform. The results are given in Fig. 2.

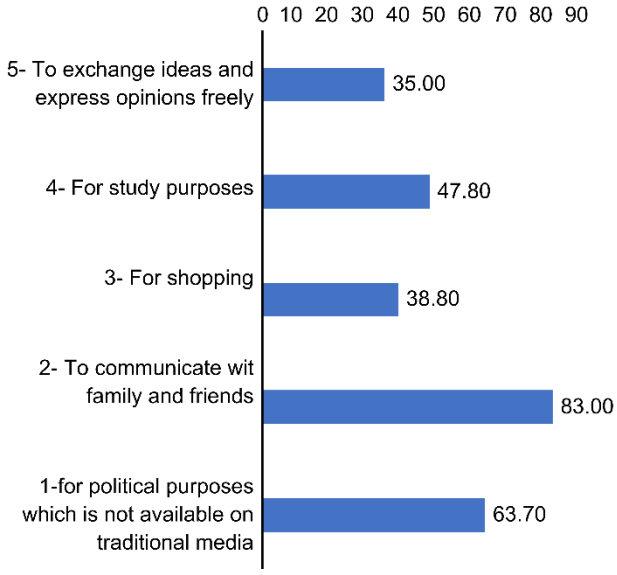

Fig. 2 shows that 83% of the survey participants use social media platforms to stay connected with others; 63.70% use one to stay updated about current events and for political purposes. Additionally, 47.80% said they use social media for study purposes, while only 38% use it for shopping online.

The means and standard deviations of privacy awareness and privacy concerns in general are given in Table 3.

Table 3. Means and Standard Deviations of Privacy Awareness and Privacy Concerns in General

Statements	Mean	Std. Deviation	Percentage
1- The privacy of my personal information on the platform is a major concern for me.	4.27	1.00	85.4
2- I am aware of the sensitive personal information that I provide to social media companies.	4.05	0.96	81.0
7- I am well-aware of the potential privacy risks and consequences of my personal data, since they are visible to people I do not necessarily know.	3.94	1.03	78.8
8- I provide my personal data such as first and last name, email address, and date of birth on social media platforms while creating my profiles.	3.84	1.01	76.8
10- I am aware that the risks of an invasion of privacy are related to the misuse by a user of his or her personal data.	3.81	1.03	76.2
4- Social media companies keep sensitive personal information they collect about users private and treat data with confidentially.	3.56	1.02	71.1
5- I am aware of Kuwait's Cybercrime Legislation.	3.31	1.22	66.2
6- I am aware that my personal data can be obtained because they are publicly available on social media and could be shared with third parties.	3.14	1.15	62.9
3- I trust social media companies to provide adequate protection and not to abuse the information disclosed.	3.13	1.06	62.7
9- I am aware who can access my private information on social media platforms.	2.74	1.17	54.8
Overall	3.62	0.45	72.4

Measured on a 1-5 scale (1 =Never, 5= Always).

The results of Table 3 revealed that the majority of participants understood their lack of awareness regarding matters of privacy and data security. A total of 85.4% admitted that they were concerned about their privacy when using social media. When asked whether they disclosed certain sensitive information in their personal data on social media platforms, 76.8% of the participants reported that

they were willing to share their private information, such as their first and last name, email address, and date of birth, voluntarily when creating their profiles on social media.

This identifiable information must be considered personal data and must be controlled by the users themselves. It is obvious that privacy in social networks is unintentionally ignored. Gruzd and Hernández-García (2018) argued that people are willing to voluntarily share their information about their daily lives, posting their photos and locations, which can be considered a behavioral intention. The latter result may be attributed to the fact that the prevalence of the use of social media increased significantly among university students due to the COVID-19 pandemic. As a result, education has changed dramatically with the distinctive rise of e-learning, whereby teaching is undertaken remotely and on digital platforms. With this sudden shift away from delivering face-to-face education to delivering online education, more student data are collected, used, and potentially exposed. Consequently, this will become a potential privacy risk involving different sorts of dangers, which can regularly breach users' privacy.

