Strategies Needed by Social Network Builders to Develop Information Privacy

Anas Azzouz
a.azzouz@my.denver.coloradotech.edu

Samuel Sambasivam
ssambasivam@coloradotech.edu

Department of Computer Science
Colorado Technical University
Aurora, Colorado 80014, USA

Abstract

This research intends to examine the strategies that social network builders are looking for to develop information privacy-approved social networks. The research methodology chosen for this study is a qualitative exploratory approach. Face-to face interviews were conducted to obtain valuable information that answers the research question. The researcher interviewed ten IT professionals who build social network platforms and applications using six open-ended questions. This study identified eight critical themes related to developing information privacy. The researcher performed a line-by-line analysis of participants' responses using NVivo 12 Pro Software. The outcomes of this empirical study may provide insights for social network builders on how to implement information privacy for social network platforms and applications. This research would help social network builders and providers to focus on the mandatory steps to develop information privacy.

Keywords: social network platforms and applications, social network builders, social network providers, information privacy, social network privacy.

1. INTRODUCTION

Research has shown that Social Network Builders need strategies to develop information privacy for social networks (Dwyer, Hiltz, & Passerini, 2007). Maintaining personal information privacy has become a challenge for social network providers to protect data and personal information. Social network providers have developed several approaches that reduce the risks to the customers' privacy (Tucker, 2014). Jeong & Kim (2017) reported that social networking platform users are concerned about various online content. They found that different content within different posting types has various privacy implications. Posting personal information on social networks can present several risks to the end-users. Social Network developers are looking for strategies that will protect users' privacy for a variety of software applications. One of the risks in dealing with personal information on social networks is obtaining detailed personal information by hackers or insiders (Aldhafferi,

Watson, & Sajeev, 2013). As a result, using sensitive personal information may lead to financial and terrorism risks, and possibly physical extortion (Gharibi & Shaabi, 2012). There has also been an evolution in social networking platform privacy features to become a significant concern for both businesses and personal users (Kumar, Kumar, & Bhasker, 2018). One of the issues that present privacy challenges with social media sites and applications is direct online communications in our lives.

2. LITERATURE

This literature review reveals the research gap in the existing body of knowledge and substantiates the presence of research problem in the area of exploring strategies social network builders need to develop information privacy-approved social networks (Golafshani, 2003). Social network services involved sharing various types of data among users online. The biggest challenge that all users face with these

services is their privacy (Such & Rovatsos, 2016). The privacy control and management are fundamental factors to success online, but most of the social network users are not socially aware (Misra & Such, 2016). Users enjoy sharing information online, this process of sharing information and data requires security and privacy to keep users' information private (Kumar, Sarvanakumar, & Deepa, 2016). It is mandatory that social network providers keep their user's information private and it is also required that all uses change their privacy settings (De & Imine, 2018). One of the latest online communication tools is a social networking site that permits users to interact with people and create a network with a public or a private profile (Osterrieder, 2013). Social media contains blogs, wikis, media (including audio, photo, video, and text), sharing tools, networking platforms, and virtual worlds (Boyd & Ellison, 2007). In the past few years, social media expanded the breadth of its applications in academia and personal realms. Social media users play a significant role in increasing interpersonal engagement outside of the classroom. They are generating innovative approaches like creating study groups and pages for virtual conference groups to increase their knowledge of specific subjects in their respective fields. Social media has benefits in communication and interaction with friends and peers; it assumes a prominent role in everyday lives. Subsequently, researchers attempt to understand the effects of social media and social networking sites on students. They are also challenged to pursue a comprehensive investigation in the field of education (Bynum, 2011; Gachago & Ivala, 2012).

(1) Social Media History

Kaplan and Haenlein (2010) stated that Truscott and Ellis developed the Usenet in 1979. Truscott and Ellis used it as an application for international conferencing that let online users create entries on their public page. Approximately 20 years before this development, the rise of social media began when Bruce Susan Abelson started "Open Diary," which is a social media website that gathered together diary writers into one group (Pezzola, 2013). Thereafter, "weblog" was shortened into the term "blog." One user changed the word "weblog" into two words "we blog" (Kaplan & Haenlein, 2010).

Social Media is a new term used to describe many online technologies that promote social networking sites as a way to communicate and share ideas and comments with others (Dabbagh & Reo, 2011). Developers in 1995 published a website called "classmates.com." as the first ever networking site. In 1997, another site was published which was named

"sixdegrees.com." Shortly after that, with the help of the efficient Internet, sites including MySpace (2003) and Facebook (2004) were launched. This event made "social media" even more popular among people. Virtual Worlds are online environments that also emphasize the use of the Internet and social media in the first world countries (Kaplan & Haenlein, 2010).

Until developers published MySpace in 2003, there has been a significant gap in social media websites (Rennie & Morrison, 2013). In 2004, "Facebook" was published and became immediately popular. These two social media websites made a massive impact on social, political and economic views worldwide. During 2006, MySpace reached over 110 million users. A few years later, in 2008, Facebook's statistics for active online users reached 110 million worldwide (Leonardi, Huysman, & Steinfield, 2013).

Improvements in technology have caused the number of users on social media to increase continuously for the past decade (Perrin, 2015). The use of social media depicts the relationships between people and how the communication takes place between them. As stated by Heidemann, Klier, and Probst (2012), social media sites are online communities that help individuals to create relationships and bond with each other. Therefore, social networking sites facilitate the process of how people find others who have similar interests. It helps sustain and uphold their relationships and allows people to find resources and knowledge (Heidemann et al., 2012). Social media has become mainstream and has increasingly attracted research (Tsiotsou, 2015). Social media technology allows the individual to develop network contacts further for business, pleasure, and communication (Nadkarni & Hofmann, 2012).

