CSCanada
Management Science and Engineering
Vol. 9, No. 4, 2015, pp. 46-55
DOI:10.3968/7850

ISSN 1913-0341 [Print]
ISSN 1913-035X [Online]
www.cscanada.net
www.cscanada.org

Social Network and Privacy

Noura Al-Alawi[a],*

[a]Ph.D. Student, Murray State University, USA.
*Corresponding author.

Received 24 August 2015; accepted 26 November 2015
Published online 16 December 2015

Abstract

Whiles some use the internet basically for commerce, other use for educational purposes whiles to others, it is all about entertainment. The internet can therefore be likened to a blank check, which serves different purposes as and how a person wants to define it. The user variety of the internet notwithstanding, recent studies have actually confirmed that an aspect of internet usage that seem to have caught up with over 70% of all internet users is the phenomenon of social media networking (Compaine and Gomery, 2011). The research paper was conducted with the aim of finding the privacy risks associated with the use of social networking sites and for the practice of social media networking. To realize this aim, five major objectives were set, based on which research questions were developed. The research questions became a guide for the researcher to collect primary and secondary data, with particular emphasis on primary data collection, where a questionnaire was prepared for 50 respondents selected from a university campus. All 50 respondents were users of social networking sites and had strong academic background in journalism and communication, putting them in a position to provid well informed answers to the questions to the respondent. The primary data collection emphasized largely on the attitude of the respondents towards privacy issues whiles using social networking sites. The primary data collection exercise was also committed to knowing the depth of knowledge on privacy issues with social media networks. Through secondary data collection also, the researcher had the opportunity of knowing what the hosts of social networking sites are doing to protect the privacy of users.

Key words: Social network; Privacy; Security issues

Al-Alawi, N. (2015). Social Network and Privacy. *Management Science and Engineering*, *9*(4), 46-55. Available from: URL: http://www.cscanada.net/index.php/mse/article/view/7850
DOI: http://dx.doi.org/10.3968/7850

INTRODUCTION

A. Background to the Study

Technology has long been with us but there is no denying the fact that the issue became very topical with the coming of the internet. Up to date, the internet is considered as the most transformed innovation in technological advancement (Zittrain, 2013). Quite so, the internet has several components and aspects that affect the lives of people in different way. The concept of social network had long been used in the social sciences to represent the connection, relationships and links that exists people and others very close to them; particularly family and friends (Al-Jenaibi, 2014). With the birth of new media and for that matter the internet, a new platform seems to have been formed with which the agenda of social networking is constantly delivered and that is the internet. It is for this reason that social media networking has been explained as the use of an internet platform to connect a person to his social networks (Zittrain, 2013). Today, there are several websites specially dedicated for the purpose of social networking and these websites continue to increase in number of users. The central question that needs to be answered however has to do with whether social media networking is all positive with no consequences.

B. Research Problem

Because the major goal of social media networks has been to link people across the globe to their friends, family and loved ones, registering unto these social networks, most of which are free require that a person makes disclosure of very important personal information that will make it

easier for their people to identify or locate them. Once a person is registering to be on a typical social network such as Facebook, it is likely to see a request for some personal information such as the one showed in Figure 1 below.

From Figure 1, personal information such as First Name, Last Name, Email Address, Date of Birth, and Gender are required to get started. According to the social network service providers in their terms, such information is required to create a unique database of identity for a person registering and also to make it easier for others to locate a person on the social media platform (Al-Jenaibi, 2010).

Figure 1
Personal Information Needed to Sign Up to Facebook

C. Personal Information Needed to Sign Up to Facebook

As a person successfully signs on to these social media network, more personal data that has to do with things like school attended, relationship status, hometown, likes, pictures, place of work, family members, contact information, religious views, political views, languages spoken, and graduation dates are all required, even though in most cases not compulsory as the basic information needed to sign up. The reason for requesting all these personal information is for the purpose of creating a profile that will make it easier for friends to be sure of the identity of a person, given the fact that using one's name alone may not be enough to locate a person as several people bear the same name. As a social platform also, such personal information given in the profile build up helps friends and family to know much about the latest happenings in the lives of their friends. The problem that arises from this issue however has to do with the question of how safe it is to put up such information to a more public domain, given the fact that most social media networks are open to the public. Apart from the exposure to the public who may arguably be genuine friends and family, there is also the issue of how safe these information are from unscrupulous people who may want to have access to these information through the use of various means of computer hacking and hijacking. In today's world of digitized marketing, there is also the problem of the social media network hosts selling out personal information to advertisers, which could bring serious privacy issues.