These results are consistent with the findings of, e.g., Aljohani et al. (2016), Nyre (2013), Tatjana et al. (2010), and Tuunainen et al. (2009), which suggested that Facebook members disclose a considerable amount of private information but are not aware of their privacy options. Consequently, the more they disclose, the greater their risk for what they themselves consider breaches of their privacy. In addition, 81.0% of this study's sample stated they were fully aware of the visibility of their information to people they do not necessarily know. When asked whether they trust that social media companies provide adequate protection and do not abuse their information, 62.7% of participants replied that they were "very confident" that social media companies protect their data. However, approximately 37.3% of users were not at all or not too confident that their data were secure.

This suggests that trust plays a crucial role in interpersonal relationships with and on social media platforms. It is the willingness of a user to be reliant on a platform and his or her willingness to provide personal information (Sonja & Sofie, 2015). This result is in line with other results in previous studies (e.g., Ampong et al., 2018; Håkansson & Witmer, 2015; Heo, 2014; Koranteng et al., 2019; Othman et al., 2013; Pensa, 2018; Sarikakis & Winter, 2017; Singh & Goel, 2014), which suggested that the willingness of a user to rely on a social media platform to protect personal user data increases their willingness to provide more personal information when using social media. The results of the questions related to personal information disclosures on social media platforms are given in Table 4.

Table 4. Means and Standard Deviations of Privacy Awareness of Personal Information Disclosures on Social Platforms

Statements	Mean	Std. Deviation	Percentage
30- I have no reservations to continue using social media in the future, regardless of the potential risk.	3.53	1.01	70.6
29- I believe that my personal identity is well protected on social media.	3.31	1.05	66.3
18- I share certain information about my daily life, posting my photos and locations and give them away voluntarily.	3.13	1.20	62.6
20- I only share my personal information and common interests with friends and family.	3.09	1.11	61.8
28- I have no problem with my friends accessing my profile through social platforms.	3.08	1.24	61.5
19- I accept friend requests from strangers and people I don't know.	3.05	1.16	61.1
26- I share my private information, such as restaurants I visit, family and children's photos, and travels, on social media.	2.88	1.19	57.6
25- My profile contains my photo as my social media profile picture.	2.75	1.28	55.1
27- I only share my personal photos and videos on social platforms.	2.73	1.23	54.6
22- I post pictures and videos of my family and friends on social media.	2.47	1.24	49.3
21- It is fun to share certain kinds of information on social media platforms.	2.43	1.18	48.5
23- I repost photos and videos of other people on social media without their consent.	2.15	1.21	43.0
24- I post certain information about my daily life that others may not want to post on social media.	2.07	1.21	41.3
Overall	2.97	0.57	59.4

Measured on a 1-5 scale (1 =Never, 5= Always).

As shown in Table 4, 70.6% of respondents said that they had no reservations to continue using social media in the future, regardless of any potential risk. A total of 66.3% declared they only

shared their personal information and common interests with friends and family. The respondents were asked whether their personal information was visible to others or not, and 61.5% admitted that they have no problems with other friends accessing their profiles on social media. When asked what type of personal information they disclose on social media, 54.6% of the respondents admitted that they share personal photos and videos. The respondents were asked whether they accept friend requests from strangers, and 61.1% replied that they accept friend requests from people they do not know. Respondents were asked to describe the personal information they disclosed on their profiles, and 55.1% admitted that they had their photo in their profile. When asked whether they reposted the personal information of others, 43.0% admitted that they reposted photos and videos of other people on social media without their consent. The respondents were asked whether they posted certain information about their daily lives that others might not want to post on social media, and 59.4% responded affirmatively.

This result indicates that preservice teachers are unaware of the extent to which their tendency to disclose personal information has spread. In previous studies, it was confirmed that there is no relation between the level of concern in general among the users of social networks and the amount and types of information they disclose (e.g., Abramova et al., 2017; Ampong et al., 2018; Sharif et al., 2021). This can be attributed to many reasons, including a lack of understanding about data privacy laws, a lack of privacy literacy, and a lack of privacy awareness (Trepte et al., 2015). Unfortunately, this can often lead to unintended consequences, including such threats as unwanted contact, harassment, stalking and identity theft (Body & Ellison, 2008).