(2) Social Media Technology

In the Information Age, social media is considered a big part of the Internet industry, which attracts individuals of all age groups (Fuchs, 2017). Napoleon (2016) expressed his opinion that social networking sites are a group of Internet-based applications that combine to become the technological and ideological base of the web and allow the design and exchange of user data. Users utilize social networking platforms and apps for a variety of purposes. A study by Perrin (2015) found that women are more likely than men to use social networking platforms and apps. Goodmon, Smith, Ivancevich, & Lundberg (2014) characterized social media technology (SMT) as network sites and apps that let individuals and companies make, take part in and communicate ideas or current content in many forms of disclosure in online communities. Social media functions in a

web environment that encourages individuals to communicate with each other (Wallace, 2015). Users of the web can build and maintain a profile, input opinions on public posts, as well as interact with each other. The use of technology in public and academic environments has dramatically increased in recent years (National Science Board, 2016). The most important reason for its popularity is the widespread use of social media; it is a quick and effective way of communicating with others (Sánchez, Cortijo, & Javed, 2014).

(3) Social Networks
1. Twitter

Twitter is a social media tool introduced during Web 2.0 that allows users to publish information like podcasts, photos, and other information (Murthy, 2018). In 2006, Twitter began as a relatively unknown website called www.twitter.com. Jack Dorsey designed an SMS-based platform used as a high-level, instantaneous communication tool (MacArthur, 2017). Odeo Company gave him a chance to go ahead with his project and develop it. The first message ever sent on Twitter was by the founder Dorsey, and the content of it was "just setting up my twttr" on March 21, 2006 (MacArthur, 2017). Users had some issues with Twitter especially its limitation of only 140 characters to Tweet or reply to others, including private messages (MacArthur, 2017). The reason behind the limited number of 140 characters is the design of Twitter as an SMS-communication platform on mobile devices. Later in 2017, the company decided to double the characters to 280, so users would feel comfortable with the service (MacArthur, 2017). Users were using a special symbol like @ before their names to identify other users within a Tweet. It was a brilliant way that users use in Twitter (Murthy, 2017). The Twitter team added this functionality to the platform in addition to hashtags. Now both @-symbol and hashtags are an integral part of the Twitter ecosystem.

About 8% of Twitter members are between 12 and 17 years old, while about 66% are adults (Kaplan & Haenlein, 2010). About 62% use it for news and politics. Females and older teens are more likely to use this application rather than other social media. Instagram is also a social media application that is currently popular amongst people who enjoy spreading photos and videos with friends and family (Kaplan & Haenlein, 2010). Schwartz et al. (2013) wrote an algorithm that helps social network builders identify users' ages in social network platforms. This approach identifies words and phrases characteristic of particular age groups by taking the language used by users and classifying the words to identify users' age groups (Schwartz et al., 2013).

2. Facebook

Facebook was founded in 2004 by a group of students at Harvard University by Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz, and Chris Hughes (Hall, 2018). Using Facebook social networking services is free, and the company makes money from advertisements on its website. The first version of the current Facebook registered under the name "http://www.theFacebook.com" in 2004 (Hall, 2018). The number of users increased by June 2004 to reach 250,000 students from 34 different schools (Hall, 2018). Facebook is a powerful tool for politics, and the first use was in 2008 by both the Democratic and Republican parties. About 1,000 groups showed up on Facebook to support the candidates (Hall, 2018). Facebook is an excellent tool for collaborative and constructive learning. Most of the users do not participate in Facebook for posting photographs and use it to share academic information.

Students take advantage of the benefits of social media websites to interact with others to get better resources for their academic work (González-Ramírez, Gascó, & Llopis Taverner, 2015). The Facebook phenomenon hit many countries around the world, and Malaysia was one of them. It is the fifth country in the numbers of people who create Facebook accounts (Ainin, Naqshbandi, Moghavvemi, & Jaafar, 2015). Students use this social networking service for activities like learning and socializing (Ainin et al., 2015). This platform provides different methods for students to communicate with each other. For instance, with Facebook groups, learners can join with similar groups of people from the entire world with the same interest. By providing various services to all users, students can educate themselves live-time. The essential advantages of using Facebook as a learning tool are its communication features and universal participation.

However, there are some drawbacks of using Facebook as a teaching tool (Roeber et al., 2015). The most significant cons are privacy and time. Most students think about the privacy of mixing their personal life and academic work online using Facebook. It is challenging for social media users to set up boundaries between private life and school work. In a study by Roeber et al. (2015), they found most students use Facebook as a teaching tool. On the other hand, but they also found some students preferred not to use it for several reasons like privacy, or they do not like non-friends to follow them, or they do not like to use

it in an educational field. Additionally, *Facebook* is very commonly used by college students in the United States, most likely since *Facebook* was founded to encourage and bring together individuals attending school (Tao, 2014). On this website, there are many ways users can interact with others, which is why it is so popular (Yang & brown, 2013). In 2004, Mark Zuckerberg, a 19-year-old student at Harvard University, published the social media icon known as *Facebook*. The first day the site was launched, over 1,200 of his fellow students were registered, by the first month over half of the students at Harvard University were connecting on to this site (Hollenbaugh & Ferris, 2014). After a short period, the website became the second largest Internet site in the world, behind Google.