D. Aim and Objectives

Based on the problem which has been identified above, the research is being conducted with the purpose of finding out the level of risk associated with social media networking in terms of privacy issues. As people sign on to social media sites, there are several promises made by the hosts of the sites on how they go to every extent to protect their privacy. However, Mowshowitz and Kawaguchi (2012) laments on the number of reports of breach of privacy issues that people report on a daily basis as a result of information they make available on social networking sites. The purpose of this study is thus in the right direction as it aims to serve as a public educational tool for users of social networking sites to come to light with the risks that they may possibly face from the use of social network sites so that with such education, they can take crucial decisions on ways of protecting their identities and privacy. To achieve the aim of research study, the following specific objectives would have to be achieved.

- To find the attitude of people towards the use of social media networks based on their demographic identities
- To measure the level of knowledge that people have about their risk to privacy exposure when using social media networks
- To investigate the negative impact of privacy issues on a person.
- To identify the different modalities that users of various social networking sites resort to in protecting their identities and privacy.
- To identify what the social networking site hosts do by way of protecting the privacy of users.

E. Significance of the Research

After the successful completion of this research paper, the researcher expects that there will be a lot of benefits and advantages that will be recorded. In the first place, the paper will serve as an important public document that enlightens people on the realities on the ground as far as their identity and privacy is concerned when using social networking sites. Based on the saying that knowledge is power, it is expected that this information that will be provided to the public domain will make it possible for people to make more informed choices on their privacy

and identity issues. The research paper is thus expected to bring about an entire era of attitudinal change for people who use social networking sites, especially when it comes to giving out private information about their lives. On the other hand of the study, various efforts that are being made by social networking sites to protect and guarantee the safety of the information of users will be known. This is an important aspect of the study as a comparative analysis of various social networking sites and their privacy policies will help the public to make much informed decisions on the best sites to use for the protection of their privacy. Lastly, the research paper will serve as a useful academic document that fills the gaps that exist in literature pertaining to privacy risks that come with the use of social networking sites. In most cases, the risk to users are the only focus of researcher but that gap of imbalance will be filled as side of the site hosts will also be taken to know what they are also doing to protect users.

F. Research Questions

In order to ensure that the data collection exercises that will be performed to collect data from respondents stay within the scope of the aim of the study, the following research questions will be used as a guide for data collection. This means that all forms of data collection will aim to answer these questions.

- What is the attitude of people towards the use of social media network in relation to their demographic variables?
- What is the level of knowledge and concern of people about their privacy when using social media networking?
- How may the use of social media networking impact on a person's privacy negatively?
- In what ways do people try to preserve their privacy on social networking sites?
- What are social media sites doing to protect the privacy of users

1. LITERATURE REVIEW

1.1 Social Network and Privacy

Technology has influenced the society in amazing and innovative ways. Social networking is one of the greatest influences in the 21st century. Up to 1.4 billion people are using various social networking sites to communicate in real time, share photos and videos (Al-Jenaibi, 2013).. Use of social networking has grown to include all people of all ages including the very young, the young, the mid aged and the old. Politicians around the world have also taken advantage of the benefits of the social networks to communicate with their followers (Salerno et al., 2012). While the use of social networks has grown remarkably, the privacy and safety of the users' information concerns have also increased. Many people wonder whether there are people who have access to the details they provide. The hacking of some of the social networking websites has also raised a lot of privacy concerns. Social networks have availed instant communication and sharing but there are grave concerns about privacy, which should be addressed to allow more people to experience the advantages of the new technology.

1.2 History of Social Networking

Unlike what most people think, the history of social networks goes back a long way. It is believed that the beginning of social networking was by the sending of the first email in 1971. Most people appreciated this for a number of reasons. Emails were much cheaper to send information to other people across the world and they could respond almost immediately. The email inspired people to come up with other ways to communicate even faster. In 1978, the Bulletin Board system was invented by Ward Christensen and Randy Suess to allow users to exchange data through the phone lines. Users could inform each other about meetings, make announcements and share data from time to time. In the following decade, a number of applications including the World Wide Web were introduced to the world. Introduction of the World Wide Web inspired many to come up with better ways of sharing information to not just a location but across the world. Beverly Hills Internet started Geocities, which is arguably the very first social networking system to be introduced to the world. Geocities allowed the users to create unique websites according to their tastes and preferences (Boyd & Ellison, 2008, p. 215).

