Cybersecurity Challenges in Social Media

Erdal Ozkaya

A thesis submitted in fulfillment of the requirements for the degree of

Doctor of Information Technology

School of Computing and Mathematics

Charles Sturt University

Certificate of authorship

I, Erdal Ozkaya, hereby declare that this submission is my own work and, to the best of my knowledge and belief, understand that it neither contains material previously published or written by another person nor material that, to a substantial extent, has been accepted for the award of any other degree or diploma at Charles Sturt University or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by colleagues with whom I have worked at Charles Sturt University or elsewhere during my candidature is fully acknowledged.

I agree that this thesis be accessible for study and research in accordance with normal conditions established by the Executive Director, Library Services, Charles Sturt University or nominee, for the care, loan, and reproduction of thesis, subject to confidentiality provisions as approved by the University.

Acknowledgements

My deepest gratitude goes to Dr. Rafiqul Islam for his unwavering support and collegiality throughout this journey. Your patience, motivation, and guidance has helped me throughout my research. I could not possibly have had a better advisor and mentor for my DIT study.

My special thanks to my wife, Arzu, and two kids, Jemre and Azra, for all your support and endless love. I know I steal a lot of time from you and spend it in my research; that's why, I cannot thank you enough.

My parents—they never went to school, they never had a chance to read and write. But all their life, they worked really hard for me to get an education and no words can explain how thankful I am for all that you have done. The same credit goes to my brothers; they supported me during my early education, and this simple line of thanks cannot reflect the respect I have for both of you

Abstract

Recent actions by social media platforms have sparked a new debate on the privacy of users. There have been reports of user data being sold to third parties and personal data being accessed for advertising purposes with or without their consent. A new wave of security threats is also coming up and is breeding on social media platforms. Social engineering has grown to be a formidable security threat due to the amounts of data that users are posting on social media platforms. Hackers do not need to search deeply for data that they can use in order to attack users. Attackers lurking on social media platforms or ganging up with the revenue-focused social media platforms have made it hard for social media users to continue enjoying these platforms free of worries.

In response to this, this research has studied the ways in which social media platforms are inherently putting users in the way of security and privacy threats. It has hypothesized that social media platforms are the culprits of increasing security and privacy threats that users are facing and research has been conducted to prove the same. In the results, it has been observed that users are increasingly getting wary of their security online due to social media platforms. From secondary data sources, it has also been found that there are many social media users who are exposed to security and privacy risks but are unaware. Based on the findings of the primary and secondary data, the research has formulated some recommendations that it hopes will reduce the security and privacy issues that users are facing on social media. The recommendations are aimed at making users more secure, encouraging government participation in regulating social media platforms, and urging social media platforms to give users more control over their privacy.

Contents

List of tables

Chapter one: Introduction

1.1 Preamble

The Internet has developed from being a secure military communication channel to becoming a public space commonly used for communication purposes (Tarnoff, 2018). Social media platforms on the Internet have almost become an integral part of people's lives (Gordhamer, 2018). They have enabled them to stay in touch with their loved ones, get to form relationships with total strangers, keep tabs on the lives of others through the posts that they share, get information, and inform others, among other things. These platforms have brought about a unification of the world where users from almost all countries, save for the likes of North Korea, are able to get in touch with people from far away countries (Talmadge, 2018). However, social media platforms have created a new problem altogether. There has been a huge increase in the amount of personal information that users have been putting out to the public domain. This information was initially just being stored on the servers of the social media platforms till they started monetizing it. Platforms such as Facebook, which initially never wanted anything to do with ads, came to be at the forefront of trading users' data for money. Many people and organizations have come to question the legality of these actions, as they are presumed to violate the privacy rights of users. There have also been ethical questions about the sale of personal data to advertisers by these social media companies. The boundary between what is regarded as private and what is not has only been reducing. Apart from the violations of privacy by social media companies, there have been concerns over the amount of sensitive data that oblivious users have been sharing on these platforms.

1.2 Overview of cyber threats

Today's cyber threat landscape keeps on expanding. It is almost like everyone who uses the Internet faces some kind of a cyber threat. There has been a surge of cyber-related criminal activity in the last few years. The more technology develops, the more new attacks come. At the same time, cybersecurity companies are seemingly playing catch up with attackers; they are responding only after new attacks have been discovered. There have been disturbing rumors that some government agencies, such as the US NSA, have a database of zero-day attacks that can be used to attack systems without being detected by any cybersecurity system (Storm, 2018). At times, these zero-day attacks have been known to get into the hands of the enemies. In May 2017, a ransomware called WannaCry caused devastation all over the world after it encrypted many computers leading to the shutdown of critical systems, loss of revenues and, sadly, loss of lives that depended on some of the attacked systems (Liptak, 2018). A hacking group called Shadow Brokers had allegedly stolen the zero-day vulnerability from the NSA and put it on the public domain (Shane, Perlroth & Sanger, 2018). The creators of WannaCry took it from there and developed the vicious attack tool that encrypted computers in seconds (Greenberg, 2018).

This is a reflection of the current threat landscape. There is a lot of unpreparedness for the attacks to come. Organizations are having to resort to cyber resilience rather than depending fully on cyber defense. They are aware that there is no certainty that the security systems they have will be able to protect them from all the threat vectors. Individual users are, however, the unfortunate lot. With the limited technical knowledge that they have, they have been exposing themselves to many cyber threats. Attackers have, therefore, turned their guns against end users.

Many social media companies have already disregarded the privacy of their users. They have been dangerously selling off sensitive information to third parties. This inherently

puts the security of the sensitive data no longer in the platforms' hands but in the hands of unknown third parties. Overall, there is a lurking problem that everyone should be afraid of. The cyber threats that Internet users, more so, social media users, are facing are many.

1.3 An Overview of privacy issues in social media

The list of privacy and security issues on social media seemingly continues to grow. The outright harvest of personal data on these platforms by combined efforts of hackers and social media companies has increased the security concerns. Hackers are on these platforms looking for any information that they can use to attack a user. Hackers want to get information such as birth dates, pet names, banks names, account numbers, and other personal information that can be used to attack the users. They also look for information that can be used to answer secret questions that a user has set up on his or her accounts. For example, if one has set up a secret question asking for a pet name and if the hackers can get this information from his/her social media account, the attack will be successful.

On the other hand of oppression, social media users are having to contend with their personal information being sold to third parties or being accessed for advertising purposes by their social media platforms. They are doing this using shoddy means to avoid consequences.

Some of these social media companies such as Facebook have been charged in court and found guilty of violations of user privacy. The EU, one of the most active organizations when it comes to digital rights of its citizens, has severally sent stern warnings to Facebook and the likes on the issue of user privacy (Tannam, 2018). However, most social media companies have remained adamant that they are acting within the law. They all make users sign away their privacy when they are joining the platforms. Therefore, an end is not in sight for the data collection activities by the social media platforms. Together with hackers, they have made it riskier for the users to share their private information on any social media platform.

1.4 Motivation

1.4.1 Problem statement

To investigate the privacy issues and impacts that social media users are facing and how to mitigate them.

Social media platforms have brought about deeply troubling privacy concerns to the users. Private user data is, first of all, being collected, stored, and sold off to third parties or being used for other purposes than what the user wished from the owners of these platforms. Social media platforms have been accused of gathering data that a user has provided in his/her account, and data in posts and messages and even photos and videos, solely for advertising purposes. Users are being forced to accept flawed terms and conditions that give rights to the social media companies to use their data in whatever ways they please. It is so hurting for the users to openly see their personal data being paraded for other companies to either buy or use for advertising purposes. Users have been tricked into giving out the ownership of their data, and all this trickery has been done to basically enable the social media companies to have the right advert to shove in a user's face when on that platform. Social media is becoming filthy; it is no longer about supporting users to get the best experience as they interact with each other; rather, it has now become all about making money out of them. There is a lot of money in digital marketing, and many companies are rushing to milk that cash cow before it runs dry. The best place to find ready data from the public without having to search much is, of course, the social media, and companies are making up to the last dime out of their users.

There is also another group targeting the personal user information. This group is comprised of attackers and governments. As for attackers, these include scammers, spammers, hackers, and social engineers. Some of them keep continually stalking users on their various social media accounts and recording their every move, post, and information

that they have shared publicly. It is easier for social engineers to find lots of details about users on social media platforms than anywhere else. They use this data to trick users into believing that they are legitimate people in banks, government, or institutions. Innocent users suffer at the hands of these attackers only because social media platforms want to keep the user data naked for all to see. Some governments have also been accused of actively spying on citizens over social media platforms. They are said to coerce the platforms to give out private user data, such as messages. They are also said to have their elite team of hackers that breaches into user accounts on a need-to-know basis. They do this in the name of protecting citizens from acts of terrorism.

Many other issues can be talked about but it is clear that there is a burning need for protecting user privacy on social media. A lot has been said and many threats have been issued, yet very few actions have been taken. It is therefore necessary for a comprehensive research to be done to unearth all these privacy and security issues that users are facing on social media. Finding these issues will allow for substantive mitigations to be suggested. The recommended mitigations will mostly help the users, the social media companies and, finally, the governments.

1.4.2 Research hypothesis

The study will be focused on the following hypothesis question:

H1: Are social media platforms putting users at more privacy and security risks?

H0: Social media platforms are not putting users at any privacy and security risks.

1.4.3 Current mitigating techniques

There have been a number of mitigating techniques put forward by social media companies to help users deal with all the privacy and security issues that they are facing on

social media. These have come from social media companies and some concerned organizations, as detailed below:

a. Social media platforms are trying to give users some level of control over their privacy via security settings. Although this control is very limited, it can help defeat the petty burglars and other profile-ogling attackers. Social media platforms have continued to provide more privacy controls that users can implement to limit the people that can view their profiles and posts. The same controls can also be used to limit people who can contact them or tag them in pictures. These controls are quite helpful but not an assurance that one's information will remain private. Social media companies, such as Facebook, are continually updating their users' security settings to make them more understandable to novice users (Larson, 2018). Facebook has also tried to simplify the presentation of the security options that a user has (Locklear, 2018).

b. Organizations have taken up the responsibility of keeping their employees safe on social media ("Employee Training is the Only Way to Prevent Social Engineering", 2018). They are scared of attacks such as social engineering that may come back to haunt the organization itself. They are, therefore, spreading awareness on the risks and threats lurking on social media. They are also teaching their users on how to secure their profiles from these attackers ("Employee Training is the Only Way to Prevent Social Engineering", 2018). A bigger part of users is not aware of some of these threats, and attackers are capitalizing on this. The efforts to spread awareness are also not so motivated. The laxity of users in implementing what has been taught is also a big challenge.

1.5 The scope of the research

This research has a wide scope. It looks at the privacy issues on social media platforms and also touches on the security issues faced by users on these platforms. On privacy issues, it looks at the issues emanating from social media companies and those coming up due to the careless sharing of information by users. This is what connects the research to the security issues on social media. Careless sharing of sensitive information on social media is the course for some of the security issues on social media. There are many cyber attackers on social media busy collecting the sensitive information so that they can utilize it in attacks. The research, therefore, combs through the privacy issues and security issues on social media. In its recommended solutions, the study also gives attention to the two issues. It focuses on governments, users, and social media companies and gives practical solutions for both security and privacy issues on social media platforms.

1.6 The aim of this research

The thesis aims at addressing the social media privacy and security issues that users are currently facing. It aims at coming up with workable solutions that they can implement, legal measures that governments should take, and responsible actions that social media companies should take in the best interests of the defenseless social media user. It also aims at informing users on the social media about the threats they may face and empowering them by teaching them the techniques they can use to mitigate these threats.

1.7 Contribution of the research

This thesis makes significant contributions to social media security, user privacy, and the challenges of cybersecurity related to social media:

a. On social media security, the thesis explores a big privacy and security problem that users are not aware of. It highlights the threats that users are often blind about and yet have severe consequences.
b. The thesis also makes contributions to the issue of user privacy. It is a big issue that is not just limited to social media platforms. There are many other cases of user privacy invasion by employers and even by governments. However, the research explores what is currently the biggest privacy violation and risk—privacy invasion by social media companies.
c. Tied to user privacy is also the issue of oblivious sharing of sensitive information. The research looks into this and makes contributions on how the issue should be handled.
d. Lastly, the thesis makes many contributions to cyber security. It focuses on social media threats and social engineering. These are two of the most prevalent security threats that today's Internet users are facing.

Chapter 2: Literature review

2.1 Preamble

The previous chapter has clarified about the issue of social media privacy and security. It has also given the motivation as to why this research was required, by highlighting the problems currently being faced and the existing solutions. The limitations of this research have also been highlighted. The boundaries of the research have been defined and its goals, clearly stated. In this chapter, the research will look at the previously conducted studies on the same and identify the problems they sought to research, the type of research they did, the results they found, and the recommendations they gave. The social media privacy issue sprung up in the last ten years when social media sites were being developed and introduced to the public.

It is important to note that in their early stages, most social media platforms that exist today were not monetized. The developers had only been focusing on how to build the platforms and get more users. Some of these platforms were actually against any ideas of monetizing their platforms. However, within the last ten years, the contrast happened. Most of the social media platforms had gotten a significant number of users, mostly in the range of half a billion users. They, therefore, saw it viable to monetize the platforms and this is when trouble started brewing (Robertson, 2018). They started collecting user information just to profile it for advertising purposes (Robertson, 2018). Even worse, at times, this data was sold to third parties. Another problem also came up. Attackers started fetching information about

users on social media and using it to exploit them. Researchers then started focusing on the issue of user privacy and security on social media platforms. A number of researches have been conducted on it, and they have unearthed a lot of problems and given their presumed solutions to this problem. This research honors the works done by four researchers that have looked into the issue of social media privacy from interesting perspectives. As a foundation to what has already been done on the topic, it will discuss, in depth, these researches, how they viewed the topic, the type of study they did, the results they arrived at, and the solutions that they gave.

2.2 Literature review

2.2.1 Privacy issues prevailing in social media

The research proposed by Loeffler (Loeffler, 2012) makes contributions on the privacy issues that are prevailing in social media. Loeffler decides to examine the legal responses to the issues flagged by users as being rather intrusive to their privacy on social media platforms. He mostly looks at the administrative policies and regulatory measures that governments may have to come up with in order to control the issue of privacy and personal data security. He gives three recommendations and the first one is that privacy should be incorporated into the design of the social media platforms. Secondly, he says that users should be provided with options concerning their data. Lastly, he calls for social media companies to provide transparency concerning the use of user data. This study does agree with all his recommendations and, especially, the call for social media platforms to provide transparency as to how they are using the data they collect.

In the article, the author first looks at the current status of social media. He talks of there being an ‘explosion’ in the usage of social media, whereby at least 66% of all adults are on one type of social media platform with millions visiting the site every day. He tries to

explain that the general public is increasingly becoming worried about the use of personal information that social media platforms have been collecting from their accounts. Of the keenest people on user privacy that Loeffler (2012) talks about, investigative reporters, regulators, and privacy activists make it to his top 3 list. He attributes the increasing public vocal movement against privacy issues on social media by users to these three types of people.