Another explanation for this is that users may feel comfortable sharing personal information on a social network for the benefit of their friends, who are active users. This observation is validated by several studies (Garcia et al., 2018; Hazari & Brown, 2014; Hew, 2011; Magolis & Briggs, 2016; Slovenia, 2009; Webb.et al., 2017; Weigel, 2013; Yang et al., 2017), which point out that a lack of privacy awareness is typical on social networks, while actual privacy risks arise when private information is shared by others and when users often disclose personal identifiable information.

4.2 RQ: 2- To what extent do preservice teachers' awareness of security settings and policies for personal data privacy on social media platforms affect their tendency to disclose personal information?

There were associations between the extent to which participants were aware of security settings and policies for personal data privacy and the effect of their tendency to disclose personal information on social media. The results are given in Table 5.

Table 5 Means and Standard Deviations of Online Personal Data Security Awareness

Statements	Mean	Std. Deviation	percentage
11- I Make sure to use the privacy features and privacy setting provided by social networking sites to protect my personal data	4.14	0.90	82.8
17- I Make sure to maintain my security settings and keep it up to date	3.73	1.07	74.5
15-I make sure to adjust and change my privacy setting on social media networking sites	3.72	1.01	74.4
16-I am aware that if I do not change my privacy setting, all members of the same network can see my profile	3.61	1.01	72.2
14- I Make sure to keep security software current against online threats to protect both privacy and security.	3.55	1.09	71.0
13- I am aware that social networks companies can change their privacy policy at any time without the user's permission	3.31	1.19	66.3
12- I read a company's privacy policy before agreeing to the terms and conditions	3.26	1.20	65.3
Overall	3.58	0.65	71.6

Measured on 1-5 scale (1 =Never, 5= Always)

Table 5 shows that preservice teachers were highly aware of these information security concepts. A total of 82.8% of the users considered themselves familiar with the privacy features and privacy settings provided by social media platforms to protect their personal data. However, the findings showed that preservice teachers were not highly aware of social media companies' privacy policies. Only 66.3% indicated that they were familiar with a privacy policy (M= 3.26, SD= 1.20). In addition, 71.6% of students stated they did not read security policy agreements before agreeing to terms and conditions (M= 3.58, SD=0.65). To understand which groups were different from each other, an independent t-test was conducted. As a result, a significant difference was observed for male students. The detailed analysis is presented in Table 6.

Table 6. t-Test Results Demonstrate the Difference by Gender

Gender		N	Mean	Std. Deviation	df	t	sig
Awareness of personal data and information on SNNs	Male	309	3.61	0.47	814	1.26	.209
	Female	507	3.56	0.54			
Awareness of privacy settings and privacy policies of SNNs	Male	309	3.68	0.68	814	1.92	.056
	Female	507	3.58	0.72			
Awareness of personal information disclosures on SNNs	Male	309	2.95	0.70	814	4.27	.000
	Female	507	2.74	0.69			
Overall	Male	309	3.34	0.47	814	3.98	.000
	Female	507	3.21	0.45			

*sig = 0.05

Table 6 revealed no significant difference in preservice teachers in their privacy awareness of personal data and information security by gender, specifically for privacy settings and privacy policies (M=.209, SD= 0.47 and M=3.68, SD=0.68, respectively). However, the results revealed a significant difference in preservice teachers' awareness of personal information disclosures of SNNs based on their gender. Females (M=3.24, SD=0.47 then males (M=3.12, SD=.45) sig at level of< 0.05. Males are significantly more likely to share their personal information on social media than females. Likewise, females tend to be much more conservative in the basic settings they choose on social media sites. Females restrict access to their profiles to friends much more than males.

The latter result may be attributed to the fact that the nature of religions and societal norms in Kuwait expect and encourage negative self-disclosures and people who feel guilty about their misbehaviors often have various reasons to feel reluctant to self-disclose their wrongdoings. This result is in line with other studies (e.g., Idemudia et al., 2017; Johnson & Sbaffi, 2016) that have suggested males are more likely than females to post their personal information when using social media. As evidenced by these results, it seems that participants who stated that they trust social networks to protect their information had never been concerned about their online privacy security were more likely to have their personal information posted publicly on their account.