The greatest milestone in the social networks was in 1997 when the World Wide Web got more than one million websites. In that year, blogging started, Six degrees was started which allowed people to create profiles and list friends like the current social networking websites, AOL was introduced and allowed people in different locations to chat in real time and black board which allowed educators and learners to connect through the internet was introduced (Curtis, 2013). In 1999, a British inventor introduced friend united, a social media platform that was to reunite students from various schools. By the year 2000, more than 70 million computers were connected to the Internet and inventors and entrepreneurs appreciated that Internet would be the greatest thing at the beginning of the new century (Fellow, 2009, p.381). In 2002, Friendster was launched and grew to have three million users in just three months, at a time when AOL had reached 34 million users. In the following year, LinkedIn, which was for business professionals and MySpace for all individuals were introduced. In 2004, Facebook was introduced and was followed by Bebo, YouTube, Twitter, Bing and Google plus at the interval of one year. Social networks have grown to include many people across the world (Lusted, 2011).

1.3 Social Networking Privacy Issues

Most people appreciate their benefits especially instant messaging and sharing. However, the issue of privacy has raised a lot of concerns about social networking. Most people are concerned that the staff working in the social networking sites may have access to their private information, which they can use against the clients (Al-Jenaibi, 2012). In fact, there are consistent claims that people in different levels in the organization may disclose confidential information like client details for some reasons. At that stage, some staff may take the information and may pass it to other people to try to access the client information. This could explain why some people's social networking accounts and commercial websites are hacked into despite having them secured well (Chang, Abu-Amara, & Stanford, 2010, p.168).

The recent revelations about Edward Snowden have caused panic among many social networking providers. Snowden was a programmer with National Security Agency (NSA) who woke up one day, moved to another country and disclosed very sensitive information to people in the countries he went to (King, 2013). Social networking providers came to appreciate that some of their employees can do the same thing especially those that are in data security department (Al-Jenaibi, 2011). According to Elovici (2012), there are always cases where employees become rogue and take sensitive data with them. Such cases are rare and the companies can do little to prevent them.

According to Fogel and Nehmand (2009), some social networking websites users feel that strangers may use their information to get to them. In a study done by these two researchers, 22% of college students were concerned that strangers may use information to know where they lived while 40% claimed that strangers may use social networking information to know their class schedules. Most of the students provided their home location and class schedules in their Facebook profile. The students felt that there should be a form of security allowing only the people they are connected to in the profiles to access their details. While this can be done by changing the privacy settings, most students still felt that strangers can access their important information (Lewis, Kaufman, & Christakis, 2008).

Some social networking providers have used their clients' private information for their own benefit to some extent. In 2007, Facebook really wanted to monetize their website. In this regard, Facebook created a program, which tracked what the users bought through Facebook and kept records, the program was interlinked with other websites which sent alerts to the individual clients when such products were available for sale. This was a violation of user details as they did not ask users for the information. There are also claims that some of the social networking and commercial websites use some spyware to access very private information from their clients' computers. They can access information that even the clients cannot post on social media and use it for their own benefit (Stewart, 2013).

Another great privacy concern is the Single Security Access Sign-On which was introduced in 2012 by most social networks. This allows people to use just one login detail to access multiple websites be it other social networking websites or commercial websites. While most people use this service to avoid having many login details for many websites, they are concerned that access of such login details by another person can be detrimental. It is unimaginable what some people are likely to do with such information. The knowledge that a user uses the same information for multiple sites would encourage the third parties who access such information to try to use the same details for commercial websites and even payment sites. Clients may get information indicating that they have used their payment wallets to make payments yet they did nothing of the sort (Federal Bureau of Investigations, 2013).

Merging of several social networking sites and the use of one login details has not been received well by governments and security experts. The Internet communications giant Google has been on the receiving end recently for planning to merge client details. Under this plan, which is included in the new privacy terms and conditions of Google, clients will use the same login details to access more than 60 Google products including You Tube, Gmail, Google plus, Library, Google Scholar and books to name but a few (CNBC News, 2012). This is a good strategy for Google as it will save the clients the hassle to have many login details. At the same time, the company can be able to track the millions of clients easly to determine those that violate the terms and conditions. Many experts agree that it is a good strategy but poses a lot of risks to private information (Williams, 2013). It is the concern of many people that social networking providers do not listen to their clients when it comes to privacy settings. In fact, clients do not have a say in the terms and conditions of private data. A study by Michelle, Lupe and Michael (2011) concludes that there are a lot of mismatch between the privacy settings of the social network providers and how the clients use the websites.