Loeffler (2012), being so concerned with the legal frameworks that should be in place to regulate social media, starts by looking at the existing legislations against privacy. He, however, complains that most laws on privacy are aged and are not effectively applicable in an online environment. He takes a keen look at the US, whereby he says that there has not yet been a comprehensive legislation concerning online privacy. He calls the existing laws being used by courts as a 'patchwork' of regulations and says that these only address few segments of personal information. This study does agree with him that the existing privacy laws in the US are either aged or simply incapable of addressing the current situation in a comprehensive manner. Loeffler (2012), however, praises Federal acts for having more solid coverage on privacy regulations. He gives an example of FTC Act 3 that has been put up to prohibit against businesses using deceptive acts to infringe customer privacy rights and threaten their data security. He also brings to light a children online privacy act called COPPA. He says that this is probably the best-defined act in terms of what personal information encompasses and has been established in order to protect children under the age of 13.

Loeffler (2012) moves on to discuss other pieces of legislation with general applicability on privacy. He brings up the FACTA act that mandates any business that collects sensitive customer information to be able to safeguard it up to a defined standard. Of course, many social media platforms fall here but the question is whether they protect user data up to the specified level. Loeffler (2012) also talks about the closely related FCRA act

that was established to deal with the issue of identity theft. Identity theft is still an issue on most social media platforms; thus, this rule is very applicable. These two acts actually present major challenges to social media companies. They draw limitations as to how customer data can be used and shared by the companies that collect it, and to top it all, they also give out some practices. Loeffler (2012) brings to attention a recent amendment to the FCRA act called the Red Flag Program Clarification Act that demands businesses acting as keepers of user information to develop systems and procedures to prevent identity theft and protect user information. Another act that Loeffler (2012) talks about is the HIPAA act that protects the usage and disclosure of personal health information. Another substantial act that he talks about is the Electronic Communications Privacy Act, which talks about issues such as eavesdropping, wiretapping, and how communications should be stored.

Loeffler (2012) finishes off his legislations review by looking at some US state laws that have been put up against user privacy infringement. He refers to these as additional patchworks to the existing shoddy legislations that have no comprehensive coverage on the broad issue of privacy. He says that it is the state Attorney General that is actually in charge of enforcing the appropriate privacy practices. He gives an example of the state of California, which has mandated all commercial websites that collect user information to provide users with a privacy policy. The privacy policy is to effectively talk about all the types of information that the website may collect and which third parties the information may be shared with. When the collected information is to be shared with third parties, the state requires the website to openly disclose to the owners of that data about the sharing and also provide them with ways to opt out. Loeffler (2012) also lightly talks about the state of Massachusetts and its regulations towards information security that protect user privacy.

Just to expound on the privacy violations, it is good to incorporate other violations noted by Martin Kristen (2016) in his research on the topic of online privacy. His focus is not

limited to social media and his recommendations are applicable on social networking platforms. He calls for the development of strong social contracts to guide privacy (Martin, 2016). He illustrates the degeneracy of privacy on several social media platforms. His first illustration is based on a feature introduced by Facebook in 2012 called sponsored stories (Martin, 2016). When Facebook users liked a posted sponsored story, their pictures would be taken with an endorsement of the story and then shared with their friends. Obviously, this was sponsored advertising where Facebook would just use the users for promotional purposes without getting their consent (Martin, 2016). A like on a post did not warrant the user of a profile to advertise a story to his/her Facebook friends.

Martin gives another illustration where he explains that Facebook mines a user's browser history so as to conduct target advertising (2016). The user's browser behavior is recorded using data-hungry cookies. Facebook then uses what the user typed in search engines and the web pages that he/she visited, in order to show advertisements. He observes the same issue with a travel search engine called Orbitz (Martin, 2016). The site aggregates the costs of fares, food, and accommodation to several destinations globally. If users arrive at the site from a competitor site, such as Trip Advisor, the site will have some bias in the pricing that it shows. It is not entirely illegal to collect user information through cookies but some practices such as the one Martin Kristen observed about Orbitz are now raising ethical concerns.

In his last illustration of privacy violation, Martin Kristen mentions a service called Precision Market Insights offered by Verizon, which allows businesses to mine its customers' call and browsing industry (Martin, 2016). The end goal is for the businesses to get fine details of where the customers are, the services that they consume, and some other preferences. Verizon has previously confirmed user-tracking rumors saying that it understands a customer's daily activity stream (Martin, 2016). This is the information that the

company sells to third parties. The same can be said about social media sites such as Facebook. Facebook extensively tracks its users and sells the data to other businesses. Martin Kristen does a good job in highlighting and relating these privacy violations and they add weight to Loeffler's privacy concerns. They also help explain why a number of these social media platforms have been settling court case after court case. It is because they are no longer valuing privacy.

The privacy violations by social media sites that both Loeffler and Martin Kristen report have been happening for some time now. There might be others that are being carried out while obfuscated from the public. The findings by these two authors warrant for further researches to be done on this topic. A lot more solutions need to be found to at least contain the issue before it spins out of hand. Users need better ways to guard their privacy. A more amicable agreement needs to be found between users and social media companies concerning the use of personal data collected from social media sites. Martin Kristen tries to bring a solution through a well-defined social contract between users and social media companies (2016). His social contract is aimed at bringing the two significant parties in this issue of social media privacy and then coming to understanding of the needs and limits of data collection (Martin, 2016). Other than this, there will just be a never-ending battle against the invasion of privacy by social media companies.

The pieces of legislation discussed by Loeffler so far have had far reaching implications on social media platforms. Loeffler (2012) gives examples of companies that have had to agree to various settlements for breaking the existing incomprehensive laws. Despite collecting and keeping sensitive user information, these platforms have not put in ways to adequately protect the user data, and they also share out private data to third parties. It seems to be a cat and mouse game between the law and the social media companies. That is why Loeffler (2012) calls for privacy to be incorporated in the design of these platforms, give

users options, and for there to be transparency as to how user personal data is collected, stored, and used.

This thesis highly regards the contributions of Loeffler (2012) and the supportive contributions by other researchers on the prevailing issues in social media. These researchers have indeed confirmed that there is a problem; user privacy is being violated. They have illustrated of how this privacy is being violated. Loeffler (2012) has even explained the court cases that these social media companies have been facing and the consequences that they have faced. There has been an examination of just how far the current social media privacy controls afforded by users have gone. Unfortunately, they have not gone so far as to protect the privacy of users from social media companies. This thesis will take all this information presented by the researchers into account when formulating its own recommendations. This thesis is of the opinion that a solution can be found. The current social media companies do not have to shut down; they only have to mend their ways. A compromise can be found between users and social media companies. The contributions from these researchers will come in handy when making the recommendations.

2.2.2 Two perspectives of privacy

Another relevant piece of literature in social media privacy is a research done by Heyman, Wolf and Pierson (2014) concerning the social media privacy settings. The purpose of their research was to basically evaluate the two types of privacy—one between two users and the other between a user and third parties (Heyman, Wolf & Pierson, 2014). Briefly touching on the findings, the trio found out that the users were given more privacy options to control the access of their personal information by other users than third parties or social media companies themselves. Basically, users could only hide their private data from other users but not from third-party applications on a social media or the social media company.

The research paper begins by talking about the existing problematic view of privacy. It insists that there are two types of privacies that most people see as one. The first type is whereby privacy is a subject and this is the normal social privacy that users enforce against each other. There is, however, another type of privacy termed as 'privacy as an object' whereby, at this level, personal information can no longer be seen by other users but, rather, by big data algorithms. The trio claim that by separating the two types of privacy, they can effectively prove how social media companies have left some exploitable blind spots on the side of user privacy. Social media platforms basically try to delve into the subjective privacy, that is, the privacy amongst the users. They effectively hide a loophole in the objective privacy where the user data interacts with third parties and some big data algorithms (Heyman, Wolf & Pierson, 2014). The three researchers look at the settings that Facebook and Twitter give to their users in order to control their privacy. They then evaluate the design of these settings according to Donald Norman's stipulations for human-centered interfaces.

The three researchers begin by briefly explaining about the two privacy perspectives that they set out. They say that on social media platforms, there are two flows of information even though users might think that there is one. The first and obvious flow of information is between users and, at this stage, the account owners can determine what can be viewed or accessed by others (Heyman, Wolf & Pierson, 2014). However, in some incidents, users cannot really limit their posts from getting to unintended people. If a Facebook user chooses to post a picture and set it to be visible to her Facebook friends only, there is no control to bar the friends from further broadcasting the picture. This has been an issue that courts have clarified. They have said that one fortifies privacy interests of any information that they choose to post on Facebook.

In 2017, Mark Sableman made a contribution that was particular to this issue of limited privacy controls that users have. He gave a real-life illustration of a court case by a

Facebook user called Chelsea Charney (Sableman, 2017). A court threw away the argument she presented in court that since she had set a post to be visible to Friends of Friends, she had protected her privacy or had acquired semi-privacy for the post (Sableman, 2017). The court said that while she (Chelsea) was able to select her Facebook friends, she was not in position to select the friends of her friend (Sableman, 2017). Therefore, the post was availed to hundreds or thousands of people that she did not know. The court also leaned to the legal precedence that one should not have any expectations of privacy for information voluntarily given to third parties (Sableman, 2017). This contribution therefore illustrates that users ought to understand that they should be wary of the semi-private privacy settings offered by social media companies. They can only provide limited control of what other users can see on one's profile.

The second flow of information goes to third parties and the social media platforms themselves (Heyman, Wolf & Pierson, 2014). Users have no control whatsoever and whatever they publish, be it public or private, is streamed directly to these two. This is the most threatening part of social media, they say (Heyman, Wolf & Pierson, 2014). These third parties see users as mere assets and they are in a position to collect all the personal data of these users without being barred or limited by some settings.

The three researchers refer to an earlier research done by the European Commission, called the Eurobarometer. This research was done in Europe and it studied the opinions that Europeans had towards sharing data, and the effects these opinions had on their data sharing habits on different platforms. In the research, the European Commission came to discover that from 100% of the respondents, 44% worried about their data being collected without their consent, 38% feared of it being shared without their knowledge, 32% feared the threat of identity theft, and 28% feared that it would be used for advertising purposes (Heyman, Wolf & Pierson, 2014). All these were different threats that the European Commission

obtained directly from the users in that region. The users were not in a position to control the threats identified using the basic privacy settings that social media platforms provided. This further exemplified the two types of privacy—one that is controllable and one that is at the mercy of the platform and third parties.

Heyman, Wolf and Pierson (2014) cling to a definition of privacy as the rights of an individual to decide what information can be given to others about him. They say that information disclosure must be surrounded by some rules and they should delimit who this information can be shared with. The privacy settings provided by the social media platforms are supposed to act as enforcers of these rules concerning disclosure according to the researchers. However, social media platforms are said to have taken advantages of being the system designers and severely limited the control that users have on their data privacy. They have played an unfair game with the affordances of the privacy settings. The three describe affordance as the relationship between an object and a user with regards to the properties of the object. A designer is in a position to limit the functional properties of an object as they make it. This is exactly what social media platforms have done; they have been clever in severely limiting the kind of privacy that a user can control. A user is able to impose privacy control over other users but not third-party apps or the platforms themselves. These platforms have not provided any means for a user to be able to control the access of data by third parties, yet they have been given access to more confidential data.

The three researchers take the time to explain more about the two types of privacy. The first one, privacy as a subject, is said to be when users are actors who make and manage their online identities (Heyman, Wolf & Pierson, 2014). This type of privacy only controls the flow of information between people. This is the one that social media platforms have really tried in ensuring that users can control what others can see. However, the user has been given an active role in controlling this privacy through the tweaking of a few settings. A user

can limit the people who can view his/her profile, block users from messaging him/her, and, also, change these settings later on. The three researchers, however, disclaim that there are some problems with this type of privacy, but they are quite different from the other type of privacy. First of all, the idea that it is a person who creates an online avatar using whatever data he/she pleases introduces some problems, that of identity theft, creation of false identities, and the inability to control the access of some aspects of private and public information to different the audience. Users have to make tradeoffs between privacy and identity, and too much privacy would mean seclusion which is not the intention of people joining social media sites.

The second type of privacy, privacy as a subject, is said to be the most controversial type of privacy (Heyman, Wolf & Pierson, 2014). The three say that the user data is basically stored in a database containing the records of millions of other users. This data is referred to as big data and it can be mined by using various tools that are powered by complex algorithms. This is done via a process called Knowledge Discovery in Databases. The trio does confirm that this is the data that social media platforms make money out of. They explain that the platforms generally collect and store all the data that a user creates on the social media platforms and use it to classify the users into certain profiles. These profiles are used to bundle users into certain groups as consumers, and the type of products the users may buy can be predicted. The only purpose of this profiling and bundling is to make a commercial value out of the user data.

Users are basically transformed into commodities and they are actually sold to companies seeking a particular audience. The audience may be people within a certain age bracket, with a certain level of education, who live at a given place, and so on and so forth. There have been heated debates around this type of privacy. Users are complaining that their privacy rights are violated from the moment they are put into these databases. Social media

platforms are not totally transparent about the type of data they collect, how it is used, and which third parties have access to this information. The three researchers describe users as laborers who do not receive any pay. They take their time to create online personalities, they generate content that keeps other users visiting their platforms, but what do platforms repay them with? Total prostitution of all their data to third parties and the users have no say about what can be shared with the third parties.

The three conclude by looking at Norman's views of affordances. They say that social media platforms should focus on using various affordances in the privacy settings to empower users rather than disempower them (Heyman, Wolf & Pierson, 2014). They define empowerment in this context as being in control of one's life or having mastery over one's affairs. They share a low opinion of the current affordances that these platforms have given to the users. They refer to an earlier research that found out that there still were many people unable to change their privacy settings due to lack of knowledge or uncertainties. This, they say, makes it even harder for users to control their subjective privacy. Secondly, users are said to have no control over their objective privacy. This is where they are basically seen as commodities and sold around to different third parties. The three researchers share the results of their research on Facebook, Twitter, and LinkedIn, and they call for the inclusion of more but simpler privacy settings on the platforms. Also, they talk about the platforms putting in place default settings that promote privacy.

In support of the recommendations listed above, John Drake came up with more ways to protect social media privacy. In his 2016 research, he recommends that businesses should avoid violation of the privacy of other people just for some short-term goals (Drake, 2016). Drake's recommendation might be subjected to the small businesses that he touched on in his research but can be extended to social media platforms. His research encompassed businesses with a tendency to violate job applicants' social media privacy by invading them to gather

and analyze data that they can use in the hiring or termination process (Drake, 2016). The same level of evil is already taking place in many social media companies. Social media companies are invading the privacy of social media users just to fetch information that they can use for advertising purposes. As Drake (2016) warns, this is for a short-term goal and there might be negative implications in the long term. For instance, if users decide to abandon social media platforms that have been associated with user privacy violations, their long-term business will be lost. With the coming up of an increasingly privacy-aware generation of Internet users, it is not far-fetched to imagine a point where Facebook will have lost many users if it continues with its current trend.