5 Discussion of the findings

The purpose of this research was to investigate privacy awareness and concerns about online social media platforms among preservice teachers at the College of Education at Kuwait University. The main goal of this study was to promote awareness of privacy policies and privacy challenges to

increase user privacy awareness and knowledge within the context of online social networks, thereby enhancing the use of existing privacy mechanisms by active users. To find evidence showing the extent of discussion in the literature, a quantitative survey instrument was developed. We designed our overarching questions based on the following criteria: 1) demographics and type of SNSs chosen by the users; 2) user awareness of personal data and information on SNNs; 3) user awareness of privacy settings and privacy policies; and 4) user awareness of self-disclosures. The criterion of privacy awareness on social media platforms includes frequency of use, information control, and self-disclosure. Cronbach's alpha of all constructs was .0811, indicating strong construct reliability for the measures.

The results revealed that the majority of participants were cognizant of their lack of awareness regarding matters of privacy and data security: 85.4% replied that they are concerned about their privacy when using social media but claim to be somewhat aware of privacy risks, laws, and regulations of SNNs and their privacy policies. This can be attributed to many reasons, including a lack of understanding about data privacy laws, a lack of privacy settings, a lack of policy-making (Michota & Katsikas, 2018), a lack of privacy literacy, and a lack of privacy awareness (Trepte et al., 2015). These findings are in line with numerous studies (e.g., Ali et al., 2019; Hazari & Brown, 2014; Paine et al., 2014; Zheleva et al., 2012), which consistently concluded that the overwhelming majority of people are 'concerned' or 'very concerned' about threats to their privacy while online. Furthermore, this result is in contrast to the 2020 Pew Research Center, which reported that 79% of Americans were concerned about their privacy while on the internet and that 64% said they had little or no control over their data being collected.

Furthermore, the results indicated that preservice teachers in our sample seemed to disclose a large amount of information on themselves. A total of 76.8% of the participants reported that they were willing to voluntarily share their information, such as first and last name, email address, and date of birth, when creating their profile on social media. This highlighted the real privacy risks inherent in sharing this information online. Unfortunately, this can often lead to unintended consequences, including such threats as unwanted contact, harassment, stalking, and identity theft. Therefore, it is important for users to be aware of the information that they are providing to protect their privacy. This finding is in contrast with the results of Lo (2010), which point out that people are willing to voluntarily share their information about their daily lives by posting their photos and locations, which can be considered a behavioral intention. Contrary to their own beliefs, users are not sufficiently aware of the visibility of their information to people they do not necessarily know (Tuunainen et al., 2009).

Trust plays a crucial role between interpersonal relationships and social media. Thus, the findings of this research indicated that 62.7% of users admitted that they trust social media companies to

provide adequate protection and not to abuse the information disclosed. This lack of awareness can lead to several privacy threats including the privacy and security vulnerabilities of one's confidential information and personal safety. This result is in contrast to the results of Waldman (2016), which suggested that trust exists between users and that a platform is a significant factor that increases a person's willingness to share information on social media. Finally, the results showed that Snapchat was the dominant social media platform among the five options, with a response rate of 75%, whereas Facebook had the lowest percentage of users at 5.1%.

The independent t-test analysis results revealed a significant difference related to self-disclosure and information sharing in preservice teachers based on gender. This suggests that males are more likely than females to post their personal information on social media. This finding confirmed previous studies that indicated that males are more likely than females to post their personal information when using social media (e.g., Idemudia et al., 2017; Kandari & Al-Hajri, 2016). Furthermore, this result suggests that females are primarily interested in using SNSs for personal reasons and to search for information, whereas men are more likely to look at other people's profiles with the intention of making new friends (Haferkamp et al., 2012; Herring & Kapidzic, 2015; Kim et al., 2020; Rollero et al., 2019). Women are also much more careful than men about the information they share online.

Our results related to the lack of awareness of data privacy issues in social media highlighted a phenomenon that is relevant to the case of a so-called privacy paradox. These risks include embarrassment, blackmailing, stalking, and even identity theft. Hence, efficient awareness is of vital importance. These observations indicate that users of online social networks may not be aware of how much they actually reveal online. Therefore, increasing Kuwaiti student awareness is essential to protect their privacy when using social media.