According to the Federal Bureau of Standards, cybercrime has increased significantly with the popularity of social networking and commercial websites. Rogue programmers across the world are working day and night to come up with programs that can access client data from their homes or offices. There are many tactics used including baiting, phrihising websites, malware, doxing, farming and phreaking. In most cases, small programs are installed in major trusted website including the social networking websites. When clients access the websites

with the small programs installed by the hackers, the programs collect their personal information including their login details to that website and other confidential information in the computer like credit card and bank details (Abraham, 2012).

Social media giants appreciate too well just how the rogue programmers across the world are determined to access client data. Recently, there were claims that a key logging software was installed in untold number of computers across the world. Some of the major social networking websites were affected with more than two million social networking accounts said to have been affected (Pagliery, 2013). Earlier in 2013, more than 250,000 Twitter accounts were hacked into and the hackers obtained login details and other private information for the clients (Kelly, 2013). In august 2013, a Palestinian Information Systems Researcher, Khalil Shreateh, successfully hacked into the account of Facebook founder Mark Zuckerberg to show security flaws of Facebook. He claimed that he could login to other people's account and post anything without their knowledge (Gross, 2013).

The massive security flaws that have been detected in most of the social networking websites have raised a lot of questions on client privacy. Experts and individuals alike question why social networking providers cannot improve the security of their websites to safeguard client information. Though social networking requires some level of openness and provision of certain information, most people feel that the providers have an obligation to protect their data. Some social networking providers like Google plus have gone the extra mile of ensuring client data protection. This has put a lot of pressure on the most common social networking websites like twitter and facebook to improve their security (Qualman, 2012).

The use of social networking sites has become very common in the last decade. Up to 1.3 billion young and old people across the world are using these websites to share information and pictures. Politicians are also using social networking sites to market their ideologies to the prospective electorate. This trend is expected to grow even faster in the coming decade. However, there are serious concerns about the privacy of the clients. Most of the social networking providers have serious security flaws, which have been proved by rogue and ethical hacking programmers. There is dire need to address the security issues to ensure better security for the client information. Social networking providers have a responsibility of getting highly secure systems such as high level encryption to protect client data. These organizations should also ensure that no single person can access the client data individually. The government has the potential and resources to compel the social networking providers to introduce better security measures for client information.

2. RESEARCH METHODS

2.1 Research Approach

In order to achieve the objectives that have been set above, it was necessary that the researcher collected primary data from people who have been directly involved in the use of social networking sites in one way of the other. For this reason, a data survey research design was developed. In using survey research design, the researcher identified a group of people from a very large base of people from whom data were collected. The responses given by these people were generalized to be the opinion or response of all the people in the research setting. As part of the survey research design, the researcher used the quantitative data collection approach to collect data for the study. In such quantitative data collection, emphasis is placed on the collection and analysis of data using numeric indexes and variables (Compaine & Gomery, 2011). In line with this, data collected were subjected to quantitative techniques such as finding mean, percentages and frequencies.

2.2 Research Design

Using a survey research design requires a lot of technicalities to make the generalization of information valid for all people within the research setting. In this research paper, one of the technicalities used was to ensure that the selection of respondents was done in a random manner to ensure that there was no biases and favoritism in the selection. Once such randomized sampling is used, one can be assured that the survey results represent the genuine views of all people within the research setting. But to have a random sampling means to have a population; where the population represents all the people within the research setting. In this study, the research setting used was a university campus. Within the setting, all students in the Journalism and Communication Faculty were included as the population for the study. However a random sampling was used to select 50 respondents who formed the sample size of the study.

2.3 Data Collection Instrument

The research instrument that was designed for the data collection was a questionnaire. The questionnaire was made up of a set of questions which were written and presented to respondents both in person and via the use of the internet through survey monkey questioner. The questionnaire contained questions that were constructed based on the research questions of the study. This means that the questionnaire was made up of an expansion of the research question to contain a total of 24 questions. 24 questions were mostly based on the first four research questions as data collection for the last research question was based on secondary data collection rather than primary data collection. 24 questions on the questionnaire were largely close ended questions, meaning that they

each had alternative responses for the respondents to select from. This was done as part of the quantitative nature of the study, which needed to have a systematic format in the way questions was answered by the respondents to make data analysis easier.