Drake (2016) also recommends for the observance of user privacy even if the users do not have a distinct right to it. This is very important since users are not granted a right to privacy in many countries. There is no constitutional provision for this right. Drake is seen to be driving a more ethical debate that aims at encouraging businesses to respect users' privacy even without an obligation to do so. This recommendation seems to be tied with the above-stated recommendation. If social media companies fail to respect the privacy of users, there is no guarantee that these users will remain on the platforms in the long term. A startup might create a privacy-aware platform that might quickly gain adoption from users, thus leading to a starvation of users in the privacy-violating social media platforms. Lastly, for a long-term solution, Drake (2016) says that there has to be respect of privacy and the enforcement of individual rights. This recommendation brings into the picture the role of legislators in different countries or regions. It is high time that legislations are formed to protect an individual's privacy. Privacy needs to be made an unalienable right unless there are legal grounds to challenge this. It is currently being taken for granted and even though some legislators have taken up the issue, many others are yet to react. Social media platforms need

to be controlled when it comes to the boundary between their business interests and the privacy interests of their users. Drake seemingly understands this, hence his recommendation.

2.2.3 Privacy comparison between China and the US

Another relevant piece of literature is a research conducted by Nemati, Wall and Chow (2014) concerning privacy copying of users in the US and in China. The researchers say that there have been too many studies done on the issue of privacy due to the social media settings. However, there has been little research done on the privacy issues that may come about due to user-specific characters in different regions. The study also looked at characteristics such as social media addictions and the different views on the perceptions of online identities. The researchers maintain that the different characteristics of users may expose them to different types of privacy violations (Nemati, Wall, & Chow, 2014). In their research, they found out that the Chinese users of social media were at more risk of privacy violations due to their online behaviors as compared to the US users (Nemati, Wall & Chow, 2014). They were found to have poor privacy coping behaviors and, thus, had a tendency to share more sensitive information.

The researchers say that irresponsible use of these social media platforms and sharing a lot of information had far reaching consequences to users. Among the greatest risks that this would expose an individual to, the leading one was identity theft. The researchers explained that the users had various ways of coping with the current privacy issues that were increasingly being brought out about social media. The three stuck to an opinion that different populations or cultures had different privacy concerns. Some populations had a high value for their data while others had less concerns. Their different privacy concerns led them to change their information sharing habits in a different manner from those who had little concerns about their privacy and did not change their privacy habits

The researchers conducted online surveys related to their privacy concerns and information sharing habits on respondents from both China and the US. There were three aspects that were closely examined and these were: a user's comfort when sharing data publicly, the amount of personal data they gave on their accounts, and their willingness to change their habits to cope with privacy concerns. The researchers sought to find out just how vulnerable different users were to privacy violations by social media platforms, third party applications, and other malicious users (Nemati, Wall, & Chow, 2014). Based on this research, the three would use the findings to push policy makers and social media platforms to further make provisions to these types of vulnerable populations. These were users who were unaware of the risks they were exposed to and thus had very little concerns about their privacy on social media. These were users who had very little barriers as to what they could post on the platforms.

The researchers identified several characteristics that distinguished the users of social media. The first characteristic was the national origin of the users, whereby they said that users from different nationalities could also exhibit different online behaviors. Some nations are advanced in technology and most citizens are learned and, thus, are fully aware of the risks on social media. In other nations, there are very few literate people, especially when it comes to technology, and thus, the nationals have little awareness about the risks on social media. The second characteristic that was used to differentiate users was the level of Internet addiction. It is not an unknown fact that there are some users who have become addicted to some social media platforms due to the content they see. The researchers pointed out that addiction to the social media platforms was a real problem in places and the same could be said about gaming (Nemati, Wall, & Chow, 2014). There were users who had strong compulsions to stay on several social media platforms for extended periods of time and even forego doing other things just to stay on the platforms. The third characteristic that the

researchers used was the sense and concern of a user's online identity. This was all about a user's personal profile on the social media platforms. The study said that users with different concerns about their online identities would have differing privacy concerns. This would ultimately affect what they could or could not post on the social media platforms.

The research findings had interesting but expected outcomes. It was found out that China had more users with characteristics that made them unsafe and more prone to privacy violations (Nemati, Wall, & Chow, 2014). It was also found out that more Chinese users were free and willing to share their personal information publicly. This, thus, put them in an unsafe position when it came to different online threats. The Chinese users were used to a culture that had lagged approach to online threats. They were willing to share their real private information on social media sites and were also less likely to withdraw the information due to fears of privacy violation or other social media threats. This was understandable due to the political restrictions the country had on some social media platforms. Some, like Facebook, were actually banned and these were people looking for any social platform to be able to interact. Therefore, they were ready to publish their actual information without fears that this may have negative consequences. Their main concern was just developing and maintaining connections with others on the Internet. US users, on the other hand, were more reserved towards giving out their personal information (Nemati, Wall, & Chow, 2014). They have access to many platforms, they are more aware of privacy concerns, there are many cases of identity theft, and, generally, the citizens are cautious about what they post.

Another finding was that there were higher addiction rates to social media platforms in China than in the US (Nemati, Wall, & Chow, 2014). The researchers co-related addiction to more careless behaviors on social media, such as posting sensitive information or readily engaging in chats with random strangers. They say that Internet addiction led to users spending more time on social media platforms and, thus, the users were more prone to

sharing a lot of their data with others, third-party applications and the platform itself. These were the users who needed to be more worried about the type of data they shared but on the contrary, they were more 'careless' with their information sharing tendencies. There was also another finding concerning the users' views on the worth of their identities, and this was rather an extrapolation of the results observed in the other characteristics. Therefore, most of the users who had a high addiction to social media and those that were from cultures that were not very concerned with online privacy turned out to have fewer concerns about their online personalities (Nemati, Wall, & Chow, 2014). Those that had a lot of concerns about their online personalities were more responsible with the type of information that they posted on the social media platforms. These were mostly the US respondents, since they extended their real lives on social media. In China, however, there were more respondents who were not concerned about the worth of their online personalities and would, thus, post just anything on the social media platforms. They were not much concerned about the impacts this would have on their online security or in real life.

Nemati, Wall and Chow (2014) affirmed that there was a growing sense of concern towards online privacy. It was, however, upon policy makers and social media platforms to put in place ways to protect the rather unaware group of users. These were users who did not have a good understanding of the severity of some consequences of posting just any type of data on the Internet. China was just an example because there are other even more critical places, such as the third-world countries. Therefore, with this type of users, the policymakers were highly encouraged to come up with legislations to prevent these users from being taken advantage of, especially by third-party applications and malicious people (Nemati, Wall, & Chow, 2014). Also, these legislations would encourage users to be more concerned about their online personalities and to understand the privacy issues surrounding the cyberspace. Social media platforms were also encouraged to help protect these users and promote

awareness towards the presence of some vulnerabilities. A good way to do so would be to have a pop-up reminding visitors from these regions to be more careful with their data. There was also a recommendation that sought the intervention of clinical psychologists. It was found out that there were some users that were heavily addicted to social media platforms, and this was possibly ruining their lives. Clinical psychologists were encouraged to be more receptive to these types of users and give them guidance that could help them break the addiction.

In conclusion to this thesis, the researchers have highlighted that there were some limitations in the research about the user characteristics that affected their privacy. They did encourage more researchers to delve into the area. This thesis totally agrees with most of the findings and claims that there were very few researches done in the area. It is for this reason that that this thesis has decided to incorporate into its study the impact of user characteristics in the issue of online privacy. This thesis makes significant contribution to the topic of social media privacy because very little research has been done about different cultures and their interpretations of online privacy. Their work is therefore highly regarded by this thesis and some ideas will be borrowed from it.

2.2.4 The mechanics of interpersonal privacy on social media platforms

The proliferation of social media platforms, such as Facebook, which has over two billion users, has welcomed researchers to do more studies on privacy. As Bryan Hammer (2013) explains, most people are used to architectural privacy, which is given by means of privacy policies on websites. This architecture, which has been made mandatory by most countries, establishes the privacy between a user and an organization or the individual owner of the website. On social media, however, users largely interact with other users and the privacy definition between them is lacking. Users are tasked with managing their own

privacy by the social media platforms. The platforms give a number of ways to secure their privacy but it is ultimately upon the users to use the techniques and controls given. Hammer, therefore, questions how privacy influences the way users share their personal information on social media sites. He comes to three answers to this question, answers that shall be expounded on. The first one is that users are driven to share a lot of personal information by the fear of social exclusion. The second one is that it depends on the multiplexity of relationships on a user's accounts; that is, it depends on the people the user is friends with or is followed by, who will see the posted information. The third answer that Hammer arrives at is that it depends on a user's subconscious approach of whether or not to share his/her personal information on social media platforms. Combining the three, Hammer says that users share personal information on social media platform due to their attitudes and perceived beliefs towards interpersonal relationships.

In his research, Hammer (2013) starts off by explaining that there seems to be an ever-changing balance between privacy and personalization on social networking sites. Supported by other researchers, Hammer argues that social media users want to have the freedom to socialize but at the same time require to be afforded some privacy protection. It is apparent that privacy is, then, hard to define as users want to participate in a global society brought to them by the social media sites. Hammer (2013) explains the sharp difference between social media sites and other types of sites. The real motivation to use social media sites is intrinsic while most other sites offer extrinsic fulfillment. An example he gives is an e-commerce website where the motivation to use it is extrinsic and outcome-oriented. He contrasts this with social media sites saying that these are process-oriented in that users are mostly looking forward to social exchanges with others. This is what gives them joy and fulfillment. With this explanation, Hammer expounds his research question of the influence

of privacy on the sharing of personal information on social media into smaller questions. He poses the following questions to help guide his research:

1. What theories can enhance our understanding of privacy in social media sites?
2. In addition to the theories, what constructs can enhance our understanding of privacy?
3. How will the conceptualization of privacy differ between a process-oriented system and an outcome-oriented system?
4. What individual differences exist related to how individuals perceive privacy?
5. How can researchers resolve the debate as to what privacy is as a concept? (Hammer, 2013)

To answer these questions, Hammer decides to give three viewpoints. These were as outlined earlier in this chapter and will be discussed in-depth. In his first viewpoint, he answers the first three questions listed above. In the second viewpoint, he answers the fifth question. In the third viewpoint, he gives an answer to the fourth question, as we are going to see below.

The first viewpoint: The need to belong vs. the need for privacy

While opening his discussion on this perspective, Hammer first explains the Need to Belong theory, which states that humans wish to live and interact with others to gain some benefits. This brings about two things. The first one is a need to get into positive interactions and the second one is to reciprocate the concern for each other's welfare. Hammer says that social media sites have been built to satisfy both of these. This, then, brings about the fear of social exclusion as a motivator for users sharing information on social media. Humans will try and avoid the fear of being rejected by or separated from the others. They will, therefore, be more willing to engage in conversations or make posts on social media to remain in touch with others. Hammer says that this gives a succinct answer to the first, second, and third research questions. As will be further discussed, Hammer gives a number of respondents a

survey to test a user's willingness to post varying levels of sensitive information based on the desire to belong to a group.

The second viewpoint: Privacy conceptualization using the social network theory

Hammer faults the existing conceptualizations of privacy that have only focused on individuals. He claims that in the context of social media, interactions and exchanges do not involve individual users. Therefore, the conceptualizations of privacy in this space should encompass social interactions between multiple users. As such, he says that a social network lens should be used. There should be a focus on the relationships between interacting individuals and the roles some individuals play in a social network. All these contribute to the privacy stands a user might take on social media when interacting with other users. Hammer introduces the term multiplexity, which he defines as a relationship formed over time between people that features multiple ties. He says that this type of a relationship takes time to form and it features an increased rate of interaction between people in the relationship. It also features interdependency and this leads to the reciprocation of concern between those in the relationship. To prove this viewpoint, Hammer does a survey where he selects users, bounds them into groups, and asks them which other users they would be willing to share some sensitive information with. This information is used to assess the multiplexity in their relationships.

The third viewpoint: The subconscious privacy mechanism

Hammer insists that till today, there have been challenges in defining what privacy is. He says that there has not yet been an agreed upon answer and, therefore, privacy is conceptualized as a right, a commodity, a state, or a control. In a search for the right definition, Hammer switches to neuroscience and psychophysiology. He says that privacy as a behavior is characterized by how one shares or withdraws from sharing some information. It is an approach-avoidance behavior where approach behavior is exhibited to get a positive

result whereas avoidance behavior is exhibited to avoid a negative result. With this view, Hammer says that privacy can then only be studied using psychophysiological tools, since approach-avoidance behavior is exhibited at an unconscious level. Therefore, a survey would not be effective at showing this. While laying his arguments, Hammer says that the individuals with the approach behavior are more likely to share their personal information on social media than those with an avoidance behavior. To test the psychology behind privacy, Hammer uses some psychophysiological tools to monitor heart rates of participants while immersed in Facebook-like scenarios.

Hammer breaks his research into three essays based on the three viewpoints introduced above. The following are the essays that make up the major part of his research:

Essay 1: Varying information sensitivity of personal information

In the introduction to this essay, Hammer highlights that privacy management has been a topic of interest due to the wide adoption of IT into people's lives. It is this adoption that has seen people share out a lot of their information, something they would traditionally avoid doing. A question of interest he poses in this essay is why an individual would give up his or her privacy on social media sites. He explains that in social media sites, users ought to understand that it is the data that they share with other users that is mined by the platforms for more personalized adverts, marketing for partners and even customizations for third-party sites. Platforms such as Facebook will scrap all usable information from posts, messages, and sites visited by a user, and even photos posted (with their face recognition engine). Due to this, Hammer says that Facebook is only motivated towards encouraging users to share out their information. This is what is good for business. If users stop sharing the information, Facebook's business will be immensely affected.

Hammer says that privacy organizations have faulted the likes of Facebook for not providing users with sufficient privacy controls. The organizations have further stated that the attempts by social media companies to enhance their privacy controls have not been satisfactory and more still needs to be done. Hammer, however, believes that there is a misunderstanding due to the context of social media. It is unexpected that Facebook can match the privacy levels of a site such as Amazon. The users on those sites have different expectations. For Amazon, the users will appreciate to know that their purchase history is safe, their payment details are confidential and their delivery addresses are never disclosed to the public. Facebook users, on the other hand, want to post messages to other users, upload new photos, chat with friends, like and comment on photos of friends and family as well as read the comments on their own photos. The interactions described show that users in Facebook want to continuously engage with other users by means of sharing some information. They are looking for the social experiences, they want the enjoyment and satisfaction derived from those actions. Privacy is, therefore, not comparable between social media sites and e-commerce stores.

Hammer also introduces the issue of the types of relationships on social media. He gives another e-commerce example where he says that a transaction between the vendor and the customer involves some privacy concerns. The customer is very concerned about the privacy of his/her personal details, and this will form the basis of the relationship between the customer and the social media site. On social media, the information shared is mostly intended to reach particular persons. Therefore, privacy concerns in social media are context-specific and they also depend on the agent a user interacted with and the type of information that was shared. Hammer chooses to focus on the type and the sensitivity of information shared on social media.

In his research for this essay, Hammer chooses Facebook as the testing platform. He says that his focus is on the user-user relationship. He poses a question about how privacy influences the sharing of personal information in interpersonal relationships. He brings up three points: how privacy differs in process-oriented and outcome-oriented systems, theories for a better understanding of privacy, and how the sensitivity of the material to be shared affects how it is shared. To carry out the study for this essay, Hammer gets a focus group that is given information on the different sensitivity levels of information of social media. He then carries out a pilot study to assess the fear of social exclusion and intention. He then takes another sample and carries out the real experiment.