(4) The Importance of Privacy of Social Media

In the US, the privacy of social media has been used continuously as a way to promote education and other useful resources, such as current event news since 2007 (Junco & Cotton, 2012). Many companies and universities have used social media to promote knowledge and marketing strategies. These academic institutions use social media platforms such as Facebook, YouTube, and Flicker to interact and share academic information with students and professors. These institutions use YouTube videos, e-journals, and documents that can be downloaded as a way to share and virtually teach students information (Guraya, 2016).

Social media platforms have also acquired a way for subscribers to share their feedback (Fox & Moreland, 2015). The use of social media in academic institutions has brought significant changes in privacy strategies, so students can work their education assignments comfortably and understand that the protection of their information is important (Sobaih, Moustafa, Ghandforoush, & Khan, 2016). As a result, universities can use social media to build school websites, which have the purpose to encourage students to use it as an educational tool (Junco & Cotton, 2012).

Research has shown that universities have given more emphasis to social media platforms such as virtual classrooms and teaching through podcasts and YouTube videos (Master, Cheryan, & Meltzoff, 2016). As an example, Ball State University created an online platform for students who are interested in writing and publishing articles and creating discussions through the Internet. With this type of online learning platforms, students prefer to use social network websites and applications as a primary source of information (Gagnon, 2015).

(5) Social Network Privacy

Participation in social networks services (SNSs) has increased in recent years (Hajli & Lin, 2016). Different applications such as Facebook or Friendster that allow users to create online profiles and share information among friends are enjoying more popularity than ever (Acquisti & Gross, 2006). The relation between privacy and social networks therefore needs to be scrutinized carefully. Users normally want to share their information only with a select group of people, and not all users on the network. Social network users should be willing to share some personal information with strangers, but not to the people they do not know well (Acquisti & Gross, 2006).

The number of online social networks (OSNs) is increasing daily (Acquisti & Fong, 2015). Millions of users are joining together on various platforms, and the objective is to build a foundation of trust to keep those users' information private. Privacy problems is a deterrent to users of SNSs, and they are worried that their personal information will be shared with others (Bibi, Hussain, Khan, & Maqsood, 2017). The study by Kayes and Iamnitchi (2017) found that there is a relation between privacy and security and they cannot be separated.

As an example, Facebook had about 2.20 billion active users in 2018 (Zephoria Digital Marketing, 2018). This number has increased by about 13% annually. Over one billion users access Facebook on mobile devices and this number increases by 23% yearly. Twitter is another SNS platform, and its number of active users as of 2018 is 330 million accounts. Eighty percent of Twitter users use mobile devices to access their accounts (Aslam, 2018a).

Privacy and security goals are the same, but there are some cases where they may conflict and cause serious issues (Acquisti & Fong, 2015). Students want privacy when they log into online social network services (OSNs). Others wish to increase their privacy by protecting their information from anonymous viewers (Kayes & Iamnitchi, 2017). Users provide an important factor in online social networks services (OSNs) to initiate online privacy initiatives. However, some users do not have an awareness of the risks of sharing personal data on social networking platforms. While social networking sites allow participants to modify their privacy settings, the researchers observe that most users do not activate these options and encounter frustration as a result (Pensa & Di Blasi, 2017).

(6) Social Network Platform Builders

Social network software builders should understand users' privacy concerns (Acquisti & Fong, 2015). Privacy issues have produced serious concerns. Literature by Islam, Watson, Iannella, & Geva (2017) used a mixed method (qualitative and quantitative) to explore privacy requirements. In the study by Islam et al., 2017, the researchers used users' privacy concerns like accountability, visibility, or transparency to integrate privacy requirements. Another study produced six essential privacy requirements that social network builders should pay attention to while designing or developing applications. The six requirements are the relationship between privacy concerns information access, information sharing, information deletion, information re-use, information alerting, and information control self-disclosure based on privacy calculus method (Culnan & Armstrong, 1999; Dinev et al., 2006).

6. Social Network Theory of Privacy

Strahilevitz (2005) wrote a universally accepted theory about privacy in social networks called, "A Social Networks Theory of Privacy." According to this theory, researchers used social networks as a tool that helps parties understand privacy issues in legal cases. A separate study by Borgatti et al. (2018) showed how the information on the network flows from one place to another, and should inform users' expectations about privacy revealed in the network. Acquisti and Gross (2006) conducted a study about social networking privacy among students at Carnegie Mellon University (CMU) and found that most of the students were willing to provide and share excessive amounts of personal information on online social networks. The researchers found that a small number of students changed their privacy settings to reduce the sharing of personal information. Researchers found that it was easy for users to upload their personal information or comment on social networking, but later the researchers regretted this decision to upload their personal information (Abdulhamid, Ahmad, Waziri, & Jibril, 2014). From a security perspective, the researchers found that the fundamental weakness of social networking sites is personal information privacy. Most SNSs users are not aware of this issue and continue to share critical information online with others (Abdulhamid et al., 2014).

3. RESEARCH FRAMEWORK

A conceptual framework is an essential tool for any research (Litosseliti, 2018). It includes the logical perception that relates to how the researcher think about the relationships between theoretical concepts, topics of interest in literature, the researcher's assumption, and the research question. It shows how ideas of our research are connected (Maxwell, 2012). It illustrates to the reader the researcher's epistemology and ontological worldview and the research's methodology. Based on the methodology chosen for the study, the researcher is able to determine the framework of the research through the study's conceptual framework, since it shows the relationships between theoretical concepts, topics, assumptions, and the research question. Using literature review information, the researcher is thus able to create a solid conceptual framework for the study (Greene, Caracelli, & Graham,1989).