2.4 Data Collection

The data collection process took place at the university campus. After going through all ethical consideration, which included the need to prepare a consent form and giving them to the respondents to read and agree to, the researcher had a mini-conference with the 50 respondents. The conference was aimed at discussing the questions with the respondents without taking their responses at that very time. Rather, it was meant to make all questions very understandable and clear to the respondents so that the responses they produced would be in accordance with the very purposes for which the questions were set. At the conference, it was agreed that each respondent would have 5 working days to finish the questionnaire and make them available for collection. In the course of the 5 days, text messages and calls were sent to remind respondents of the deadline. As part of ethical consideration for the research work, the researcher was the only person who handled the questionnaire and did not make use of a third person. Again, after the data analysis, the questionnaires were returned to respondents to be discarded by them.

3. SURVEY RESULTS

The survey results section of the research paper is basically dedicated to making the findings that were made in the course of primary data collection known, interpreted and discussed. Because the study was a quantitative study, the approach to the survey results is a quantitative approach. This means that researcher shall make the findings available by use of various mathematical indexes and formula. After this has been done for various data, there shall be a discussion on the implication of each set of findings in accordance with the research problem. The findings are presented in four major themes, which are based on the first four research questions which were used to prepare the questionnaire. Under each theme, there are two sub-themes that summarize all questions on the questionnaire that were linked to the theme. This means that the survey findings section will end with all the 24 questions on the questionnaire presented and discussed in one form or the other.

3.1 Attitude of People Towards Social Media Networking

This theme was focused on knowing how different people approached the use of social media networks and why they use social media networks at all. Two major sub-themes are considered under this theme with findings as follows.

3.1.1 Average Time Spend on Social Networking Sites in a Day

A question was posed to respondents on the number of hours they spend on social networking sites in a day and reasons for which they use the social media networking sites most. The following findings were made on the number of times they spend on social networking sites.

From the chart above, the modal time spent on social networking is 3-4 hours, which were selected by 18 respondents. This was followed by 1-2 hours, which were selected by 13 respondents. The time average with the least number of respondents is 0 hours. The implication of this statistics is that there is very high rate of social media networking usage among the respondents who responded to the questionnaire. This is because in literature, McGinn (2011) noted that the average time spent on social media networking by people is 1 hour. For the modal time score to be 3 to 4 hours therefore means that there is a high rate of social media network usage. Further data collected seemed to justify the trend of the results. This is because data on the age group of respondents showed that respondents were in the age of 17 to 28. Meanwhile, Mowshowitz and Kawaguchi (2012) said that people below the age of 30 have the highest number of addiction to the use of social media networking. Another question on the questionnaire on the reasons respondents uses social media showed that they used it mainly to stay in contact with friends and then with the family. A lot of the respondents also spent these times following celebrity and entertainment events. The implication of this result is that people within the age of 17 to 28 have a higher risk to privacy issues since it takes them making as many of their personal data available as possible to make it possible for their old friends to locate them and stay in contact with them.

3.1.2 Time Spent on Reading Privacy Policies

This line of data was collected to know the attitude of users towards the reading of privacy policies as the researcher identified that social media hosts play their part of the privacy issue by making their privacy policies clearly known to users and that by using the social networking sites, users automatically bind themselves to the privacy policies. Once this the question on whether respondents ever take time to read privacy policies, the following data were gathered.

The findings made above clearly shows a negative attitude towards the reading of privacy policies of social networking sites. This is because the least number of respondents gathered for a particular response was those that answered to the affirmative. The modal score was surprisingly those who have never had time to read privacy policies, made up of 20 respondents, representing 40% of the total population. Meanwhile, Waters and Lee (2003) said that the privacy policies serve as important legal commitment and agreement between users and the

hosts. The implication of these findings is that most users of social media networks can hardly have the legal basis to argue their cases out in terms of breach of privacy issues (McGinn, 2011). This is because they hardly know what the policies state and so can hardly tell whether these policies are good for them or not. At the saying goes, knowledge is power and so it will be important for users of social media networks to be well informed about what holds for them in the use of these networking sites before they go into their use, especially when it comes to issues with their privacy.

3.2 Concern of Users About Privacy Issues

These lines of data were collected to know if users have any concerns about their privacy and identity when using social networking sites. It was also know their level of knowledge about privacy issues. For this reason, various questions were asked to focus on this theme, the results of which have been indicated below.