In his findings and conclusion for this essay, Hammer says that there is a strong effect of interpersonal beliefs on privacy concerns. Therefore, users will share more personal information with the people they have strong relationships with. He also says that the fear of being secluded only factors into the sharing of personal information only when the information is of low sensitivity. Therefore, people that feel like they are secluded on social media will give out some information on these platforms but it will not be highly sensitive. Hammer believes that his study takes an often-ignored route in the research about social media privacy.

Essay 2: Reconceptualizing privacy through social network analysis

Hammer introduces this essay with a question as to why users share their personal information and at the same time want privacy. To explain the reason, he begins by explaining that social media activities occur between entities and these entities mostly have some sort of a relationship. In some incidents, this relationship is one-dimensional, especially in the cases of forum posts. The aspects of relationships have not been looked at in privacy literature, he says. He exclaims that this is despite the fact that social media sites are characterized by richer relationships than other types of sites such as e-commerce stores. The

relationships in the sites influence the way users act on social media and on other types of websites. He then introduces the research to multiplexity, social norms, and moral influence on user privacy concerns. In this essay, he focuses on investigating the reasons why the relationships on social media platforms cause users to lay low their privacy concerns and share their personal information.

Hammer first refers to another research paper that gave meaningful categorizations of the conceptualizations of privacy. The paper gave two categories: value-based, which views privacy from an ethical lens, and cognate-based, which views privacy as a cognitive phenomenon in one's brain. He elucidates these conceptualizations, starting with the first one where he says the EU acts as a block to protect its users' privacy from third-party sites while the US does not. This is a real-life view of the conceptualization of privacy as a value that is recognized by some institutions such as the EU. As for cognate-based conceptualization, he says that privacy is viewed as an abstraction that exists outside institutions and is fully under the control of an individual user.

Hammer then explains the need to belong theory, which explains a user's interest in being in a relationship with others or being part of a group. This is characterized by frequent interactions and reciprocity of each other's welfare. Social media sites cater for these two by giving users multiple ways to start interactions with other users and many ways for other users to respond to an interaction. He then explains multiplexity of relationships as the different direct ties between people in a relationship. He explains that social media sites encourage the formation of multiplexity of relationships. This makes users feel more secure to share details with other users since they are in a rich relationship with them and have several ties built over time on the platform. In his study for this essay, he investigates whether an increase in multiplexity of a social media relationship leads to more trust among the

affected users. In his second hypothesis, he seeks to know whether multiplexity in a relationship leads to a decrease of privacy concerns between users in the relationship.

In his research, he selects a sample of student-run Facebook groups from a US university. These groups were games-related and had been created by students that had something in common such as graduating, being ineligible to play, being injured, and so on. The study was conducted through interviews with the individual group members, mainly to determine their relationship with some other group members and what they could share with them. In the results and discussion, it was determined that the type of relationship that a user had with another or several others influenced the type of information they could share. Those that had relationships with multiplexity were found to share more highly sensitive information with other users. This research, therefore, introduced another dynamic in privacy, multiplexity in relationships.

Essay 3: Privacy-related behavior through activation and inhibition systems

The third essay that Hammer writes in his research is about privacy as a behavior that can be activated or inhibited by one's psychological system. In this essay, he views privacy as a non-conscious element of the human brain. Therefore, it cannot be studied through the normal research tools such as surveys. He says that privacy can be studied using psychophysiological tools and also implicit associations. He explains the reasons why he views privacy as a psychological issue. In his explanation, it is human behavior that influences whether one will share or withhold certain information. He says that one will be non-hesitant to share certain information with a friend and will be completely unwilling to share the same information with a stranger. He says that there is a sensory process behind the motivation and demotivation to share information with.

In his study, he used headsets to measure psychophysiological activities in the brain, eye trackers, screen recorders, and cameras. The participants first fill out a questionnaire just

to get them accustomed to the sensors and also to give out information relating to any disorders they might have that may influence the study's results. After this, the participants are asked questions that put them into a situation where they have to share their information. They are constrained towards sharing the information on two platforms, Amazon and Facebook. They are given scenarios that involve the sharing of either highly-sensitive or lowly-sensitive information on both platforms and asked whether they would share the information. In between scenarios, participants are distracted with some other tasks such as solving simple math problems. The types of information that the participants are asked on whether they would share include credit card numbers, account balances, debts, gender, real names and their physical address.

In the results, the psychophysiological tools were able to determine the subconscious operation of privacy through an approach-avoidance mechanism. It was visible that the participants showed approach when asked to share lowly sensitive data. However, they were more cognitively involved and more withdrawn towards sharing highly sensitive information. Participants were more withdrawn towards sharing highly sensitive information on Amazon than on Facebook. Hammer says that his tools were able to study the participants longitudinally rather than in a snapshot. Therefore, the results arrived at had the element of accuracy. They also proved that privacy is a subconscious element of the human brain.

In conclusion to this work of literature, it can be seen that Hammer did an expansive research on the topic of social media privacy. He incorporated three researches into one paper to bring out a thorough understanding of users on the issue of privacy. His three different takes on privacy from the eyes of the users are instrumental to this thesis. Therefore, his work will be highly regarded and some arguments in the thesis will be born out of the information gotten in his paper.

2.2.5 Impacts of privacy, trust and user activity on intentions of sharing Facebook photos

Malik et al. ponder on a similar issue that this thesis is focused on, privacy and its impacts to users (2016). The authors of this research paper concentrate on the possible impacts of users sharing their photos on Facebook. The authors emphasize that there is little that is known about how privacy issues on social media are influencing the sharing of photos on social media, in this case, Facebook. They, therefore, seek to find the consequences of the current privacy issues on Facebook users' intentions to share photos. In their paper, Malik et al. discuss the normal usage patterns of users on social media networks (2016). They claim that the current usage patterns of posting personal information and pictures has been exposing users to more privacy and security risks. They also note that users are seemingly unaware about this. On the other hand, they say that social media platforms are profiting from this ignorance. They have been selling this information to third parties and, also, using it for advertising purposes. This thesis shares the same idea that social media platforms are the main beneficiaries of the personal information exposure of social media users. They have, therefore, been encouraging users to share more just to harvest more of the advertisement-ready content from their profiles.

When narrowing their research to photos, Malik et al. say that one of the visible usage patterns of social media platforms has been the posting of pictures (2016). From their statistics, they estimate that over 350 million photos are uploaded daily on Facebook and the sum total when all top five social media platforms are combined jumps to 1.8 billion (2016). They fault the research community for not giving enough attention to the impacts that privacy issues have had on users' tendency to share photos on social media. They say that the impact is unknown, hence their focus on this problem. They, therefore, bring up the following three research questions:

1. How do users' privacy concerns and awareness impact their trust in Facebook?
2. How do users' privacy concerns and awareness impact their activity on Facebook?
3. How do users' trust levels influence their Facebook photo sharing?

In their review of literature, Malik et al. bring to light the fact that a number of earlier researchers have said that social media sites encourage users to share their personal information (2016). Despite the users being given some privacy settings, they are lazy and, therefore, ignore. In one of the quoted literature, 36% of the Facebook user population make profile posts with default settings. These posts, therefore, get to the public domain and are exposed to more people than users can imagine. Other literature also highlight that social media users underestimate the security threats on social media.

Malik et al. bring forth their research model which is aimed at explaining the impacts of privacy awareness and concerns on the trust and usage of Facebook. The usage pattern that their research model focuses on is the sharing of pictures. Their research model is warranted by the fact that social media users have increasingly been warned about the privacy issues on social media. These researchers try to uncover an area that has been so far ignored by earlier researchers, of the effect of privacy concerns on the sharing of information on social media (2016). Malik et al. posit that the social media space is quite different and there is a possibility that despite the increased awareness campaigns, social media users might still be sharing personal information that they have been warned against sharing (2016). They give a defense for this. They observe that social media activity has only been rising. In their research model, they give an early deduction that Facebook users trust the platform and might be more willing than not to keep on posting. In their study and findings of 378 users, they identify that privacy awareness has led to more trust in Facebook. In their area of focus, which is photo uploading, users that were aware of privacy concerns would make future uploads to a more limited number of connections. This was due to the trust that their pictures

would only get to the people that they intended. As can be seen from their results, it can be said that users are not growing scared of Facebook once they learn of the privacy issues; they are using it but in a safer way. These results offer some insight to the thesis. They give hope that some of the mitigation measures it aims at giving to users will not lead to the death of some social media sites. Rather, sensitization of users on privacy issues on social media will lead to more careful usage.

Malik et al. also come to a finding that there was a positive relationship between privacy awareness and Facebook activity (2016). Therefore, privacy awareness did not force users to shy away from this social media. When explained on the privacy issues and safe usage patterns of Facebook, it can be seen that users did not abandon this platform. They were more aware of their privacy and security on these platforms and knew how they could secure themselves. In turn, this led them to use Facebook with a higher level of trust. This is a good indication for this thesis. It can be deduced that when users are taught on several privacy protection measures, they are likely to feel more confident in a social media platform and thus use it more. This is a finding that is welcomed by this thesis. In the recommendations, the thesis aims at teaching users several techniques to use to secure themselves on social media. This research paper by Malik et al. is an important realization of what is most likely going to be the outcome of the user education exercise (2016). Users will not feel restrained from using these social media platforms; rather, they will be encouraged to use them in a safe way in which they do not put themselves in danger.

In conclusion to this study, it is important to pick up the most important contributions of Malik et al. to the topic of privacy in social media. The researchers have secluded and investigated one form of content sharing, the uploading of photos on social media. Their research has pointed out the impacts of social media privacy concerns on this type of activity. Fortunately, they have determined that user awareness on social media threats do not lead to a

complete seizing of social media activity. When users better understand the privacy risks and the threats they face and how to handle them, they are more motivated to share content. This thesis is aimed at promoting user awareness as part of the ways to mitigate the problem of social media privacy. There are simply too many users that do not know how to protect their online privacy. There are others that have not taken the initiative to improve their social media privacy by hiding some information from the public domain. This research is aimed at these types of users. Malik et al. have already determined that if these users are enlightened on social media privacy, they will not ditch these revolutionary communication tools; rather, they will gain more trust in them. It is an outcome that this thesis hopes for. Malik et al. to have opened eyes on a topic that other researchers had paid a blind eye to, and that is why it has been considered in this thesis.

2.2.6 Legal interpretations of social media risk and threat mitigations in organizations

With the ever-increasing popularity of social media, there has come a number of privacy and security threats. These threats have descended down from individuals to organizations because employees have been quicker to adopt and use social media in their workplaces and on organizational computers. There has also been an increasing adoption of social media by organizations for publicity and marketing purposes. Therefore, organizations have no choice but to proactively react to the threats they may be facing due to the social media craze. Whilst social media can lead to the growth of sales and improved brand awareness, it can also lead to unwanted consequences, ranging from malware to the destruction of an organization’s reputation.

In a law journal, Russell and Stutz (2014) have published a piece of literature on what employers are expected to know about social media. This thesis highly considers this literature, since it is focused on mitigation measures that organizations should deploy to protect themselves from social media privacy and security threats. Of core importance to this

research is how end users, organizations included, can protect themselves from the negative effects of social media. This is especially due to the increasing number of threats that are being witnessed on social media platforms. Russell and Stutz give a number of approaches that organizations can use and this thesis will borrow from these.

Russell and Stutz (2014) say that an organization should pay attention to the social media accounts of their potential employees during recruitment. This is a sound security practice that this thesis acknowledges. It allows organizations to study the potential risk profile of an employee in terms of exposing sensitive information on social media platforms. However, there are certain legislations that may come in the way of this that Russell and Stutz wants organizations to know. In the US, employers need to be authorized by candidates in order to snoop around their social media accounts during background checks. It would otherwise be termed as illegal for organizations to disqualify candidates based on social media activities observed without permission from a job candidate (Russell & Stutz 2014). On the other hand, the United Kingdom requires employers to give job candidates a chance to determine the accuracy of the data available online about them (Russell & Stutz 2014). Other countries such as France have banned the use of information gathered from social media platforms for hiring purposes (Russell & Stutz 2014). However, it allows for the use of information from LinkedIn since it is a professional social network. Most other Europe countries follow the same trend. This information by Russell and Stutz is quite important. It shows the legal demarcation of how far an employer can establish the social media risk profile of a potential recruit. From this information, it can be seen that organizations' powers are quite restricted here and a recommendation to check the social media profiles of recruits might not be so effective in today's workspace and legal environment.

Russell and Stutz then look at the issue of organizations monitoring the usage of social media at the workplace. This thesis deems social media usage in the workplace as a

security concern because threats that a user faces can easily flow to the organization. If a user downloads a linked malware or visits a malicious website, it is a workplace computer that will be infected. In this case, the employee will have put into jeopardy the security of many other computers in the organization. Therefore, it is good for organizations to monitor the way employees use social media. Russell and Stutz still focus on the legal viewpoint and they look at different jurisdictions. In the European Union, employees are given the right to privacy and private life while in the workplace (Russell & Stutz 2014). For an organization to monitor this type of information, it needs to announce it beforehand.

Russell and Stutz (2014), however, give a hint of a leeway to this where they say that EU courts allow organizations to investigate employees that they suspect of violating company policies on social media. This is the one circumstance where the employer does not have to inform an employee that his or her social media usage will be monitored. There are other countries that the duo discuss that have even stricter rules concerning the monitoring of users. They say that Switzerland prohibits employers from monitoring their employees even if it is for preventive measures. This discussion in their work brings yet another important piece of knowledge to the argument on social media privacy. The legal system seems to be leaning too much with employees in order to protect their privacy. Therefore, most jurisdictions will find fault in organizations that try to monitor the social media activities of their users without pressing reasons to do so.

Lastly, Russell and Stutz look at the issue of employee dismissal due to the inappropriate use of social media. Employees can be careless about what they post or what they access on their social media accounts and this may have some consequences for the organization. Some employees may disclose information that is regarded to be confidential according to the company. Other employees might engage in proscribed social media activities such as clicking of links and this may result in the infection of some organizational

computers with malware. Others may simply overuse social media, thus resulting in low productivity. Whilst the main focus of this thesis is not about dismissal of employees, these actions spark an interesting conversation around how organizations should handle the inappropriate usage of social media. Russell and Stutz (2014) explain that employers have the advantage in court in several jurisdictions when they believe that an employee has inappropriately used social media and thus deserves to be dismissed from employment. They begin with Canada where they say that the laws allow for employee dismissal if an employee breaches a company policy or does actions that cause damage to the company (Russell & Stutz 2014). A breach of policy is an action such as posting a client's personal identifiable information. An example of an action that may lead to damage to a company is the clicking of malicious links leading to the malware infection of an organizational computer. In the Canadian legal jurisdiction, these actions may warrant a legal termination of an employment contract by an employer (Russell & Stutz 2014). In Australia, the courts tend to lean more towards employers when punishing inappropriate social media use (Russell & Stutz 2014). As such, even an excessive use of the Internet for personal social media purposes may be disregarded as misconduct that is punishable via dismissal. In France, an insulting comment to an employer on social media is taken seriously and the courts allow for dismissal of such offensive employees. However, the employees must have been forewarned that posting derogatory remarks about the employer might lead to termination.