The narrative framework of the research starts with the following topics: social media purpose, information privacy concern, social networking usage, and social networking privacy. This design guides the researcher into how to think about the strategies that needed by the social network builders to develop information privacy-approved social networks. The graphic below presents the conceptual framework.

(FIGURE 1 - Appendix)

4. RESEARCH METHOD

The problem addressed in the proposed study was the strategies social network builders need to develop information privacy-approved social networks have not been established (Kokolakis, 2017). The purpose of the proposed qualitative exploratory study was to explore the strategies social network builders need to develop information privacy-approved social networks. The vulnerability of privacy features of social networking platforms has evolved as a significant concern for both businesses and users (Kumar et al., 2018). Social media sites and applications stand out at the forefront of mobile apps as determinants of frequented communications for users. Social networking builders are not entirely socially aware of privacy problems, even when confidentiality is a fundamental factor to success (Misra & Such, 2016). As a result, software designers must respond to the demands to develop and design more security mechanisms that increase privacy for online social networks.

The research question is: What are the strategies social network builders need to develop information privacy-approved social networks? The research design for this study used a qualitative approach, which also incorporates an exploratory method. The

researcher investigated the study participants' opinions about social network builder strategies and social network privacy (Creswell, 2009). In this study, the researcher used exploratory qualitative research to obtain valuable information from IT experts. The researcher interviewed study participants, asking about their opinions and ideas about social network builder strategies and social network privacy (Creswell, 2009). Edmondson and McManus (2007) found that there are three categories of research: mature, intermediate, or nascent. Mature research provides well-developed concepts and models that already researched in the past. Intermediate research proposed relationships between established and new research (nascent) (Edmondson & McManus, 2007). The researcher should understand which method applies to the research, as delineated below.

Using the methodological fit from Edmondson and McManus (2007), this research study falls within the area of nascent research. It is nascent because there is a marked lack of studies on social network builders who are employing knowledge-sharing to develop privacy in social networking platforms. Researchers have conducted few studies that explore the advantages and disadvantages of using social networking platforms (Panahi, Watson, & Partridge, 2016). Researchers have not conducted any research investigating the strategies needed by social network builders to develop information privacy-approved social networks. An exploratory qualitative approach provides a necessary framework to guide this research project because researchers know little about the strategies needed by social network builders to develop privacy (Maxwell, 2012). The qualitative method answers the research question thoroughly and comprehensively (Creswell, 2018). This study explored the strategies needed by the social network builders to develop information privacy-approved social networks. The researcher selected professionals who can best inform the research question based on specific recruitment criteria (Kuper, Lingard, & Levinson, 2008). The researcher used specific recruitment criteria that included the following for study participants: (a) experience in software developing of more than ten years; (b) IT professionals who use Social Networking Services; (c) employees who successfully passed security and awareness training; (d) employees who have experience in privacy policies; and (e) either male and female. These criteria above helped the researcher obtain valuable information that helps answer the research question.

5. DATA ANALYSIS

The researcher used NVivo 12 Pro to code the data for themes and patterns to explore the strategies needed by social network builders. The initial task of the interpretation was to organize the collected data in order to discover the appropriate information; this helped in revealing clarifying examples and interview data (Wilson, 2013). The process of data analysis started by looking for specific words that relate to the interview questions. The data analysis approach for the qualitative method included: (a) collecting data from interviews; (b) organizing the data; (c) coding; (d), identifying themes (Creswell & Clark, 2017). The coding process included looking for similar words, phrases, and sentences to create a pattern or keyword (Saldaña, 2015). According to Creswell (2018), coding was used to make logic and sense of the interview responses and helped to identify themes with the categories of the codes. The primary task when the researcher wants to conduct qualitative research was theme identification. The gathered themes from NVivo Software provided the researcher with an insight into the participants' opinions and experiences (Bryman, 2012). For transcript accuracy, the researcher read and verified them by comparing them to the digital recordings. The researcher reviewed all transcripts multiple times to detect the keywords within the data (Saldaña, 2015). NVivo coding consists of five steps: (a) conduct data cleaning; (b) upload the data into the software; (c) reorganize the data; (d) conduct data exploration by using a query; and (e) start coding (Gibbs, 2018). This software provided the ability to organize the data into themes by the nodes (Zamawe, 2015). A node in NVivo software is a collection of references about a specific theme or area of interest. Nodes are essential in the software because they help the user to gather related materials or information in one place so that the researcher will have the ability to categorize emerging patterns and ideas (Zamawe, 2015). The software helped coding data into categories of words and phrases to detect themes (Zamawe, 2015). Coding data is the process by which researchers employ specialized software to process the inputted data and categorize them according to pre-established criteria (Glaser, 2017). Saldana (2011) established three methods of coding that would assist the researcher in identifying themes. The first method is initial coding; the researcher used this method to organize large groups of data into small groups. The second method is axial coding; the researcher can use it by organizing and potentially creating subcategories to facilitate a more precise presentation of data. The third approach is theoretical coding; which identifies

relationships between categories and organizes the categories in a manner that promotes the direction of the study. Once the researcher completed the interviews, the researcher began analyzing the data. The researcher colored each node that contained the keywords and the key phrases in the software to classify the data and create themes. This process helped the researcher to develop useful categories that process the information.

6. FINDINGS

The main aim of exploring the strategies that social network builders need is to provide privacy for all social network users. Users seek the protection of their data while using social networking services. Social network platform policies and strategies are aimed at securing data and reducing data theft. After interviewing the participants, the researcher came up with 6 themes as the following:

1. Steps to Build Social Network Platforms or Applications.
2. Software Development Lifecycle Steps.
3. Data Users Share and Transmit.
4. Important Training & Training Materials.
5. Privacy Factors & Privacy Process.
6. Data that Providers Collect from Users.