3.2.1 View on Importance of Privacy Within Social Media Realm

How much a person is concerned about an issue may easily be manifested through the importance they attach to the issue. For this reason, the researcher asked the respondents to indicate the level of importance they attach to privacy when it comes to the use of social media networks. Rating from 1 to 5 with various parameters of score, the following results were obtained.

From Figure 3, responses give about the importance of privacy in social media to the attitude of respondents towards the reading of privacy policies can be said to be contrasting. This is because even though greater percentage of respondents find privacy to be an important issue, they still did not border to read about the privacy policies to know whether or not these policies where towards a direction that benefited their interest. This is because according to the data collected, only 2% of the respondents said privacy did not matter in the realm of social media networking. The modal response was "high", which was selected by 23 respondents, representing 46% of the total sample size. In secondary literature, the lack of synchrony between importance attached to privacy and attitude towards reading privacy policies is well explained. This is because Ostrom (2003) noted that most users find themselves in a helpless situation to deal with the risk that comes with privacy. This is because even though they may be concerned, they know they can do very little in stopping their privacy to be invaded by people who may want to do so. This is particularly because the avenues for which people may get access to their private information are so much and virtually uncontrollable (Waters & Lee, 2003). It can be implied therefore that users weigh the advantage of using social networks to the disadvantage of privacy risk and select the advantage over the disadvantage.

3.2.2 View on Who Is Responsible for Ensuring Safety With Internet Experience

Other sets of questions that reflected the concern of respondents' privacy issues on social media network were questions that tried to test the ones the respondents held as being responsible for ensuring safety with internet browsing experience. On one of such question that asked respondents about who was responsible for ensuring that there was ultimate safety of the internet experience, the following responses were received from the respondents.

From the data presented above, it would be noted that a good number of respondents believe that it is the responsibility of service providers, rather than the users in ensuring that there is safety with the browsing experience. This is because 31 respondents representing 62% said that social networking hosts should take up the responsibility of ensuring that there was safety with the entire browsing experience. Meanwhile, literature reviewed from Ferguson (2005) showed that the role of ensuring the safety with the browsing experience should actually be seen as one that is a shared responsibility but largely dependent on the users. This is because it was noted in literature that most of the things that service providers do to ensure safety are static and unchanged. Example of this is the fact that the service providers provide privacy settings, where users can manipulate who should have access to their information and who should not; once their pages are viewed or searched. Once such provisions are made, users must take advantage and use them adequately. On the other hand, respondents may be agreed with as there are other times that hackers have access to people's accounts and go behind privacy settings. The network providers must therefore be in a position to consolidate their security systems that make their networks resilient to the activities of hackers and hijackers such as what was reported in the Edward Snowden (NSA leaker) case. This is because other questions answered that showed that the information that Edward Snowden brought to light have changed their mind concerning the way in which they use and integrate with social media.

3.3 Impact of Social Media Networking on Person's Privacy

These set of data were collected to identify the worse forms of privacy risks that users of various social media networks identify themselves with while using various social media networks. On the whole, there were two major variables that were used to measure these privacy risks to users and these two variables have been outlined below.

3.3.1 Most Troublesome Third Party Privacy Users

The respondents were asked of the group of third party users who when they have access to their private data and information possesses the worse trouble to them. Base on the impact that each of the third parties have on the users, the following responses were produced.

From the data gathered above, it would be noted that respondents perceive government agencies as having the worse form of impact on their privacies once their personal data and information gets to these agencies. This line of data could be said to be in line with literature reviewed on the activities of some government agencies as showed in the Edward Snowden leakage (van Vark, 2004). This is because once such information gets to the government agencies there are different forms of sabotage functions that can be played with these data. A good number of respondents represented by 30% of the total sample were also concerned about the impact that private data that gets to advertisers can play against them. This is because in literature, it was seen that most advertisers keep pestering potential customers with series of calls and emails for them to patronize their products. Not much of the respondents really saw any major negative impacts with their private data getting to the network hosts themselves. This is however a puzzling revelation that indicates how the respondents are not adequately informed of the marketing purposes that most social networking hosts use the information about their users for. This is because Ostrom (2003) noted that the sale of personal information continues to be the major source of income for most social media network sites, who charge users nothing for using their services.

3.3.2 Percentage of Identity Thief Through Social Networking Platforms

Identity thief has been identified in literature to be one of the most critical pivacy risks that most users of social media networks have reported. Because of this, the researcher wanted to know how seriously respondents saw the issue of identity thief as an impact of social networking risk on a person's privacy. To do this, respondents were asked estimate the percentage of identity thefts utilized through social networking as a means of setting information about potential victims. This question produced the following responses.