In conclusion of this work of literature, it was of importance to bring to light the issue of social media security and privacy in the workplace. Organizations need to know how to react to protect themselves when their security and privacy is brought to question. This thesis pays attention to all the people affected by social media threats and attempts to give recommendations on how they can handle them. Organizations are however peculiar in that, they are not a particular individual, they represent the interests of many and their affairs are

intermingled with laws. Therefore, if some recommendations are made to protect organizations from social media threats and privacy concerns, they have to fall within the law. There is a challenge in that the law is different in different jurisdictions. Somme countries are still formulating laws to handle social media related cases. This unique literature by Russell and Stutz has dived into the legal matters surrounding organizations and how they can mitigate security threats on social media and the laws that they need to be in comprehension of. To protect themselves from hiring employees that might be social media security risks, organizations might see that it is best to mitigate this risk by doing a social media background check. However, as has been discussed, it is not as simple as it sounds because some jurisdictions require job candidates to consent to this. While working in an organization, it might be regarded as safer for the organization to protect itself from harmful use of social media platform by monitoring employees' usage. This way, they may be able to prevent some threats from happening, such as the downloading of malicious files or the posting of sensitive information about the organization. As it turns out, some jurisdictions are totally against the monitoring of employee activity on social media while others give tough conditions for this. Dismissals might be the last option in an organization's rule book to do away with employees that present privacy and security risks due to inappropriate social media use. Fortunately, courts in several jurisdictions understand this and do lean on the side of the employers, provided that there are sensible reasons behind the dismissals. This legal literature has been great at dissecting the legal implications of some of the recommendations that may be passed down to organizations to help them combat social media security and privacy risks.

2.3 Conclusion

This chapter has gone through six related researches that have been done by other researchers on the same topic. The first literature by Loeffler has looked at the prevailing privacy issues on social media. The reason why this work was picked is because it focuses on the infrastructure of social media platforms that have led to the current privacy issues. The second work of literature that has been discussed is by Heyman, Wolf, and Pierson. They have helped solve the conundrum surrounding the definition of privacy. They take a unique approach that this research adapts; they view privacy from two perspectives.

The third work is a real-life comparison of privacy between users of two different regions, the US and China. This research is only picked due to its real-life approach to this topic. The researchers have conducted a research on two types of users and they share their findings. The researchers do a good job trying to explain the distinct characteristics between the two groups of users that lead them to show the observed behavior on social media.

The fourth work of literature that this research has discussed is by Bryan Hammer who discusses social media privacy using a very interesting approach. Instead of approaching the topic from a singular viewpoint, Hammer breaks his research into three, where each part views privacy from a different lens. The last two pieces of literature give short but important contributions to this topic of social media privacy. The first of these two looks at the direct impacts of increased user awareness on social media content sharing. The second literature is on the legal side of the discussion about social media privacy. It examines the legality of the ways that organizations can use to protect themselves from social media privacy and security risks.

Chapter Three: Social engineering

3.1 Preamble

Social engineering is an attack technique that has gained popularity due to a continued streak of hugely successful attacks that it has been used to orchestrate. This hacking technique is quite unique in that it targets the weakest link cyber security, the human (Lior, 2005). Systems, networks, and devices enjoy the luxury of being protected from hacking through a wide variety of ever-evolving cyber security products. There is no product that can reliably protect a human from social engineering attacks other than the human itself (Bamberger, & Mulligan, 2010). The current level of advancement and sophistication in security products has been discouraging attackers from directly attacking systems. The old tricks in the book, such as brute force, are fast becoming ineffective against many systems. This is forcing them to look at the other avenues of compromising organizational systems and stealing information and money. Human users have become the most promising targets and, thus, many attackers are turning to social engineering to either effect their attacks or get information to attack systems.

Social engineers have the advantage in these attacks in that they can carefully study their targets, determine their weaknesses, and then exploit them by means of phone calls, emails, or short chats (Tan, 2012). Technological revolutions have also made it easier to attack today's users. The proliferation of social media platforms encouraging users to put out information about themselves has made information gathering about targets to be simpler for social engineers (Mital & Sarkar, 2011). This chapter will discuss the entirety of a social engineering attack. Social engineering presents a real-view of the privacy issues surrounding social media. Because users have not been careful when dishing out their private information

on these media, it is out there and easily accessible by attackers. The following sections will discuss more about the attack.

3.2 The techniques used

Social engineering is a hacking technique that involves manipulating people into giving out some information or complying with some malicious requests (Mouton, Leenen & Venter, 2016). It can be used to get to the core of an organization, bypassing multiple layers of security that the organization might have put up. It does not rely on technical knowledge or possession of the latest hacking tools, all one needs is knowledge of the human psychology (Granger, 2001). There are some aspects of a human that can be taken advantage of such as courtesy, gullibility, sympathy, obedience, and greed. A social engineer will make a target make some questionable decisions by pulling some strings attached to these psychological aspects of a human. The following section will outline the lifecycle of a social engineering attack, presenting some of the key phases. It is, however, important to note that it is not necessary for a social engineer to use a linear path, that is, going phase by phase. The attack can be concluded at any of the phases depending on the objectives of the attacker.

3.3 Lifecycle of social engineering

3.3.1 Information gathering

This might just be the most torturous step in the entire social engineering exercise and may last anywhere from a few hours to a few years (Krombholz et al., 2015). Not only is it long, it is demanding and requires an attacker to always be keen in observing the target. Today's social engineer needs to be well-informed of the data to look for and the software tools that can help with this. The quick adoption of social media platforms by a large percentage of people has made this process somewhat simpler. However, this data is at times

insufficient or too fabricated to be of help and, therefore, more data sources may be required. An attacker may, therefore, be forced to gather data using specialized software tools or using soft skills to directly get this data from the target without raising alarm.

Information is hardly gathered all at once. Doing so is hard and is therefore common for a social engineer to collect small pieces of data and combine them to complete a puzzle about the target. For instance, while gathering information about a CEO, an attacker may start by interviewing people that the CEO comes across or talks to. Janitors, secretaries, subordinates, or even visitors may be wisely interviewed to find out small pieces of information that may not be so useful discreetly but very powerful when put together. Even the most insignificant of people that a target interacts with may have a key to unlocking a much larger puzzle. Therefore, any source of information is treated as valuable.

3.3.2 Elicitation

Even with their weaknesses, humans will generally be withdrawn at first from confiding in anyone. It takes skills to be able to break people from their comfort zones so that they can start spewing out private information (Heartfield & Loukas, 2016). Elicitation is more than building rapport with strangers, it's a technique used in interrogation rooms, used by therapists and by doctors to get information from people that they would otherwise withhold. Elicitation, therefore, is the second step in the social engineering framework that is followed during social engineering attacks. The attackers use elicitation techniques after gathering enough information about a target to initialize a conversation.

3.3.3 Pretexting

This is normally the third step in a social engineering attack. It is where the attacker becomes anyone in a position to influence the target into making some decisions. The attacker chooses a certain personality that befits the character he or she opts to become during

the social engineering attempt (Heartfield & Loukas, 2016). With the advent of the Internet, it is easy to become anyone. There are so many informational resources that a social engineer can use to adapt the character of anyone. Pretexting is an imperative skill that any social engineer needs in order to accomplish an attack. Pretexting is more than just acting the role of a person, it can be considered as becoming the person. There should not be an iota of doubt to the target that the social engineer is not the person he or she claims to be. The social engineer's character, the manner of speech, body language and any other noticeable characteristic must fit that of the person he or she is pretending to be. It is a vital skill that will allow a social engineer to carry out an attack unsuspected.

3.3.4 Mind tricks

The whole social engineering attack is based on mind tricks, so this is a step that is used in many of the other parts of the social engineering attack framework. This part of the social engineering attack involves the use of specially crafted tricks to alter the thought patterns of victims. Mind tricks are used to some degree in many other areas in life, such as in sales, to make product prices appear less costly and in interrogation rooms to make suspects take a plea. Mind tricks are more of a psychological affair and they are used to unlock the minds of the targets exposing them to the control of the social engineer. An excellent social engineer is a good mind reader and this is achieved by mastering a number of mind tricks.

3.3.5 Persuasion

Just like mind tricks, persuasion is a cross-cutting topic in the whole of the social engineering process and, thus, cannot be constrained to a certain step. So as to persuade a target, a social engineer needs to appeal to the target’s interests first (Bullée et al., 2015). Persuasion gets targets to react, think and do exactly as the social engineer wants. Persuasion leads to unquestionable influence in the minds of the targets. So that the attack is successful,

social engineers perfect their persuasion skills. They make sure that the influence they have on the targets is undetectable but far-reaching.

3.4 Social engineering through social media

One of the key enablers of social engineering is social media. Attackers would have been starved of information about targets if it were not for social media platforms. A lot of information gathering for a social engineering attack is done on social media. Social media platforms, ever since their creation, have encouraged users to share every tiny detail about themselves (Kim, 2014). A platform such as LinkedIn encourages users to share information about their professional lives. They post their educational history, the organizations they have worked with, the titles they had, and a description of duties for all these titles. Facebook, on the other hand, encourages users to share information about their entire lives, their daily activities, the schools they have gone to, the workplaces they have been at, their spouses, and so much more. Instagram wants users to keep uploading pictures of wherever they are just to tell their followers what they are up to. The list of social media platforms and what they encourage users to do is long. Social media companies understand that they rely entirely on the content that users generate and, therefore, want them to keep sharing information, no matter how risky it has become to do so.

Social engineers are among the beneficiaries of the binge-sharing of personal information by users (Algarni, Xu, and Chan, 2017). The users are helping social engineers to learn how to best attack them. It is no longer a hustle to get details about a target; social engineers are just hopping onto the target's social media accounts to get flourished with extensive details about the target (Edwards, 2017). The only way users can stop this is by limiting the people that can view their data. Fortunately, the users are so lazy that they do not want to go to the settings given to them by their platforms to limit their audience.

Another way that social engineering is being conducted through engineering is through direct attacks to the users. It is unbelievably easy for a social engineer to create a fake or a cloned social media profile (Mouton et al., 2015). Social engineers are using these fake or cloned accounts to get users to do them some favors such as giving out some information or lending them some money (Bakhshi, Papadaki, and Furnell, 2009). Other attackers are using these profiles to issue threats or commands to users and giving them ultimatums to have some information or some money sent. There is also another group of social engineers that uses social media to send malicious links to users. They come up with the most enticing reasons to get users to click on these links. There are those that claim to be giving out free money, others claim to have a system that can generate likes and followers, and others are even offering ridiculous opportunities with an unbelievable pay (Snyder, 2015). Anything that can capture the interest and attention of a user is being used.

Social media has become one of the largest vehicles for social engineering. Every fair-minded person can turn to be anyone on social media. Users on social media are not so keen, and therefore it is easy for them to fall victim of cheap scams, requests from fake accounts, and threats.

3.5 Challenges in social engineering

3.5.1 Threat vectors

One of the biggest challenges in social engineering is determining who the foe is. Social engineers are just normal people, they speak so, act so, and at times have undergone some training to avoid arousing suspicion. Therefore, these threat vectors are invisible until it is too late. It is common for an old friend to hit someone up on social media to catch up. It will not come out as suspicious if that old friend asks for some money to get him out of a tight spot. The same scenario can be orchestrated by a social engineer on social media

platforms. All that the attacker will need is a good profile picture of the actual friend to use it to validate the whole pretext. Therefore, the attacker is always concealed and it is difficult for a victim to tell that he is being attacked (Thompson, 2006). It is not the normal type of an attack where the attacker is easily known. At times, it is the victim that will willingly give out money or information to the social engineer. All that the social engineer needs to do is come up with the perfect pretext such as a young attractive girl looking for a close friend on social media.

3.5.2 Enterprise security

A social engineering attack can have consequences to an enterprise even if it is an individual employee that is attacked. Some attacks have blown-back consequences to the enterprise as a whole. If a social media user is going through Facebook on his workstation during lunchtime and suddenly finds one of these enticing malicious links, clicking on it may cause viruses to be planted on the organization computer. If that workstation is not secured, the virus could jump to another workstation and slowly start propagating all over the network. All this will have been a result of the actions of the single user that was browsing Facebook on a workplace computer. Therefore, enterprise security is easily linked to the security of a user.

3.6 Proposed solution

Social engineering is a unique threat; it can hardly be solved through software or hardware mitigations. Therefore, organizations face it rough when securing themselves from this attack than when securing against other types of attacks. There are however a number of solutions that can be implemented to significantly reduce the success chances of a social engineering attack. These will be discussed from a viewpoint of defending an organization against the attack. They are as follows:

3.6.1 Implementation of best practices

Social engineering happens because of the laxity of an organization or simple mistakes that can be exploited by the attackers. Poor practices should be avoided and a strict implementation of security best practices should be encouraged. One of these best practices is to require anyone entering the organization's premises to show proper identification (Young, Zhang, and Prybutok, 2007). Security guards and reception personnel must be trained to verify all visitors, especially those that claim to be service personnel sent to do maintenance tasks. Another best practice is to communicate to all users that passwords are never to be exchanged via phone calls or emails (Young, Zhang, and Prybutok, 2007). The standard way of changing or recovering passwords should be followed. A user should not get used to calling or emailing the IT department requesting a password that he or she has forgotten. It is this loophole that social engineers will exploit.

The third best practice is to forbid users from writing down their passwords on notes or storing them in a text file on their desktops. Users should be encouraged to use password managers instead if they fear that they might not be able to recall all their passwords. Another best practice is the implementation of the Caller ID technology that can tell between calls originating from within and outside the organization. Social engineers can call and pretend to be a user within the organization requesting for a password, but if this technology is in place, the IT Help Desk will determine this to be a lie. Lastly, the best practice that is effective against social engineering attacks is shredding of confidential information that is in the print form.

3.6.2 Policies

Policies and standards are effective tools for putting in place checks to ensure that social engineers do not prevail. Organizations should take time to set up policies that close all the gaps that social engineers can use. These policies should also remove laxity from users

and make them responsible for the type of information that they share outside the company's systems. Policies must also be reviewed and updated with time and should not be unattainable by employees.

3.6.3 User education

The best solution to combat social engineering attacks is to educate users on what it is and how it is done. Users should particularly be taught not to give out information over social media, rush a process because a client demands so, yield to intimidation, agree to allow some small mistakes, or give system access to other people.

3.7 Analysis of the proposed solutions

The proposed solutions above can be very effective against social engineering threats to the organization. The implementation of best practices is particularly important since it seals off the existing insecure avenues that can lead to an organization being attacked by social engineers. Policies are also important tools that are sometimes neglected. Users should be taught to follow them and they will save the organization from attacks. Lastly, it is known that the best solution to social engineering is user education. Therefore, this is a very practical way to defeat social engineers. The only problem with the proposed solutions is that they do not focus more on the individual user, they focus on a user within the organization environment. Most of the time, users will be away from the organization and may be more exposed to social engineers.

3.8 Conclusion

Social media has created a healthy breeding ground for social engineers and that is why the vice has grown uncontrollably. This chapter has shed more light on social engineering. It has given the lifecycle of social engineering attacks and then explored how

social engineering is mediated by social media. The challenges that make it hard for social engineering to be detected and also particularly dangerous to an enterprise have been stated. Solutions have been given detailing how best social engineering can be handled in an organization. These solutions have been evaluated and the only identified challenge is that they do not focus on an individual user but rather assume that the user will be in an organizational context.