All respondents believed that they have to identify their audience or users before they start designing and coding. Also, the participants emphasized the software development lifecycle in theme two. These participants indicated that developing a social network platform or an application must follow the software development phases. Study participants showed that sharing data is one of the most featured and functions that social networking platforms and applications provide to all users. Respondents explained that without sharing data, users would stop using social networking platforms. Theme three covered the types of data that users can share and transmit through a social network platform or an application. However, theme eight deals with the data that the social network provides gather from users. Inclusively, study participants acknowledged that there are some necessary data that providers collect from users to allow the end user to access the service. Social network builders acknowledged that training is one of the most effective approaches to implement and improve privacy. Each training has different materials that help them to understand the security mechanism and intruders approaches to provide the total security system. Respondents in them four and five explained the essential training that social network

builders should receive. Participants on theme six and seven described the privacy factors and the privacy process. They have been framed to ensure the safety of users' data. Respondents mentioned that all users must change their privacy settings when they create social network accounts. Specific processes and strategies are necessary to maintain users' privacy and avert a chaotic situation. Strategies and processes are fundamental as they serve as the backbone to any social networking platform or application. Furthermore, these strategies and processes ensure that the platform or the application runs efficiently. Steps need to be taken to prevent loss of data and safeguard users' data.

7. LIMITATON OF THE STUDY

The first significant limitation was how to obtain reliable data from the participants. This limitation depended greatly on the participants' honesty or willingness to formulate responses that were straight-forward and not exaggerated or projected. In order to provide accurate results, the researcher must obtain reliable data from the participants. Eliciting reliable data means obtaining robust results and findings that lead to data-rich explanations (Golafshani, 2003). The second limitation was the amount of time allowed to perform data collection and analysis. The third limitation of this qualitative exploratory research study was the small sample size of 10 participants compared to the large population of social network builders (est.50, 000) in Denver, Colorado, metro area.

8. IMPLICATIONS OF STUDY AND RECOMMENDATIONS FOR FUTURE RESEARCH

This qualitative study explored effective strategies that social network builders need to develop information privacy-approved social networks. The study participants provided valuable data that described the key challenges for exploring appropriate strategies to develop privacy. Moreover, participants provided in-depth information from their professional and technical experiences, and team interaction in the process of building social network platforms and applications. This study revealed and highlighted critical areas of definition and improvement, which could be used as research data and proposes the following recommendations for subsequent research.

Recommendation 1
Dealing with users' information and data is a critical process in the social network world. This recommendation is for social network

providers. Training is a significant success for any organization. Having trained and skilled employees can make a big difference in securing social network platforms and applications. Proper training for all staff plays a significant role in implementing security and privacy. Investing in training supports information system security and improves the confidentiality, integrity, and availability (CIA). Creating a training program and not rely on the employee's experiences and certificates will enhance the cybersecurity and information privacy strategies. It is recommended to have a training program for all organizational staff four times a year. The training program should include the latest security technologies and modern approaches for software development. This recommendation concurs with other researchers who insist that HR or area supervisors screen candidates and oversee current employees to assure quality control of job performance. This finding is consistent with Gandy (1993), Graham and Wood (2003), Phillips (2004), Stalder (2002), Islam and Iannella (2011), and Islam (2014), who maintained that improving security is necessary to improve the security and the privacy of the social network platforms. They listed various privacy solutions for securing social network frameworks. Security and privacy training are one of the solutions users, and IT professionals should receive to be aware of the privacy issues.

Recommendation 2

The current privacy policy for social network platforms and applications is not clear for large numbers of users around the world. The researcher recommends that privacy policy cover all information that users are looking for, such as knowing what the providers do with users' information and data. Moreover, users have difficulties reading privacy policies because current privacy policies are too long and require at least 25-30 minutes to read. The location of the privacy policy is unknown to a large number of users. The researcher recommends that social network providers create a short privacy policy that meets users' requirements. Also, most social network providers place their policies in a difficult location that regular users cannot find. The researcher recommends that social network providers locate their policies in a convenient site that all users see and reach. This information corresponds to the research study by Schneier research (2010) who stated that the current design of social network platforms had become a centralized and integrated system that does not allow to all users to control their privacy settings. Also, this finding is consistent with the study by Williams (2009), who stated the current privacy settings were not robust and appropriate to protect user's

information and data. This recommendation is also consistent with Baek et al. (2014), who stated that achieving high-level social network platforms, privacy is provided after giving the users more control to change privacy settings. Baek et al. (2014) also provided another solution, which is to develop a new privacy policy that all users can easily access. Overall, the researcher recommends that all users change their privacy settings once they create accounts on social network platforms and applications.