From the data collected, it is noted that up to 50% of respondents fell in the modal range of 0-10% saying that perceived rate of identity thief was promoted by use of social media networks. The implication of this result is that there is very little believe among respondents that social media networks pose any privacy risks in terms of identity thief. Linking this line of data to literature, it would be said that there is a high level of misinformation among respondents in terms of the risk that social media networking pose to their privacy issues in terms of identity thief. This is because Ferguson (2005) reported that up to now, the use of social media platforms is the second highest means by which most people engaged in identity thief get their information from. It will not be wrong to imply that most social media network users are indeed exposed to high rates of risks of identity thief as they do not appreciate the level of risk that they are truly faced with as a result of making their private information available and having these private information hacked into. The reason for this inference is that in terms of security, van Vark (2004) argued that the better a person has knowledge about an issue, the more likely it is that the person will take steps towards controlling any risks associated With The Issue.

3.4 Interventions Towards Promotion of Privacy Protection

Having established from literature that there were indeed several risks associated with the privacy of people who use various social media networks, the researcher proceeded to ask the respondents if they took any steps towards minimizing or preserving their privacy on social networking sites. Different questions were asked in this direction, for which the following data were produced. The respondents were asked if they allowed location services on their social networking sites. This is because knowing the location of a person is part of the major variables with privacy that have been discussed in literature. Once the question of whether respondents allowed location services on any of their social networking applications, the following responses were produced.

From the responses above, it would be noted that one of the major means by which respondents ensure their privacy is by disabling location services on their social media network sites. This is because out of a total of 50 respondents, as many as 34 representing 68% said they did not allow location services on any of their social networking sites. This way, it is possible to keep their locations to themselves without this being known by other users on other sides of their social network sites. On the part of 16 respondents, making their locations known to their respondents was all part of the social contracts they had with their friends and loved ones and so did not see the need for keeping their locations from their friends and family. Through the review of further literature, it was found that disabling one's location settings was not really an effective way of hiding one's location privacy because there are new applications that enable people to detect locations of one end user as long as their internet settings remain active.

CONCLUSION

Data collected largely showed that as much as greater percentage of respondents are concerned about their privacy when using social networking sites, there is very little that they are able to do to guarantee such privacy. This is because of how open the system of most social networking sites are, allowing people who are neither friend nor followers to view the profiles of other people. Even though there is the option made by social networking sites such as Facebook for users to limit people that can view their profile, the respondents said blocking their

personal information from the general public was like going hiding from the public and that would kill the essence and idea of social media networking. A good number of respondents confessed to having looked at the profiles of other people they did not actually know for curiosity purposes. These findings confirm that indeed the issue of privacy remains one that continues to pose challenge with the use of social media networks. This is because even with the little provisions made by the site hosts to promote identity privacy, not a lot of people are making use of these as they find them contrary to the whole idea of social networking.

Based on the findings, it can be concluded that people have different attitude towards the use of social media network, with the younger age, mainly focused on the need to make as many friends and followers who will know about what happens in their daily lives as possible. Because of this attitude to the use of social media network, very little concern is shown towards privacy issues. A conclusion that the risk of privacy will continue to be felt by most users, especially younger people below the age of 30 will be a valid conclusion. Also, based on secondary data which suggest that social network hosts are using their sites as a major marketing platform through the sale of important user data, the conclusion that a refusal by a user to be personally concerned about privacy would mean an automatic exposure to privacy risk can also be validated. Until such a time that users will take their own privacy into their hands and ensure that no sensitive private data are made available on social media networks as part of building social profile, very little can be done by the hosts to guarantee safety with privacy, especially as the works of hackers remain uncontrolled.

REFERENCES

Abraham, A. (2012). Computational social networks*: Security and privacy*. New York: Springer.

Al-Jenaibi, B. (2014). The nature of Arab public discourse: Social media and the "Arab Spring". *Journal of Applied Journalism & Media Studies, 3*(2), 241-260.

Al-Jenaibi, B. (2013). Satisfying public relations: The Promise of social media in the UAE. *International Journal of E-Adoption, 5*(1), 1-16.

Al-Jenaibi, B. (2012). The scope and impact of workplace diversity in the United Arab Emirates–A preliminary study. *Malaysia Journal of Society and Space, 8*(1), 1-14.