6 Conclusion

The analysis of the data and the findings of this study lead to the following conclusions: The results of our study should be considered in light of its limitations based on its sample size, which was restricted to preservice teachers at the College of Education at Kuwait University during the 2021 academic year. A second limitation is based on the internal and external validity, which was limited due to the reliability of the instruments used. Therefore, our claims are based on results that concern preservice teachers' awareness when using social media.

Given the identified categories and the main results of the studies we analyzed, we propose that future research continues analyzing students' privacy awareness in other colleges at Kuwait University, since the majority of this study focused on the College of Education, to investigate

factors that influence self-disclosure and to analyze the relationship between individual-level cultural differences and online self-disclosure behaviors while measuring the impacts of security, trust, and privacy on information sharing. From a practical perspective, our research results provide other researchers with critical knowledge and information about privacy awareness on online social media platforms. This outcome will inform further initiatives related to user privacy awareness at Kuwait University.

References

Abdullahi, H. O., Said, A., & Ibrahim, J. (2012). An investigation into privacy and security in online social networking sites among IIUM students. *Journal of (WCSIT), World of Computer Science and Information Technology*, *2*(2), 57–61.

Abramova, O., Wagner, A., Krasnova, H., & Buxmann, P. (2017). Understanding self-disclosure on social networking sites - a literature review. In 23rd *Americas conference on information systems* (pp. 1–10). AMCIS.

Alalawi, N., & Al-Jenaibi, B. (2016). Social network and privacy. *Journal of Mass Communication & Journalism*, *5*(1), 1000288. https://doi.org/10.4172/2165-7912.1000288

Aldhafferi, N., Watson, C., & Sajeev, A. (2013). Personal information privacy settings of online social networks and their suitability for mobile internet devices. *International Journal of Security, Privacy and Trust Management*, *2*(2), 1–17. https://doi.org/10.5121/ijsptm.2013.2201

Al-Enezi, K. A., Al Shaikhli, I. F. T., & AlDabbagh, S. S. M. (2018). The influence of internet and social media on purchasing decisions in Kuwait. *Indonesian Journal of Electrical Engineering and Computer Science*, *10*(2), 792–797. https://doi.org/10.11591/ijeecs.v10.i2.pp792-797

Ali, A., Kamran, A., Ahmed, M., Raza, B., & Ilyas, M. (2019). Privacy concerns in online social networks: A users' perspective. *International Journal of Advanced Computer Science and Applications*, *10*(7). https://doi.org/10.14569/ijacsa.2019.0100780

Aljohani, M., Nisbet, A., & Blincoe, K. (2016b). A survey of social media users privacy settings & information disclosure. In M. Johnstone (Ed.), *The proceedings of 14th australian information security management conference* (pp. 67–75). Edith Cowan University.

Al-Kandari, A. A., Al-Sumait, F. Y., & Al-Hunaiyyan, A. (2017). Looking perfect: Instagram use in a Kuwaiti cultural context. *Journal of International and Intercultural Communication*, *10*(4), 273–290. https://doi.org/10.1080/17513057.2017.1281430

Al-Rahmi, W., & Othman, M. (2013). The impact of social media use on academic performance among university students: A pilot study. *Journal of Information Systems Research and Innovation*, *4*, 1–10.

Aloudat, A., Al-Shamaileh, O., & Michael, K. (2019). Why some people do not use facebook? *Social Network Analysis and Mining*, *9*(1), 19. https://doi.org/10.1007/s13278-019-0564-z

AlSagri, H. S., & AlAboodi, S. S. (2015). Privacy awareness of online social networking in Saudi Arabia. In *2015 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1–6). IEEE.

Alsurehi, H. A., & Al Youbi, A. A. (2014). Towards applying social networking in higher education: Case study of Saudi universities. *MAGNT Research Report*, *2*(4), 217–231. https://doi.org/14.9831/1444-8939.2014/2-4/MAGNT.29

Ampong, G. O. A., Mensah, A., Adu, A. S. Y., Addae, J. A., Omoregie, O. K., & Ofori, K. S. (2018). Examining self-disclosure on social networking sites: A flow theory and privacy perspective. *Behavioral Sciences (Basel, Switzerland)*, *8*(6), 58. https://doi.org/10.3390/bs8060058