Recommendation 3

Users of social network platforms create profiles and share data with others. Social network builders design these platforms and applications to satisfy users' needs and requirements. The researcher recommends that all users understand the dangers of sharing personal information online and do not wish to share their data with unknown people. Users should share their information only with specific groups of people, and not with all people on social network platforms or applications. Social network users share a variety of types of data, such as photos, videos, audio files, comments, opinions, names, numbers, email address, locations, links, and emoticons. Users should refrain from sharing personal information with strangers online because this information can be passed on illegally. Third-party companies, advertisers, and hackers are interested in users' data and may obtain large amounts of data daily. They make money by selling users' information and data to individuals and corporations. Unfortunately, some users ignore privacy settings and share personal information with strangers. Thereafter, they recognize that these strangers stole their data and passed it on to unauthorized people. This finding is consistent with the research of Acquisti and Gross (2006) who stated that sharing information is one of the services that social network platforms and applications offer to their users, but that it should be secure. They also examined that a large group of users are willing to share personal information with unknown people and demonstrate carelessness. Zyskind and Nathan (2015) reported that sensitive information should not be shared online in order to reduce privacy violations. Bibi et al. (2017) indicated that privacy issues start after sharing personal information with others and ignoring privacy settings. Literature by Kayes and Iamnitchi (2017) found that users increase their privacy by reducing the amount and type of personal information shared with anonymous users. A study by Abdulhamid et al. (2014) showed that users regretted sharing personal information with others because of the compromises of privacy. Another study by Parra-Arnau et al. (2017) stated that users who

share personal information are the most vulnerable users. In summary, users must develop a thorough understanding of the implications of sharing personal information with others.

9. CONCLUSON

The focus of this research study was to explore the strategies that social network builders need to develop information privacy-approved social networks. This study explored social network platforms and applications in order to develop a strategy that social network builders use to enhance social network platforms and applications security and privacy. The researcher used a qualitative exploratory approach and collected the data from ten participants using semi-structured interviews. This semi-structured interview consisted of 6 questions that addressed the research question. The researcher interviewed ten IT professionals to obtain valuable information that answers the research questions. This study required a review of current literature and used a qualitative approach to explore experts' perspectives, thoughts, and experiences to solve the problem of identifying the strategies social network builders need to develop information privacy-approved social network. The literature helped the researcher to identify any gaps in the body of knowledge. Literature collection began with a review of the introduction of social network services, followed by an explanation of the importance of privacy of social media, social network privacy, social network platform builders, and the theoretical framework obtained from the literature review. The researcher collected the interview data from ten participants who had significant experience in building social network platforms and applications. The data collecting process started with conducting face-to-face interviews by asking six open-ended questions to obtain answers that addressed the research question. For the data analysis, the researcher used NVivo 12 Pro Software. This investigation required uploading the recorded transcripts into NVivo 12 Pro Software and identified eight major themes. These themes included the following: Steps to Build Social Network Platforms or Applications; Software Development Lifecycle; Data Users Share and Transmit; Important Training; Training Materials; Privacy Factors; Privacy Process; and Data that Providers Collect from Users. Through the findings of the study, the researcher discovered practical strategies that social network builders need to develop information privacy platforms. The most significant outcomes of this study were identifying topics which led to developing the following recommendations: training is mandatory for all social network builders to develop information

privacy-approved social networks and sharing personal data among users should be reduced. The researcher also recommends that future researchers should conduct studies using different research methods such as mixed-method or quantitative method. Also, future studies should include research privacy using third-party security and privacy services to measure the current privacy in social network platforms. Finally, the researcher recommends that future studies should focus on protecting big data and cloud services used in social network platforms and explaining the process of protecting the users' data and privacy.

10. REFERENCES

Abdulhamid, S. M., Ahmad, S., Waziri, V. O., & Jibril, F. N. (2014). *Privacy and national security issues in social networks: the challenges. arXiv preprint arXiv:1402.3301* .

Acquisti, A., & Fong, C. M. (2015). *An experiment in hiring discrimination via online social networks.*

Acquisti, A., & Gross, R. (2006). Imagined communities: *Awareness, information sharing, and privacy on the Facebook*. Paper presented at the International workshop on privacy enhancing technologies.

Ainin, S., Naqshbandi, M. M., Moghavvemi, S., & Jaafar, N. I. (2015). *Facebook usage, socialization and academic performance. Computers & Education, 83*, 64-73.

Aldhafferi, N., Watson, C., & Sajeev, A. (2013). *Personal information privacy settings of online social networks and their suitability for mobile internet devices*. *arXiv preprint arXiv:1305.2770*.

Aslam, S. (2018a). Twitter by the Numbers: Stats. *Demographics & Fun Facts*. [*(accessed on 19 September 2017)*].

Baek, Y. M., Kim, E.-m., & Bae, Y. (2014). *My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns.* Computers in Human Behavior, 31, 48-56.

Bibi, A., Hussain, Z., Khan, F., & Maqsood, A. (2017, January). *Quantitative evaluation of Security and Privacy perceptions in online social networks: A case study*. In Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on (pp. 425-433). IEEE.

Borgatti, S. P., Everett, M. G., & Johnson, J. C. (2018). *Analyzing social networks*. Sage.

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210-230. doi:10.1111/j.1083-6101.2007.00393.x

Bryman, A. (2012). Sampling in qualitative research. Social research methods, 4, 415-429.

Bynum, S. L. (2011). Utilizing Social Media to Increase Student Engagement: A Study of Kern County Public Schools. *Online Submission*.

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research*: Sage publications.

Creswell, J. W. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches*. Thousand Oaks: Sage.

Creswell, W. J. (2009). *Qualitative, Quantitative, and Mixed Methods Approaches* (Research Design).

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science, 10*(1), 104-115. doi:10.1287/orsc.10.1.104

Dabbagh, N., & Reo, R. (2011). Impact of Web 2.0 on Higher Education. *Technology Integration in Higher Education*, 174-187. doi:10.4018/978-1-60960-147-8.ch013

De, S. J., & Imine, A. (2018, April). To reveal or not to reveal: balancing user-centric social benefit and privacy in online social networks. In Proceedings of the 33rd Annual ACM Symposium on Applied Computing (pp. 1157-1164). ACM.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce–a study of Italy and the United States. *European Journal of Information Systems, 15*(4), 389-402.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, 339.