Al-Jenaibi, B. (2011). The practice of public relations departments in increasing social support in the diverse workplaces of the United Arab Emirates. *Cross-Cultural Communication, 7*(3), 41-54.

Al-Jenaibi, B. (2010). Differences between gender treatments in the work Force. *Cross-Cultural Communication, 6*(2), 63-74.

Boyd, D., & Ellison, N. (2008). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13,* 210–23.

Chang, W., Abu-Amara, H., & Stanford, J. (2010). *Transforming enterprise cloud services*. New York: Springer.

CNBC News. (2012). *Google data merge called privacy threat*. CNBC. Retrieved from http://www.cbc.ca/news/technology/google-data-merge-called-privacy-threat-1.1130198

Compaine, B., & Gomery, D. (2011). *Who owns the media?: Competition and concentration in the mass media industry* (3rd ed.). Mahwah, NJ: Lawrence Erlbaum Associates.

Curtis, A. (2013). *The brief history of social media: Where people interact freely, sharing and discussing information about their lives*. Retrieved from http://www.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html

Elovici, Y. (2012). *Security and privacy in social networks*. New York: Springer.

Federal Bureau of Investigations. (2013). *Internet social networking risks*. Retrieved from http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1

Fellow, A. (2009). *American media history*. Stamford: Cengage Learning.

Ferguson, C. H. (2005). What's Next for Google?: The search firm wants to organize all digital information. That means war with microsoft. *Technology Review: MIT's Magazine of Innovation*, *5*(3), 45-64.

Fogel, J., & Nehmand, E. (2009). Internet social network communities: Risk taking, trust, and privacy concern. *Computers in Human Behavior, 25,* 153-160.

Gross, D. (2013). *Zuckerberg's Facebook page hacked to prove security flaw*. CNN. Retrieved from http://edition.cnn.com/2013/08/19/tech/social-media/zuckerberg-facebook-hack/

Kelly, H. (2013). Twitter hacked; 250,000 accounts affected. *CNN*. Retrieved from http://edition.cnn.com/2013/02/01/tech/social-media/twitter-hacked/

Kings, J. (2013). Privacy concerned social network for activists launches. *Digital Journal*. Retrieved from http://digitaljournal.com/article/358617

Lewis, K., Kaufman, J., & Christakis, N. (2008). The taste for privacy; an analysis of college student privacy in an online social network. *Journal of Computer Mediated Communication, 14,* 79-100.

Lusted, M. (2011). Social networking*: MySpace, facebook, & twitter*. Edina: ABDO Publishing.

McGinn, R. E. (2011). *Science, technology, and society.* Englewood Cliffs, NJ: Prentice Hall.

Michelle, M., Lupe, J., & Michael, B. (2011). *The failure of online social network privacy settings.* New York: Columbia University Press.

Mowshowitz, A., & Kawaguchi, A. (2012). Bias on the Web. *Communications of the ACM, 45*(9), 60.

Ostrom, M. A. (2003, February 26). Pasdena, Calif., commercial search firm to buy web search properties. *San Jose Mercury News*, p.4

Pagliery, J. (2013). 2 million Facebook, Gmail and Twitter passwords stolen in massive hack. *CNN Money*. Retrieved from http://money.cnn.com/2013/12/04/technology/security/passwords-stolen/

Qualman, E. (2012). *Socialnomics: How social media transforms the way we live and do business*. Hoboken: John Wiley & Sons.

Salerno, J., et al. (2011). Social computing, behavioral-cultural modeling and prediction*: 4th international conference*. SBP 2011, College Park, MD, USA, March 29-31, 2011. Proceedings. New York: Springer.

Stewart, K. (2013). Social network*: An extraordinary guide on social networking for business, social networking for career success, social network marketing, diaspora, digital age and more*. Montgomery: Tru Divine Publishing.

van Vark, C. (2004). Search engines: Search still sets the pace. *Revolution, 4*(2), 24-34.

Waters, R., & Lee, A. (2003, March 5). Ask Jeeves to Join Excite Internet. *The Financial Times*, p.43.

Williams, C. (2013). *Google faces privacy investigation over merging search, Gmail and YouTube data.* The Telegraph. Retrieved from http://www.telegraph.co.uk/technology/google/9966704/Google-faces-privacy-investigation-over-merging-search-Gmail-and-YouTube-data.html

Zittrain, J. (2013, April 13). In searching the Web, Google Finds Riches. *The New York Times*, p.4.