Andrews, D., Nonnecke, B., & Preece, J. (2003). Electronic survey methodology: A case study in reaching hard-to-involve internet users. *International Journal of Human-Computer Interaction*, *16*(2), 185–210. https://doi.org/10.1207/s15327590ijhc1602_04

Arab Times Cybercrime. (2020). *Kuwait hit by 1,305 cyber-attacks tied to COVID-19 during H1 of '2011/10/2020*. Retrieved from https://www.arabtimesonline.com/news/kuwait-hit-by-1305-cyber-attacks-tied-to-covid-19-during-h1-of-20/

Asbury, T. (2018). Online interactions: Comparing self-disclosure and self-presentation between friendship and dating. *Psychology and Behavioral Science International Journal*, *9*(3), 555761. https://doi.org/10.19080/pbsij.2018.09.555761

Body, D. M., & Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Cañares, M. (2018). *Teenage clicks: Can teens protect their privacy on social media? World wide web foundation*. Retrieved from https://webfoundation.org/2018/09/teenage-clicks-

Choi, Tae & Sung, Yongjun. (2018). Instagram versus Snapchat: Self-expression and privacy concern on social media. Telematics and Informatics. 35. Doi: 10.1016/j.tele.2018.09.009.

Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. Sage Publications.

Din, I., Islam, N., Rodrigues, J., & Guizani, M. (2018). Privacy and security issues in online social networks. *Future Internet*, *10*(12), 114. https://doi.org/10.3390/fi10120114

Gaál, Z., Szabó, L., Obermayer, N., & Csepregi, A. (2015). Exploring the role of social media in knowledge sharing. *The Electronic Journal of Knowledge Management*, *13*, 185–197.

Grabner-Kräuter, S., & Bitter, S. (2013). Trust in online social networks: A multifaceted perspective. *Forum for Social Economics*, *44*(1), 48–68. https://doi.org/10.1080/07360932.2013.781517

Gruzd, A., & Hernández-García, Á. (2018). Privacy concerns and self-disclosure in private and public uses of social media. *Cyberpsychology, Behavior and Social Networking*, *21*(7), 418–428. https://doi.org/10.1089/cyber.2017.0709

Håkansson, P., & Witmer, H. (2015). Social media and trust — a systematic literature review. *Journal of Business and Economics*, *6*(3), 517–524. https://doi.org/10.15341/jbe(2155-7950)/03.06.2015/010

Hamade, S. N. (2013). Perception and use of social networking sites among university students. *Library Review*, *62*(6/7), 388–397. https://doi.org/10.1108/lr-12-2012-0131

Hazari, S., & Brown, C. (2014). An empirical investigation of privacy awareness and concerns on social networking sites. *Journal of Information Privacy and Security*, *9*(4), 31–51. https://doi.org/10.1080/15536548.2013.10845689

Herring, S., & Kapidzic, S. (2015). Teens, gender, and self-presentation in social media. In S. Herring & S. Kapidzic (Eds.), *International encyclopedia of the social & behavioral sciences* (pp. 146–152). Elsevier.

Idemudia, E., Raisinghani, M., Adeola, O., & Achebo, N. (2017). The effects of gender on social media adoption the effects of gender on the adoption of social media: An empirical investigation. In *23rd Americas conference on information systems* (pp. 1–11). AMCIS.

Kemp, S. (2020). *Digital 2020: Global digital overview*. Retrieved from https://datareportal.com/reports/digital-2020-global-digital-overview

Kim, B., Shin, K. S., & Chai, S. (2015). How people disclose themselves differently according to the strength of relationship in SNS? *Journal of Applied Business Research (JABR)*, *31*(6), 2139–2146. https://doi.org/10.19030/jabr.v31i6.9472

Kim, H. J., Kim, M. A., Kim, H. L., Choi, D. J., Han, S., Jeon, E. S., Cho, M. C., Kim, J. J., Yoo, B. S., Shin, M. S., Kang, S. M., & Chae, S. C. (2020). Gender difference in the impact of ischaemic heart disease on heart failure. *European Journal of Clinical Investigation*, *50*(5), e13232. https://doi.org/10.1111/eci.13232

Kisilevich, Slava & Mansmann, Florian. (2010). Analysis of Privacy in Online Social Networks of Runet. Proceedings of the 3rd International Conference of Security of Information and Networks / ed. by Oleg Makarevich. New York, NY : ACM, 2010, pp. 46-55.doi 10.1145/1854099.1854112.