Chapter Four: Social Media Threat in Cyberspace

4.1 Preamble

Social networking sites have drastically changed the ways through which people used to interact with others. They have also made changes to people's professional lives. Today, social media platforms play extensive roles on how businesses are conducted. They also control the ways through which people communicate with others and also how corporates reach out to their customers. However, social media has introduced the world to risks that it might not have been prepared for (Workman, 2008). Attackers have proliferated these media and have been continuously striking social media users.

4.2 Threats in cyberspace due to social media

There exists quite a number of threats on social media platforms, and it seems that they only keep getting added with time. The following are some of the known threats:

4.2.1 Worms

There have been worms created by hackers that have been used to create botnets using the devices of social media users. One of these worms is the notorious Koobface ("W32.Koobface | Symantec", 2018). This worm is said to be propagated through social media platforms and it enlists the devices it spreads to a network of zombie computers. The infected devices are used to further spread the worm to other computers without the owner's knowledge. Once joined to the network, the infected computers are used in DDOS attacks or to give the hackers extensive computing power to carry out other types of attacks.

4.2.2 Targeted phishing attacks

There is an increase in the number of reported cases of users that have been contacted by people that used fear, anxiety, or greed to get them to part with some money (Harrison, Svetieva, and Vishwanath, 2016). There are also reports of users that have been lured into signing in to Facebook through phishing emails to attend to an urgent issue. The links provided by the emails have been said to been redirecting users to a website with the URL fbaction.net, where once they entered their credentials, their accounts would within minutes get compromised. There have been many other websites that users have been redirected to. To counter this, Facebook has been blacklisting many of them. This, however, remains to be a big threat since it is very easy for one to create a domain and also to replicate Facebook emails to be sent to users in the phishing emails.

4.2.3 Data leaks

Social media platforms are built with the intention of getting users to share lots of information about their personal lives. Users are carelessly doing so and at times they have been sharing information that can put themselves and the organizations they work for at risk. There are users that have shared details about undergoing projects in organizations, sensitive financial details, internal organizational changes, secret organizational scandals, and other private details about their personal and professional lives. This user-borne threat continues to flourish hackers with a never-ending supply of sensitive information that they can use to actualize an attack.

4.2.4 Shortened links

The ability to shorten URL links using services such as bit.ly has been a marvel that has helped users to make long URLs short so that they can be fit into small spaces. However, they have increasingly been used for malicious purposes on social media platforms. Rogue

users make enticing titles and share links to malicious websites through shortened URLs (Cao, 2016). Unaware, other users click on these links in expectation of the enticing content just to get a rude shock of malware invasion their computers.

4.2.5 Fake accounts

It is surprisingly easy for people to create fake profiles on social media. Before verification services by most social media platforms, celebrities were dealing with this problem of impersonation on social media where people would create fake profiles with the celebrity names. The fake celebrity accounts were being and are still being used to get a massive social media following and the new followers can easily get spammed. For example, if a famous celebrity releases an album, the fake profile could give malicious links to the followers telling them that they can get the album for free by clicking on the attached links. The problem of fake accounts is still relevant today, where malicious people have been creating fake accounts with the intention of using them to defraud or request for some favors from unsuspecting users (Harris, Seetharaman and Tau, 2017). Due to the difficulty in differentiating between the actual and fake accounts on social media platforms, this threat is seemingly not going to get a solution anytime soon.

4.2.6 Rogue third-party applications

Sometime in 2016, a researcher unearthed rogue third-party applications on the social media platform with the highest number of users, Facebook. The third-party applications had extensive rights to a user's profile and were using these rights to collect a lot of sensitive data from the user's account. There are other rogue applications that are being said to have malicious codes. When a user uses these applications, they are said to ultimately compromise the user's device and gather sensitive information stored on the browser. There are quite a number of third-party applications that are present on different social media. They include:

- Facebook Color Changer – This third-party app claims to be able to change one's Facebook profile from the ‘boring blue' color to other colors. It only ends up using one’s account to get free promotion to other people and then lead users to malicious sites.
- Who has viewed your account – It is another third-party app that tells users that it will be able to show the people that viewed their profile. Users then give it their login credentials which are taken by the spammers to access a user’s account and also friends list.
- Instant followers – Followers have become a way of accreditation and most users want to have many followers on their accounts. There are malicious apps that have been created to sell this false hope to users and also to hack them in the process. There are apps that claim to be able to get users more followers only if they are given the login to one’s account. Once they get the login of a user, they use the victim’s account to contact other users.
- Instagram likes – It is similar to the above-explained third-party threat. In this threat, the user gets promised by the app that he or she will get thousands of free likes on Instagram and at times even free followers. The catch is still the same, one has to give out the valid login credentials only for them to be stolen.

4.2.7 Identity theft

There are increasing reports of users complaining that their social media accounts have been hacked and taken control of by malicious people. Hackers have commonly used the ‘forgot password’ feature provided by these platforms to enable them to recover their accounts when they do not recall their passwords. Most recovery procedures will involve the user being asked to provide a birth date or answer a secret question. This is where stalking a user comes in handy. By merely going through the social media profile of the target, a hacker

can tell a user's birthday from birthday wishes from one's friends. As for the secret question, some of the answers can also be obtained from a user's profile. The secret question might ask the name of a pet, friend, wife, mother, or cousin. This is information that can be conveniently obtained from the user's profile. With this, it is possible for a hacker to steal the account of a social media user and use it for malicious purposes (Seda, 2014). The malicious purposes include extorting money from one's friends, using the account to get some sensitive information from other people such as coworkers and even getting the privilege of asking some favors.

4.2.8 Scams

There are hacker groups that have only been specializing in spreading scams on social media and they have been doing so with a lot of success. There are many people joining social media for the first time and these are the main targets for the attackers. The following are some of the scams:

a) Nigerian prince – This scam is as old as emails but is still being used just with different variations. It mainly has a purported Nigerian prince that has a huge inheritance from his father but cannot access the money due to some legal or personal challenges. The scammer asks a social media user to help them by either giving out their bank account information to be used to deposit the huge amount of money. In other scenarios, they plea with the targets to help settle some charges for the money to be released. Of course, the money is never released but the target only finds out after spending quite some amount to help get the money released.

b) Cash grabs – This is an effective scam used by attackers that have already obtained the login information of some social media users. Mostly, these are credentials stolen by malware from browsers. The attacker will look at the

friends list or relatives of the user and then tell them that they have been involved in a bit of a situation and need money urgently. The concerned friends or relatives send the money to the scammer. The only problem is that the real account owner will not have been in any situation and will not even be aware that someone is taking advantage of their family and friends.

4.3 Reviewing existing security policies

Quite a number of organizations have some security policies that are supposed to govern social media use. However, these policies are either weak, are not being followed, or do not encompass the threats that social media use introduces to the organization. Social media cannot be simply banned because the same organizations have marketing departments that utilize these platforms. Even though some organizations have resulted to a total ban of traffic headed to social media sites, others have simply been using some policies to control the use and promote the security of the organization. The following are some of the existing security policies in organizations:

a) Social media hours – To prevent the overuse of social media platforms, some organizations have gone ahead to define the times within which users can or cannot use social media. The objective of reducing the time spent on social media while on the premises of an organization is aimed more at productivity than security. Due to the addictive nature of social media, if workers spend four hours each day in a 40-hour week, their productivity will have reduced by half. The security perspective of this policy is that if users have less time on social media while in the organization, they might be less tempted to post sensitive details about the organization. It is just a demotivation and nothing more.

b) Posts about an organization – There are organizations that restrict their users from posting any details about their roles or current undertakings on social media. This is a very effective policy when it comes to safeguarding the security of an organization. The reason why hackers have an easy time isolating their targets is because employees define the roles they play or the departments they work in on social media platforms. For example, if a user posts a picture in the accounting office complaining of how keeping accounts is tiring, a hacker might pick up this information. The hacker may then prepare an attack against this user. It, therefore, makes sense if an organization prohibits users from sharing on social media the intrinsic details about the functions they play in the organization.

c) Authentication – Some organizations have taken upon themselves the burden of ensuring that their employees secure their individual social media accounts as well as those of the organization. Therefore, they have extended some authentication policies applied on organizational systems to the users. It is hard for the organization to enforce these obviously because they do not control the social media platforms and thus do not have the powers to tell who is obeying these policies and who is not. One of the authentication policies that organizations have been recommending their users to follow is that of multi-factor authentication.

d) Two-factor authentication or multi-factor authentication - This is a secure login feature that ensures that a user has to authenticate himself or herself in at least two ways so as to log into a system. This means that simply knowing the account password is inadequate to get access to one's account. It is necessary for the person trying to log in to have another factor such as being in

possession of a mobile phone number or biometrics of the registrant of the account. Most, if not all, of the social media platforms, have an option for users to turn on two-factor authentication. This feature, however, comes deactivated by default.

e) Password characteristics – Policies touching on password characteristics tend to get into the nerves of many users as they prohibit them from using their usual, easy-to-remember passwords. Since hackers know how to profile passwords that users may use, it is important for the users to avoid creating passwords with information that is easy to guess. A common password choice of employees is that of their birthdays, spouse's birthdays, pet names, a combination of one of their names and birth year, and so on. These are very insecure passwords, and there are many tools that can give hackers most of these combinations based on the known information about a user. With this in mind, organizations are encouraging users to adopt complex password character combinations. Password reuse is yet another problem facing users, whereby the same password used for emails is used on ten or so other platforms. If a hacker is able to find out the password for one of these platforms, then he inherently knows the passwords for many other platforms used by the same user. Organizations are therefore encouraging users to use different passwords for both their social media accounts and also for organizational accounts.

f) Password age – Due to the increasing threat of theft of the login credentials stored on web browsers, organizations are urging their users to regularly change their passwords. There are many threats lurking around the Internet, and they have the capability to either steal the stored logins or implant

themselves onto browsers and continually send back the sensitive information they collect on a browser to hackers. The common 90-day password expiry period is, therefore, being extended to users on social media. When the password is regularly changed, the login credentials stolen by hackers becomes unusable. However, it is not irrelevant since hackers may use it to profile the passwords that a user creates and uses.

g) Privacy settings – Social media platforms give users a number of privacy settings that they can use to make their accounts a bit more secure. However, many users are not keen enough to stay updated with the privacy settings at their disposal. Most platforms will keep on introducing new security settings to respond to the increasing number of threats. Therefore, if well used, these settings can help one eliminate some privacy and security concerns that linger on social media. There are settings that can limit the people that can see one's posts. It is however not surprising that many users have left this setting at public meaning that just anyone on the Internet can see their posts. There are other posts that users can use to limit the people that can message them on some social media. There are many other helpful settings that users do not know or simply do not take time to view. Some organizations are therefore educating their users on the settings available for the social media platforms commonly used by employees.

h) Restrictions on connections – Connections, which are mostly identified as friends or followers on social media, can be a burden for users. They may turn out to be liabilities for one's personal and professional life. The number of connections that one has can directly impact his or her security on social media. There are simply too many malicious people on the Internet sending

friend requests, connection requests, or following other people just to keep tabs on them and harvest the sensitive information that one may reveal. There are others that simply establish these connections with users to be able to share malicious links or messages. It, therefore, makes total sense in a security perspective for one to either block, unfollow, or unfriend users that one is not familiar with. Organizations, therefore, put in place policies to help users curate their connections. Also, some organizations advise their users not to accept connection requests from random strangers on the Internet. It is hard to tell between a hacker and a genuine user on the Internet and therefore the best way to handle this issue is to be vigil with the type of information that one shares on the Internet.

4.4 Threat intelligence

Threat intelligence is the end result of the collection, evaluation, and rigorous analysis of information pertaining a certain threat. Threat intelligence enables preventative measures to be developed in advance in order to combat a threat. There are four types of threat intelligence; tactical, technical, operational, and strategic. Tactical threat intelligence informs users of the methodologies used by attackers, the tools they use, and the tactics that they employ in order to do an infiltration. Technical threat intelligence, on the other hand, is indicative of malware and gives the mitigation measures. Operational threat intelligence captures details about a specific attack and determines the readiness of an organization to the threat. Lastly, strategic threat intelligence is for changing risks and is shared with top management.

In the context of social media threats, this section will outline a tactical threat intelligence. It will look at the tools, tactics, and methodologies used by attackers to attack

social media users. To begin with, it is important to break down the threat landscape. For a threat to be there, there should be three things. These are intent, which is a desire to cause harm, capability, which is the availability of something that can cause harm, and lastly opportunity, which is an opening that can allow the threat to occur. In social media, there are many people with malicious intents due to reasons of jealousy, greed, financial distress, poor upbringing, and so on (Schaab, Beckers, and Pape, 2017). There are also free or low-cost means to cause harm to people, thus the capability of a malicious person to cause harm is always there. Lastly, there are many opportunities to attack social media users. They simply have too many exploitable vulnerabilities, which makes it very easy to attack them. If the target was a system, the attacker would take time to identify an exploitable vulnerability by means of scanning tools. However, since the targets are humans, they can be easily compromised through manipulation (Luo, 2011).

The tools that attackers use on social media are a few, mostly because they do not need any. The only way to attack a social media user is to persuade or convince them to do something that ends up being malicious. The few tools that social engineers use are the ones that can facilitate an attack. One of these tools is a URL shortener, which is used to compromise the URLs of malicious websites before a user is given the link. This hides the domain name of the website that the user is being led to (Perri and Brody, 2012). It is fairly easy to access these tools as they were meant for a totally different and non-malicious purpose, that is, to shorten long URLs. Another tool used by attackers of social media users are website cloning tools. These come to play when the attackers want to lead the users to a website that they are familiar with and thus will not hesitate to give in their personal information or just to log in. Attackers have a tendency of giving links to cloned Facebook, Twitter, Instagram, Gmail, Yahoo, and PayPal websites. They do this with the intent of getting the users to give out some sensitive information such as their login details. Lastly,

attackers use tools that can generate template messages that appear to be from legitimate people or organizations. There is a reason why such tools exist, some of these attackers are not native English speakers and therefore make horrible grammatical errors (Castelluccio, 2002). To add weight to this is a group of hackers that was nabbed in India that was responsible for a wave of increased IRS scams targeting US citizens (Alkhalisi, 2018). They were sending template messages to US citizens claiming to be from the IRS. Mostly, these emails claimed that they were following up on some skipped payments or they wanted to do a refund. These attackers were not so good in English and thus had to use template messages. There is a reason why many phishing emails contain grammatical errors; it is because they are not sent by people conversant in English. The same attackers extend their attacks to social media and therefore they tend to use the same scripts in their messages.