Edmondson, A. C., & McManus, S. E. (2007). Methodological fit in management field research. *Academy of management review, 32*(4), 1246-1264.

Fox, J., & Moreland, J. J. (2015). The dark side of social networking sites: An exploration of the relational and psychological stressors associated with Facebook use and affordances. *Computers in Human Behavior, 45*, 168-176. Fuchs, C. (2017). *Social media: A critical introduction*. Sage.

Gachago, D., & Ivala, E. (2012). Social media for enhancing student engagement: the use of Facebook and blogs at a university of technology. *South African Journal of Higher Education, 26*(1), 152-167.

Gagnon, K. (2015). Using twitter in health professional education: A case study. *Journal of allied health, 44*(1), 25-33.

Gharibi, W., & Shaabi, M. (2012). Cyber threats in social networking websites. *arXiv preprint arXiv:1202.2420.*

Gandy, O. H. (1993). Toward a political economy of personal information. Critical Studies in Mass Communication, 10(1), 70-97. doi:10.1080/15295039309366849.

Gibbs, G. R. (2018). *Analyzing qualitative data* (Vol. 6). Sage.

Glaser, B. G., & Strauss, A. L. (2017). Discovery of grounded theory: Strategies for qualitative research. Routledge.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report, 8*(4), 597-606.

González-Ramírez, R., Gascó, J. L., & Llopis Taverner, J. (2015). Facebook in teaching: strengths and weaknesses. *The International Journal of Information and Learning Technology, 32*(1), 65-78.

Goodmon, L. B., Smith, P. L., Ivancevich, D., & Lundberg, S. (2014). Actions Speak Louder than Personality: Effects of Facebook Content on Personality Perceptions. *North American Journal of Psychology, 16*(1).

Graham, S., & Wood, D. (2003). Digitizing surveillance: categorization, space, inequality. Critical Social Policy, 23(2), 227-248.

Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs.

Educational evaluation and policy analysis, 11(3), 255-274.

Guraya, S. Y. (2016). The usage of social networking sites by medical students for educational purposes: a meta-analysis and systematic review. *North American journal of medical sciences, 8*(7), 268.

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics, 133*(1), 111-123.

Hall, M. (2018). Facebook American Company. Retrieved from https://www.britannica.com/topic/Faceboo k

Heidemann, J., Klier, M., & Probst, F. (2012). Online social networks: A survey of a global phenomenon. *Computer networks, 56*(18), 3866-3878.

Hollenbaugh, E. E., & Ferris, A. L. (2014). Facebook self-disclosure: Examining the role of traits, social cohesion, and motives. *Computers in Human Behavior, 30,* 50-58.

Islam, M. B. (2014). Privacy by design for social networks. Queensland University of Technology.

Islam, M. B., & Iannella, R. (2011). Privacy by design:Does it matter for social networks? Paper presented at the IFIP PrimeLife International Summer School on Privacy and Identity Management for Life.

Islam, M. B., Watson, J., Iannella, R., & Geva, S. (2017). A greater understanding of social networks privacy requirements: the user perspective. *Journal of Information Security and Applications, 33*, 30-44.

Jeong, Y., & Kim, Y. (2017). Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Computers in Human Behavior, 69*, 302-310.

Junco, R. (2012). Too much face and not enough books: The relationship between multiple indices of Facebook use and academic performance. *Computers in Human Behavior, 28*(1), 187-198.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business horizons, 53*(1), 59-68.

Kayes, I., & Iamnitchi, A. (2017). Privacy and security in online social networks: A survey. *Online Social Networks and Media, 3*, 1-21.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security, 64*, 122-134.

Kumar, S., Kumar, P., & Bhasker, B. (2018). Interplay between trust, information privacy concerns and behavioural intention of users on online social networks. *Behaviour & Information Technology, 37* (6), 622-633.

Kumar, S., Saravanakumar, K., & Deepa, K. (2016). On Privacy and Security in Social Media–A Comprehensive Study. Procedia Computer Science, 78, 114-119.

Kuper, A., Lingard, L., & Levinson, W. (2008). Critically appraising qualitative research. *Bmj, 337*(aug07_3), a1035-a1035.

Leonardi,P.M.,Huysman,M.,&Steinfield,C. (2013). Enterprise social media: Definition, history, and prospects for the study of social technologies in organizations. *Journal of Computer-Mediated Communication, 19* (1), 1-19.

Litosseliti, L. (Ed.). (2018). *Research methods in linguistics*. Bloomsbury Publishing.

MacArthur, A. (2017). The History of Twitter You Didn't Know. *About. com Tech*.

Master, A., Cheryan, S., & Meltzoff, A. N. (2016). Computing whether she belongs: Stereotypes undermine girls' interest and sense of belonging in computer science. *Journal of Educational Psychology, 108*(3), 424.

Maxwell, J. A. (2012). *Qualitative research design: An interactive approach* (Vol. 41). Sage publications.

Misra, G., & Such, J. M. (2016). How socially aware are social media privacy controls? *Computer, 49*(3), 96-99.

Murthy, D. (2018). *Twitter*: Polity Press.

Nadkarni, A., & Hofmann, S. G. (2012). Why do people use Facebook? *Personality and individual differences, 52*(3), 243-249.

Napoleon, E. (2016). The effect of social networking sites on students' academic performance in girne american university, North Cyprus. *Ozan Ormeci Makaleler (Ozan Ormeci Articles).*

National Science Board. (2016, January 11). Science and Engineering Indicators 2016. Retrieved from https://www.nsf.gov/statistics/2016/nsb20161/#/p ermissions

Panahi, S., Watson, J., & Partridge, H. (2016). Social media and physicians: exploring the benefits and challenges. *Health informatics journal, 22*(2), 99-112.