Koranteng, F. N., Wiafe, I., Katsriku, F. A., & Apau, R. (2019). Understanding trust on social networking sites .among tertiary students: An empirical study in Ghana. *Applied Computing and Informatics*. https://doi.org/10.1016/j.aci.2019.07.003

Kuczerawy, A., & Coudert, F. (2010). Privacy settings in social networking sites: Is it fair? *IFIP Advances in Information and Communication Technology*, *352*, 231–243. https://doi.org/10.1007/978-3-642-20769-3_19

Kuo, T. (2015). Gender differences in factbook's privacy settings. *Issues in Information Systems*, *16*(1), 149–154. https://doi.org/10.48009/1_iss_2015-149-154

Lee, W., Zankl, W., & Chang, H. (2016). An ethical approach to data privacy protection. *ISACA Journal*, *6*(1), 1–9.

Leedy, P. and Ormrod, J. (2001) Practical Research: Planning and Design. 7th Edition, Merrill Prentice Hall and SAGE Publications, Upper Saddle River, NJ and Thousand Oaks, CA.

Lohar, Pintu, Xie, Guodong, Bendechache, Malika , Brennan, Rob , Celeste, Edoardo, Trestian, Ramona &Tal, Irina (2021) Irish attitudes to privacy in COVID-19 times: sentiment analysis on Twitter and survey data. In: 16th International ARES Conference on

Availability, Reliability and Security ARES21, 17- 21 Aug 2021, Vienna, Austria + Online. ISBN 978-1-4503-9051-4

Lo, J. (2010). Privacy concern, locus of control, and salience in a trust-risk model of information disclosure on social networking sites. In *Proceedings of the 16th Americas conference on information systems.* Paper 110 (pp. 1–13). AMCIS.

Long, M., & Robinson, P. (1998). Focus on form: Theory, research and practice. In C. Doughty, & J. Williams (Eds.), Focus on form in classroom second language acquisition. Cambridge, UK: Cambridge University Press.

Magolis, D., & Briggs, A. (2016). A phenomenological investigation of social networking privacy awareness through a media literacy lens. *Journal of Media Literacy Education*, *8*(2), 22–34.

Michota, A. K., & Katsikas, S. K. (2018). Towards improving existing online social networks' privacy policies. *International Journal of Information Privacy, Security and Integrity*, *3*(3), 209–229. https://doi.org/10.1504/ijipsi.2018.10013220

Moreno-Becerra, T., Gajardo-León, C., & Parra-Ortiz, E. (2016). Privacy: how it is understood and managed on facebook. A case study of young Chileans. *Revisit Latina de Communication Social*, *71*, 715–729. https://doi.org/10.4185/RLCS-2016-1117.

Muñoz, L. A., & Bolívar, M. P. R. (2015). Theoretical support for social media research. A scientometric analysis. In E. Tambouris, M. Janssen, H. J. Scholl, M. A. Wimmer, K. Tarabanis, M. Gascó, B. Klievink, I. Lindgren, & P. Parycek (Eds.), *Electronic government* (pp. 59–75). Springer International Publishing..

OECD (2020), Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides, Digital Economy Outlook 2020 Supplement, OECD, Paris, www.oecd.org/digital/digital-economy-outlook-covid.pdf.

Pensa, G., Ruggero. (2018). Enhancing privacy awareness in online social networks: A knowledge-driven approach. In *Proceedings of the CIKM 2018 workshops co-located with 27th ACM international conference on information and knowledge management (CIKM 2018)* (pp. 1–2). CEUR-WS.

Peterson K., Siek K.A. (2009) Analysis of Information Disclosure on a Social Networking Site. In: Ozok A.A., Zaphiris P. (eds) Online Communities and Social Computing. OCSC 2009. Lecture Notes in Computer Science, vol 5621. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-02774-1_28.