Concerning the tactics and methodologies that the attackers use, all of them are geared towards manipulation. They target fear, greed, and obedience to authority, sympathy, and excitement among other things to get users to click on malicious links, to agree to take some actions, or to give out some information (Musthaler, 2006). Looking at the use of fear, these attackers can threaten social media users to either comply with some requests or face some consequences (Burgess et al., 2004). It could be a fake threat that the IP address of a user has been found to be downloading pirated content and that the user has 24 hours to deposit a certain amount in fines or face jail time. It could also be a threat to expose some private or nude photos of a user that were found online by a hacking group and that the user has to pay some amount to prevent this from happening. Fear is a very strong emotion, and it can make the user comply with these requests. Sometimes, the attackers play on greed. They promise the users huge fortunes for doing some small favors. Earlier in the discussion, there was an explanation of the Nigerian prince scam, where users are told to pay certain fees so as to allow the huge fortune to be released and they will be rewarded handsomely. Another

commonly used tactic that exploits the greed in users is that of surveys. The users are told to take a survey and they will be rewarded with crazy prizes or cash rewards (Schwartz, 2012). However, once they click on the link to the survey, they are led to malicious sites that infect their browsers.

Obedience to authority is also another commonly exploited tactic by attackers. This commonly occurs when the attacker has some information about the target such as where the target works. This is information that is available from a user's posts or their profile page, where they list their bio. With this information, an attacker can simply create an account with the names of a senior employee in the organization that the user works at. On a weekend, the attacker can send a message to the user asking to be sent some information or for some money to be sent to a certain organization through a new bank account. Since the user knows that the message came from a superior, there is a chance that he or she will not question the request and will just proceed and comply with the orders given. Although this happens through email, there is an organization called Ubiquiti Networks that was attacked through this tactic (Goldman, 2018). Hackers sent accountants messages pretending to be a senior employee and requesting money to be sent to new bank accounts since the suppliers had changed their payment details. Blindly, the accountants complied with these orders until close to $40 million was lost.

Sympathy is a common tactic used everywhere to take advantage of people's willingness to help the less fortunate (Greavu-Serban, and Serban, 2014). There are beggars that have specialized in this, living off the sympathy of others. This tactic is still used on Facebook. Mostly, the attack will be targeted towards old people on Facebook. An attacker finds out the details about a grandson or a granddaughter of an elderly Facebook user and then creates a fake account with a similar name. The attack takes place when the attacker starts requesting money from the seniors claiming to be either in a fix or having suffered a

tragedy and thus needing some money. They also urge the elderly users not to share this information with their actual parents. This way, the attacker creates a means of fleecing these users.

There are many other tactics that attackers might use; the discussed ones do not even cover a quarter of all the tactics. They are so many because humans are so porous when it comes to being manipulated (Savage, 2003). There are some professions that rely on the manipulability of humans. Therefore, it is only a matter of time before they crack open when an effective tactic is used. Law enforcement agencies best understand this. With social media, the chances of manipulation are even higher since it is easy for attackers to create new identities.

4.5 Proposed framework

The threats in social media are many; the targets are weak and their vulnerabilities are many. This means that a lot needs to be done if all targets are to be secured from the risks they face. It is not an overnight transformation, but with time, measures can be put to secure humans from social media threats (Parker, 2002). This section discusses a framework that can be used to develop social media security for the benefit of individuals and the organizations they work for.

i. Development of organizational social media security policy – Some organizations operate without a defined security policy applicable to social media platforms. They only concern themselves with threats and risks present on their ERP systems and forget about social media. This brings about a breeding ground for threats and risks that users are hardly aware of and the organization is ignorant about (Endicott-Popovsky, and Lockwood, 2006). Therefore, the step of the framework

is the creation of a practical social media security policy. Among other things, this policy should govern how social media is used in the organization. The policy must touch on security aspects such as password requirements and the information that one can give out on their profiles.

ii. Creation of a multi-dimensional risk-based approach – Social media threats are to be taken with the same seriousness as other risks and threats to organizational systems. The threats target lack of information, lack of awareness, poor implementation of policies, and poor security concerns (Kerkstra, 2005). Therefore, organizations should take a risk-based approach when addressing social media threats. On other systems, infrastructure-based approach works best since everything is owned by the organization. However, social media networks are not owned by the organization and the information that users share is also theirs (Peltier, 2006). Therefore, the best way to boost security is by first informing the users about the risks they face and then giving them solutions to these risks. If this is not done, another approach will simply lead to rebellion from the users.

iii. Network visibility – Other than asking users to give out some sensitive information, attackers mince out this type of information from users through malicious links leading to cloned or malicious websites. Therefore, organizations need to monitor the network activity of computers connected to social media sites (Gan and Jenkins, 2015). Hence, when a user clicks on a link to a malicious site, security systems will detect this and report it. Even if the systems do not detect

the malicious site, it will be easy to identify the sites that a user visited when a security incident happens, such as a malware attacking a workstation. Since users accessing social media from their workstations put the entire organization at risk, should they click on malicious links, all computers should have tools to prevent data loss, detect malware, and filter web content.

iv. Classification of sensitive data – When coming up with the security policy mentioned in (i) above, it is good to classify the sensitivity of data. Not all data shared on social media is a security threat; some of it presents no risk to the organization or the individual user (Sisk, 2008). Therefore, an organization should classify the sensitivity of different types of data that users might share on social media. For example, giving out the roles that one play on social media might be a security concern. An attacker can easily use this information to plan an attack on the organization. On the other hand, posting a picture of a puppy is totally harmless. It might not be easy for novice users to determine the sensitivity of the data that they may share on social media and therefore, the social media security policy should do this for them.

v. Protection of endpoints – As mentioned in (iii) above, when employees visit social media sites while in the workplace and also on their workstations, they inherently put the organization devices at risk. Therefore, if they were to click on a malicious link thus landing on malicious sites that infect the browser they are using, it is the organizational data that would be stolen. Sensitive login credentials to the organizational systems that would have been stored on the browser

would all be stolen by the hackers. Such type of data is expensive and can be used to tear apart the organization by the hackers (Sayers, 2005). Therefore, it is paramount that endpoints in an organization be secured. There are many endpoint security solutions that can offer protection from malware and others that come with an endpoint firewall. Therefore, if the worst happens, the organizational data on the browsers will at least be secure.

vi. Educating employees – Last in this framework is the greatest tool that is effective against social media threats, educating users (Albrecht et al., 2011). Users fall victim simply because they are not aware of the risks they face. A user who does not know the existence of the Nigerian prince scam, for example, will give a listening ear to hackers that present their story to him or her. Similarly, a user who does not know the risks of clicking on links sent via social media is also not going to hesitate to click on them. Therefore, employees must be educated on how to detect scams on social media. They must be made aware of some of the scams that have been happening on social media. They must also be told the risks that they put organizational computers in when they open social media platforms and do prohibited actions, such as clicking on shortened links.

4.6 End user awareness

In the proposed framework section, it was said that users, at times, fall victims just because they do not know better. Therefore, they easily comply with the requests of attackers or fall into their traps just because they are not aware that these scams exist. Similarly, they

pour out so much personal information since they still believe that social media is the place to tell the world everything. This section will look at what users should be made aware of about social media to make them more informed and thus more secure.

4.6.1 Limit personal information

Attackers, ranging from hackers to common burglars, will turn to one's social media account to see whether there is any information that might help them to stage an attack. A burglar will look for a home address and posts about one having left for a vacation. A hacker will look at other nitty-gritty details present on the account, such as one's birthday, pet names, spouses names, children's names, posts about one's bank, tax filing rants, and costly insurance company complaints. From this list, it can be seen that the more one shares on social media, the worse for them. A fake account masquerading as a friend or follower could be owned by a hacker who will be busy collecting this information. Also, information, even if thinly spread on different networks, can easily be pieced together by a determined hacker. Sarah Palin, a US Vice Presidential candidate was hacked in 2008 after a hacker was able to piece together answers to the security questions that she had set for her email. The information was gathered from Google and Wikipedia. Today, it is very likely that the answers to secret questions set by users on their email addresses can easily be found on their Facebook accounts only.

4.6.2 Do not overshare sensitive details

As mentioned earlier, a burglar might know which house to break into by conveniently reading a post by a user that he or she will be traveling to some other place from a certain date. There is an urge on social media of users wanting to announce to the public some details that might just make them targets. If one has huge amounts of cash in their

house, why flaunt on social media? Users ought to be cautious about the posts they make on social media lest they put a mark on their heads to be attacked.

4.6.3 Strong passwords

The most popular password in 2015 was 123456. The others that came close were password and QWERTY. This shows a huge problem on computer systems and social media; users are reluctant to use complex passwords. This is despite them knowing the risks they put themselves into when they use such passwords. The laxity of users to use complex and non-easily guessable passwords is alarming. Therefore, it is best if they installed password managers to help them create and store passwords.

4.6.4 Not clicking on suspicious links

It was highlighted that attackers use URL shorteners in order to obfuscate links that lead to malicious websites. There are also tricks to make a URL appear as if they are of legit companies. For example, let's say that an attacker has a clone of the PayPal login page. He can use this page to get social media users to enter their actual PayPal logins. A trick to get them to this site is by giving an irresistible prize such as $100 for completing a survey. This will get a number of clicks. The hacker can tell the targets to first login into Paypal in order to be able to claim this prize and give them the link to the cloned site. Since the cloned website will look entirely similar to the official PayPal website, very few will have doubts on whether the site is legit. There is laxity in users to verify the URLs of the sites they visit, especially when these are provided through shortened URLs. It is also easy to host a website with a fake but similar URL. There are also some tricks that can be used when hosting a fake site to make a domain name appear more legit. For example, the hacker, in this scenario, could host the domain name com_password.net.

He can then subdomain it with a name such as PayPal so that he gets an end URL that looks like this:

Paypal.com_password.net

To a novice user, this looks like a legit URL from PayPal because it has the Paypal.com part. The hacker uses this URL together with a cloned PayPal login page to get a user to give his or her login credentials.

The scenario just explains one type of the many attacks that are done with the help of links. Therefore, users ought to be cautious when clicking on links sent to them via social media messages or social media posts. When a deal sounds too good, it is highly likely to be a scam. No one is going to offer $100 to have a simple survey completed. There are very many other tactics that are used to get people to click on links. Users need to be aware of all this and avoid clicking these links at all costs.

4.6.5 Identifying targeted phishing attempts

A determined attacker will take time to study the social media account of a particular user just to identify the weak spots they can exploit. An accountant, for example, could get a message from a purported senior manager on Facebook asking for some amount of money to be sent to a certain bank account. An underlying and superficial excuse could be that the senior manager wishes to keep that information off the records since it would be impugning to his or her reputation to have delayed in paying the person the money is being sent to. An IT officer could get an inbox on social media from a user claiming to be a colleague in the same organization who has forgotten her email password and wishes to get it so that some urgent files can be sent to her boss. There are many other scenarios, where targeted phishing may be used in order to get a user to divulge some information or comply with malicious requests of users. Mostly, they will masquerade as people known by the target. It is not suspicious for a user to reach out to an IT officer on Facebook anyway. Targeted phishing

attacks are particularly dangerous due to the length that the attackers take to get something that the target will yield to.

4.6.6 Managing accidental disclosures

At times, social media users end up disclosing very sensitive information. For example, one can unknowingly give out his or her social security number. A picture of one's new work laptop could also show a nearby piece of paper that has a number of login credentials listed on it. Some posts may disclose one's bank account number or debt status and other private information that should remain private. Therefore, users ought to be careful when posting information. They should look keenly at what they are posting to ensure that there is no sensitive information that will be disclosed.

4.6.7 Using privacy settings

Social media platforms, despite their many shortcomings, try to provide their users with tools to improve their privacy and security. One great privacy setting is the one that limits the audience for the posts. Social media sites, such as Facebook have an icon on each post a user makes that gives the user the option to change the audience or who can see the post. Therefore, when traveling, the post can be made to be visible to friends only. When sharing information about general things that present no security harm, such a post can be left to be public. There are other things that a user can control. Some sections of one's bio can be hidden. It is of no importance for one to announce to the world private information such as schools attended, all workplaces one has been through, or even pet names. On other platforms, such as Instagram, one can make his or her account private. This means that the posts he or she makes will get to a much smaller audience and therefore, it is safer. Users need to be made aware of these settings. Some social media platforms are really trying to get

more practical privacy settings on their platforms to help the users secure the information that they share.

4.7 Recovery

In the worst-case scenario, a user will have fallen victim to the social media threats. Therefore, it is good to know how to recover when this happens. The following are some of the recovery ways categorized as per threat:

4.7.1 From spamming

If a user has fallen victim to a scammer and sent some money to them, the best way to handle this is by reporting the matter to legal authorities as well as to one's financial institution. Responsible banks will try and follow up the matter to see whether the money can be recovered. Legal authorities might try to nab the suspect in future attack attempts. It is also good to retain the digital evidence of the scam just in case it is needed.

4.7.2 From malware

When a malware infects a user's computer due to the user clicking on malicious links or downloading malicious files, the best way to recover is by using an end-host security program. If the computer did not have one or it was not active, it is best to get it running and also updated. Most antivirus companies will keep updating their software to be able to handle these kinds of attack vectors. If it is too late and the malware has done some damage, such as theft of data and damage to files, it is best to clean up the whole system by formatting and reinstalling backups. Also, any login credentials stored on browsers might have to be changed.

4.7.3 From identity theft

It is common for identity theft to occur especially when the attackers are able to take control of a user's account by stealing the actual credentials and changing the passwords. The best way to recover the account is by trying to recover the account with the 'forgot password' option. This may lead to a point that requires the account to be re-authenticated with information such as real ID card, which the hackers may lack but the real user will have. If everything fails, it is best to write an email to the social media platform.

4.7.4 From sensitive information disclosure

There is a common saying that the Internet does not forget and this is something that a user should always be mindful of. If some sensitive information has accidentally gotten to social media, it is best to remove it upon discovery. This may prevent people with malicious motives from accessing this information.

4.8 Conclusion

This chapter has looked at the security cyberspace of social media networks. It has discussed the different types of threats that users on social media face. These threats emanate from the information they share on their bio, the posts they make, the messages they receive, and the shared links they click on. The existing security policies in different organizations have been reviewed. Their intents, accomplishments, and failures have also been discussed. A tactical threat intelligence for the discussed social media threats has been created and discussed. To deal with threats, a framework has been established that can be applied by organizations to reduce the risks that they and their employees face from social media. A practical solution on putting an end to the issue of users falling victim to social media threats is end-user awareness. This chapter has delved into it and given several points on what users

should be made aware of. Lastly, a recovery process has been discussed to help users recover in the unfortunate scenario where they have fallen victim to social media threats.

Chapter Five: Research Methodology

5.1 Preamble

This chapter explains the methodology of research. It looks at the method that was used to collect data in this study, the reasons behind the methods, and the data collection procedure.

5.2 Data collection methods

This study will use qualitative research methods to discover the privacy issues that users of social media are currently facing and the extent of their impacts. Qualitative research methods will come in handy for collecting a lot of diverse and credible data from a significantly smaller number of respondents. This will be actualized in the primary data sources, whereby a questionnaire will contain many questions but will be intended for a few respondents. This will enable the identification of the most intricate details concerning the study. In this research, asking each respondent more questions will be better for discovery of problems that they are facing rather than if the study used quantitative research methods. The main aim is to derive as much data as possible from each single respondent. The study is focused on the opinions and attitudes of the users of social media. This is why it will aim at extracting all the relevant information that each respondent will give for the study. At the end, all that will count is having an in-depth understanding of what issues users are facing and how they feel about the privacy and security of several social media platforms.