Parra-Arnau, J., Mármol, F. G., Rebollo-Monedero, D., & Forné, J. (2017). Shall I post this now? Optimized, delay-based privacy protection in social networks. Knowledge and Information Systems, 52(1), 113-145.

Pensa, R. G., & Di Blasi, G. (2017). A privacy self-assessment framework for online social networks. *Expert Systems with Applications, 86*, 18-31.

Perrin, A. (2015). Social media usage. *Pew Research Center*, 52-6

Pezzola, D. (2013). *Exploring the role of social media on social behavior*. In proceeding of the 2013 Northeast Region Decision Science Institute (NEDSI) Annual meeting (pp. 5-7).

Phillips, D. J. (2004). Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies. New Media & Society, 6(6), 691-706.

Rennie, F., & Morrison, T. (2013). *E-learning and social networking handbook*: *Resources for higher education.* Routledge.

Roeber, B., Rehse, O., Knorrek, R., & Thomsen, B. (2015). Personal data: How context shapes consumers' data sharing with organizations from various sectors. *Electronic Markets, 25*(2), 95-108.

Saldana, J. (2011). Fundamentals of qualitative research: OUP USA.

Saldaña, J. (2015). *The coding manual for qualitative researchers*: Sage.

Sánchez, R. A., Cortijo, V., & Javed, U. (2014). Students' perceptions of Facebook for

academic purposes. *Computers & Education, 70*, 138-149.

Schneier, B. (2010). A taxonomy of social networking data. IEEE Security & Privacy, 8(4), 88-88.

Schwartz, H. A., Eichstaedt, J. C., Kern, M. L., Dziurzynski, L., Ramones, S. M., Agrawal, M., ... & Ungar, L. H. (2013). Personality, gender, and age in the language of social media: The open-vocabularyapproach. *PloSone,8*(9), e73791.

Sobaih, A. E. E., Moustafa, M. A., Ghandforoush, P., & Khan, M. (2016). To use or not to use? Social media in higher education in developing countries. *Computers in Human Behavior, 58,* 296-305.

Stalder, F. (2002). Privacy is not the Antidote to Surveillance. Surveillance & Society, 1(1), 120-124.

Strahilevitz, L. J. (2005). A social networks theory of privacy. *The University of Chicago Law Review, 919-988*.

Such, J. M., & Rovatsos, M. (2016). Privacy policy negotiation in social media. *ACM Transactions on Autonomous and Adaptive Systems (TAAS), 11(1), 4*.

Tao, K. W. (2014). Too close and too far: Counseling emerging adults in a technological age. *Psychotherapy, 51*(1), 123.

Tsiotsou, R. H. (2015). The role of social and parasocial relationships on social networking sites loyalty. *Computers in Human Behavior, 48*, 401-414.

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546-562.

Wallace, P. (2015). *The psychology of the Internet*. Cambridge University Press.

Wilson, C. (2013). *Credible checklists and quality questionnaires: A user-centered design method*: Newnes.

Yang, C.-c., & Brown, B. B. (2013). Motives for using Facebook, patterns of Facebook activities, and late adolescents' social

adjustment to college. Journal of Youth and Adolescence, 42(3), 403-416.

Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis:Evidence-based reflections. MalawiMedical Journal, 27(1), 13-15.

Zephoria Digital Marketing. (2018). The Top 20 Valuable Facebook Statistics – Updated September 2018. Retrieved from https://zephoria.com/top-15-valuable-facebook-statistics/.

Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), 2015 IEEE (pp. 180-184). IEEE.
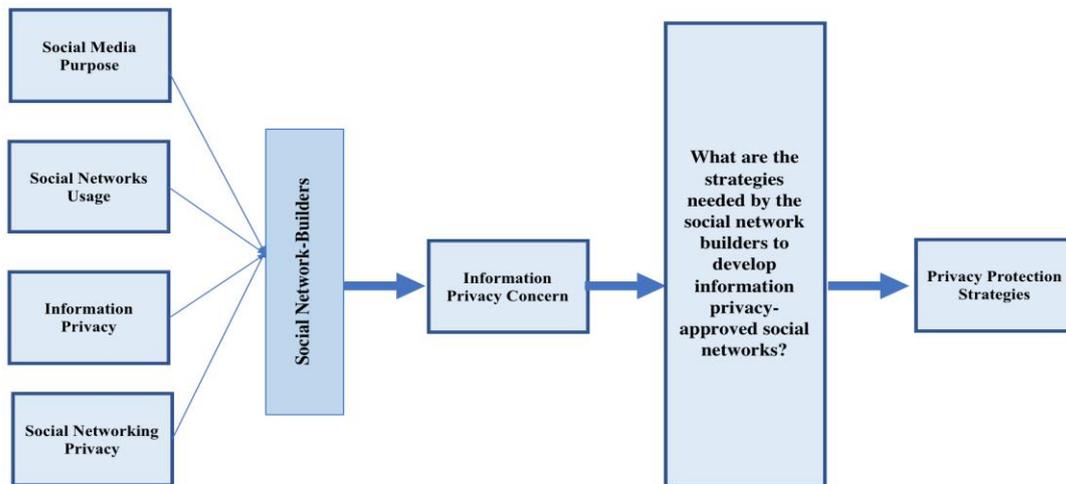
APPENDIX (FIGURES)

Figure 1. The Conceptual Framework