Pew Research Centre. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Retrieved from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Rafique, G. (2017). Personal information sharing behavior of university students via online social networks. *Library Philosophy and Practice*, *2017*(1), 1454

Rao, A., Schaub, F., &Sadeh, N. (2014). "What do they know about me? Contents and concerns of online behavioral profiles," in Proceedings of the Sixth ASE International Conference on Privacy, Security, Risk and Trust (Greensboro, NC)

Rollero, C., Daniele, A., & Tartaglia, S. (2019). Do men post and women view? The role of gender, personality and emotions in online social activity. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *13*(1), 1. https://doi.org/10.5817/cp2019-1-1

Rowley, J., Johnson, F., & Sbaffi, L. (2016). Gender as an influencer of online health information-seeking and evaluation behavior. *Journal of the Association for Information Science and Technology*, *68*(1), 36–47. https://doi.org/10.1002/asi.23597

Salih, A., & Mohammed, A. (2018). Students attitude towards the use of social media for learning purposes. *Journal of Literature, Languages and Linguistics (Case Study: Al-Baha University, College of Sciences & Arts- Biljurashi)*, *50*, 31–36.

Sarikakis, K., & Winter, L. (2017). Social media users' legal consciousness about privacy. *Social Media Society*, *3*(1), 205630511769532. https://doi.org/10.1177/2056305117695325

Shabnoor, S., & Tajinder, S. (2016). Social media its impact with positive and negative aspects. *International Journal of Computer Applications Technology and Research*, *5*(2), 71–75. https://doi.org/10.7753/ijcatr0502.1006

Sharif, A., Soroya, S. H., Ahmad, S., & Mahmood, K. (2021). Antecedents of self-disclosure on social networking sites (SNSs): A study of facebook users. *Sustainability*, *13*(3), 1220. https://doi.org/10.3390/su13031220.

Sonja Grabner-Kräuter & Sofie Bitter (2015) Trust in online social networks: A multifaceted perspective, Forum for Social Economics, 44:1, 48-68, DOI: 10.1080/07360932.2013.781517.

State of Kuwait, Ministry of Interior.(2016) Cybercrime Legislation No. 63..Retrieved from https://www.moi.gov.kw/main/content/docs/cybercrime/ar/law-establishing-cyber-crime-dept.pdf

Tatjana, T., Aristodemou, E., Shitta, G., Laouris, Y., & Arsoy, A. (2010). Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook profiles as an example. *International Journal of Media & Cultural Politics*, *6*(1), 81–101. https://doi.org/10.1386/macp.6.1.81/1

Tessem, B., & Nyre, L. (2013). The influence of social media use on willingness to share location information. In S. Furnell, C. Lambrinoudakis, & J. Lopez (Eds.), *Trust, privacy, and security in digital business* (pp. 161–172). Springer.

The Office of the Privacy Commissioner of Canada. (2014). *Privacy and cyber security: Emphasizing privacy protection in cyber security activities*. Retrieved from https://www.mccarthy.ca/en/insights/blogs/consumer-markets-perspectives/privacy-and-cyber-security-summary-report-privacy-commissioner-canada.

Trepte, Sabine & Teutsch, Doris., Masur, Philipp K. & Eichler, C., Fischer, Mona., Hennhöfer, Alisa & Lind, Fabienne. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). 10.1007/978-94-017-9385-8.

Tuunainen, V. K., Pitkänen, O., & Hovi, M. (2009). Users' awareness of privacy on online social networking sites –case facebook. In *BLED 2009 proceedings.* Paper 42 (pp. 1–17). BLED.

van den Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2019). Privacy and information technology. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy*. Stanford University.

Waldman, A. E. (2016). Privacy, sharing, and trust: The facebook study. *Case Western Reserve Law Review*, *67*(1), 193.

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review*, *31*(5), 618–627. https://doi.org/10.1016/j.clsr.2015.07.002

Yang, H. (2013). Young American consumers' online privacy concerns, trust, risk, social media use, and regulatory support. *Journal of New Communications Research*, *5*, 1–30.

Zheleva, E., Terzi, E., & Getoor, L. (2012). Privacy in social networks. *Synthesis Lectures on Data Mining and Knowledge Discovery*, *3*(1), 1–85. https://doi.org/10.2200/s00408ed1v01y201203dmk004

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. Security and Communication Networks, 7(12), 2728–2742. doi:10.1002/sec.795