5.3 Choice of data sources

The research intends on capitalizing on already existing secondary data and complementing it with primary data. The study is aware that there have been other similar studies done that may have used more extensive data collection methods and thus, it will be of significance to include their search results. This is not a relatively new issue as there exists a number of researches into the privacy issues surrounding the social media industry. Therefore, there will be some data that will be borrowed from researchers who have researched about privacy issues in digital media, especially social media platforms.

The study, however, has seen it fit to do a primary data collection. This is because there have been some evolutions of new privacy settings, new acquisitions of applications, and other factors that have changed social media platforms. It is thus important for fresh data to be collected from users, especially after they have just witnessed the new changes in the various platforms that they are on. The study will give out online-based questionnaires to respondents. These questionnaires will revolve around the current situation or atmosphere of social media and will try and get as much user feedback as possible. The feedback will be concerning the privacy and security issues that the users are now experiencing.

5.4 Data collection

5.4.1 Primary data collection procedure

The primary data collection tools were questionnaires; however, these questionnaires were given online. A respondent accessed the questionnaire through a link and filled it online and submitted his/her responses online. The advantage of this is that the data collection process was made less costly since there was no printing, copying, and distribution cost incurred. Also, the responses were easier to process since there was no conversion process from data on hard copies to become a soft copy. The coverage was also better since the

online-based questionnaires could be filled from any web browser, that is, on both desktops and mobile phones.

The targeted respondents for this questionnaire were people in the age bracket of 18 to 45 years. There are many people in the world within this bracket that are active on social media. Therefore, the respondents had to be sampled to come up with just an adequate number. The research targeted to get well over 200 responses, and thus the sample size was made to 250 respondents. Over 100 responses were considered to be adequate as the research was intended to be qualitative rather than quantitative. The online questionnaire contained 80 questions, and it was estimated that respondents would take between 20 to 30 minutes to give their responses. Prior to the questionnaire being sent, invitations for interested respondents were sent via email to persons in different social media groups. Within the first 2 weeks, 300 people volunteered to take the online survey/questionnaire. This group of respondents was made up of people from different genders, ages, location, and education level, thus was considered more or less ideal for the study. From the 300 volunteers, the questionnaire links were sent to 250 via several media. The questionnaire tried as much as possible to respect the privacy of the respondents and thus no personally identifiable information was requested for. As such, all submissions made were anonymous since they did not contain the respondents' names, email addresses, postal addresses, social media accounts, or phone numbers. However, there were some mandatory fields that respondents were required to fill such as their age and gender; this was solely for the purpose of analysis.

The following Table 1 shows the breakdown of the types of respondents that were able to answer and submit the questionnaire in time. The total number of valid responses within the given time was 110.

Table 1: Shows the breakdown of the types of respondents

Demography	**Number**	**Percentage**
Age		
18 - 23	48	44%
24 - 28	27	25%
29 -33	18	16%
34 - 37	8	7%
37 - 45	9	8%
	110	100%
Education		
Up to Undergraduate	75	68%
Masters	20	18%
PhD	15	14%
	110	100%
Computer literacy		
Beginner	30	27%
Amateur	57	52%
Professional	16	15%
Expert	7	6%
	110	100%
Gender		
Male	61	55%
Female	49	45%
	110	100%

The full questionnaire has been provided in the appendix section of this paper. The questionnaire managed to get 110 full and valid responses within a week. This was good considering the short time that respondents had been given for the rather long questionnaire. The research decided to halt the data collection process after receiving 102 responses to allow for in-depth analysis to take place. Again, this was because the study was focused on being qualitative and 100 responses were termed as sufficient to gather the required data. Since the questionnaire was online based, processing and analyzing the data was rather easy. The data

was retrieved from the database and converted into a ‘.csv' format, which could be opened using MS Excel. MS Excel was chosen for analysis since it was easy to use and more readily available, than SPSS, since it came with the Office suite. MS Excel also provided greater convenience for transferring data to MS Word. MS Excel also produced more aesthetical graphs and provided greater customizations in terms of color and adding information for better presentation of data.

5.4.2 Secondary data collection

Some secondary data was borrowed from earlier researches conducted by others. First of all, the paper borrowed data from a research done in 2015 about social media and privacy by Alawawi (Alalawi, 2015). The researcher collected responses from 50 respondents concerning the issues of privacy and security in social media platforms (Alalawi, 2015). The researcher looked into five groups of questions in general. The first group of questions were aimed at gathering data about the attitudes of people towards different social media platforms. The second group of questions looked into the attitudes of users towards the then available privacy policies. The third group of gathered data about the concerns of the users when it came to their privacy on different social media. The fourth group of questions looked at the importance of social media and whether it was viable to scrap it off. The last group gathered information about the user perception of who was responsible for ensuring the privacy of users.

This study also borrowed data from a leading research institute globally, Pew Research Center. Pew Research Center had just done a survey of 607 adults living in the US about their perceptions of privacy and security on social media platforms. Sample of 1537 respondents had been selected, of which 935 accepted the invitation and finally only 607 completed the survey. The survey engaged the respondents for a prolonged period of time and at times held online group chats with them. The organization ran the survey online for

some time and got a huge number of responses which they disclosed. Their survey sought to discover the information users had concerning the government monitoring their private conversations. The survey also looked at the concerns of the US citizens towards surveillance. It also looked at the confidence levels that users had on different platforms. The users were also asked if they believed if it was possible to protect their privacy online. The survey also asked respondents to disclose the personal information that they were most sensitive about being disclosed.

5.5 Research question design

The research questions were aimed at gathering data and spreading awareness about social media security and privacy. The primal focus was on data collection, where user characteristics, security awareness, and social media usage patterns were studied. The respondents' age, level of education, computer literacy, and gender gave the basic characteristics needed for the research. Questions on their favorite social media platforms, frequency of use of social media platforms, and number of friends or followers were used to gauge their social media usage tendencies. This would be effective at profiling them to the type of security and privacy risks that they would be facing.

There were questions on the respondents' awareness of existing privacy issues on social media, their encounters with social media issues, their thoughts on privacy controls, the names they used on social media, their privacy settings, knowledge of social media privacy policies, and changing the default data collection settings. These were aimed at finding out the social media privacy awareness of users. The questionnaire included questions on the respondents' views on platforms that were too aggressive, used deceptive tactics to gather data, had poor user support, and were selling data to third parties. These questions not only collected data but also enlightened users on the prevailing issues on social media. If users had not been aware of such issues, these questions would spark interest in them. Finally, the research questions also tried to get the respondents' opinions on the possible mitigation measures to social media security and privacy issues. The respondents were thus asked on their views on the practicality of the involvement of governments to control social media platforms and punish platforms that would violate privacy of users through fines and censorship.

5.6 Survey instrument

The questionnaire was administered using Google Forms, which would capture and return the collected data in real time. The questionnaire was comprehensive and ensured that all the topics of interest to the research had been covered in the questions. To access the survey, a respondent had to view it on a browser. Google Forms was the most ideal as it supported the use of many data collection tools, such as radio buttons and checkboxes. It was also more mobile friendly and had no display issues on the respondent's devices. Since the forms were not scripted, there were no errors arising from the failed capturing of data.

Google Forms was also effective in breaking the entire questionnaire into tiny and related bits. Users would submit the questionnaire in parts; thus, they were not discouraged by its actual length. The breakdown of the survey into bits also made it appear to be more streamlined and focused on a particular issue at a go. The distribution of the questionnaire was done through Gmail. The respondents were not required to have a Gmail account in order to access it; they were only required to visit the link sent to their emails and access the questionnaire. The details about the respondents that received and completed the questionnaire were not stored. This is because such action would have to be treated as private information and thus require more security for storage. The Google Forms form was set to be completed in guest mode. Therefore, the users would not later on be identifiable; only the data submitted on the forms would be received. The senders' addresses were not recorded in this mode as well.

5.7 Statistical analysis

Data collection was done using Google Forms and the analysis part completed in Microsoft Excel. The data obtained was mapped back to the questions and then, the analysis was done. The collection of the data using Google Forms was such that the collected data

would be easy to formulate findings. From the raw figures, percentages were calculated to help make more sense of the data. The raw numbers were the actual number of respondents that gave a certain answer. From the total responses, the calculation of responses was quite simple to achieve.

In some instances, data had to be cross-tabulated in order to arrive at finer details. For example, if it was of interest to find out the number of particular respondents in a subgroup that gave a certain answer, cross tabulation would be done. Mostly, cross tabulation was of use when correlating the respondents' age, education level, and literacy level to certain social media usage tendencies.

Codes were also used in the statistical analysis of data. Since the data collection was qualitative, this type of data was not ready to be analyzed. Therefore, codes had to be used to convert the data into values that could be analyzed. For example, questions that asked users to rank their most and least used social media platforms had to be codified so that this data could be analyzed.

Charts were used to display the data in a richer and more appealing graphical format. This data would be drawn from the Google Forms backend and then carefully mapped into pie charts, bar graphs, and line graphs. Graphical representation helped to easily interpret the responses derived from the respondents. Graphs could readily tell the trend of responses and also discuss better the story that the data was telling.

5.8 Ethical considerations

The research was strict on ensuring that there were little or no ethical issues that came up. This was obvious since the research was studying an unethical practice by social media platforms. Where ethical issues arose, there were ready mitigation measures in place that

would be implemented. The following is a discussion of these ethical issues and their mitigation:

Use of participants' time – The respondents may have had some concerns on the time that they would spend filling the online questionnaire. This was fully understood as they would be breaking away from their activities and putting efforts into completing the 20-30 minute questionnaire. To avoid upsetting the respondents, they were informed, at the sampling stage, the duration that the questionnaire would take and that they were free to opt out at any time. The participants were also informed beforehand that there would be no rewards given other than an honest vote of thanks.

Identity of the participants – Since the respondents would receive the questionnaire form through their emails and fill it on their browsers, there were ethical considerations on whether the form would collect their personal information or store cookies in their browsers. To mitigate this, the questionnaire was configured not to collect the details of the persons that filled them. Participants were also informed that the form would temporarily store cookies as they filled the forms by Google. They were also informed that it was a standard practice for all Google services and this cookie data was not to be used by or for the purposes of the research.

Intellectual property – There were concerns that some of the participants would claim the data they gave during the research as their intellectual property. To mitigate this, the form had a disclaimer that informed the respondents that their contributions were merely for observation of trends and individual contributions would not be published. Also, the respondents were not asked to contribute solutions to the problem that was being researched, something that closed the avenues for intellectual property claims.

Chapter Six: Results and discussion

The study collected and processed a lot of information from both the primary and secondary data sources. To begin with, this chapter will discuss the outcomes of the secondary data collection first before moving on to the most comprehensive presentation of the results of the primary data.

6.1 Secondary data results

There were two secondary data sources and the paper wishes to begin by disclosing the results of the survey done by Pew Research Center that was successfully undertaken by 607 respondents (Madden, 2016). The first question that respondents were to answer was whether they were aware of the claims that the US government was monitoring their communications. This question related to the privacy of their communication across all media, not only social media. 43% said that they were aware of those claims, 44% said they had once or twice heard those claims, while 5% claimed that there were no such allegations.

The next section asked respondents about their concerns over the issues of increased spying by businesses and governments on their personal information. The respondents were asked to state whether they felt that they still had control over their information. 91% of the respondents said that they believed that they had lost their control and 88% said that it was impossible to delete their information online. 80% of the respondents who were registered on at least one social media platform said that they had concerns over third-party businesses and the level access they were being given to a user's data. 70% of the respondents said that they were also concerned about the government accessing the information that they shared on social media without seeking for their consent first. 80% of the respondents said that US

citizens ought to have been concerned about the government monitoring their communications across various media. When asked whether the government should have been more involved in regulating adverts, 64% were for the options, with 34% against it, and 2% undecided. The respondents were asked to either agree or disagree with a statement that said that increased access to personal data led to more efficient services online. 61% of the respondents disagreed with the statement strongly, 30% disagreed, and 9% slightly agreed with it. However, when asked to pick a side as to whether they were ready to share their personal information with companies for free services, the results were unexpected. A total of 334 respondents affirmed that they would be willing to share their data so as to continually access free services such as emails.

The third section looked into the confidence levels that users had with some communication media. Respondents ranked social media platforms as the most insecure communication media, and thus they had the lowest confidence levels about it. Landlines were seen to be the most secure communication media, closely followed by cell phone calls, and text messages. 81% of the respondents felt not very secure or totally insecure when using social media platforms for communication. This was closely followed by 68% of respondents who felt the same about communicating over chat or instant messages.

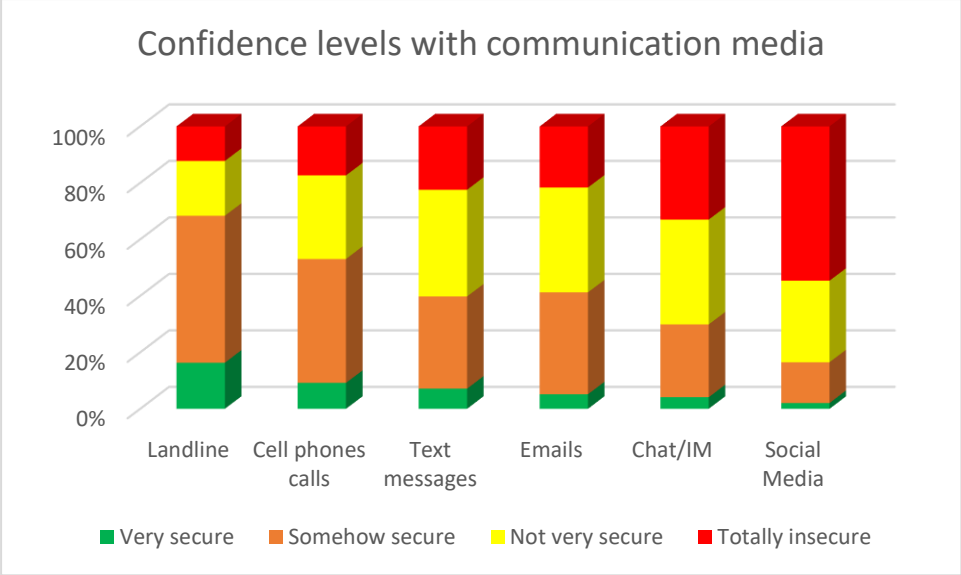

Figure 1: Confidence levels with communication media

The next section asked the respondents about their wish to protect their privacy online and whether they thought it was possible for one to be anonymous. 61% said that they wished to do more to protect their online privacy, while the rest said that they had already done enough. About anonymity, 76% of the respondents claimed that it was impossible for them to be truly anonymous online. Concerning their reputation online, it seemed that the demography of users above the age of 50 were more vigilant about their information online. However, in total, 62% of the respondents affirmed that they had searched for their own names on the Internet and 47% believed that their names had been searched by other people. A very vigilant 6% of the respondents affirmed that they had set up an alert system to notify them whenever their names were mentioned anywhere online.

The following section enquired from the respondents, the contextual factors that may have determined whether they did or did not disclose their information online. Concerning the use of their names, 58% of the respondents agreed that they always posted on social media using their actual names, while 42% said that they preferred posting without using their real names. On the part of contexts that forced users to disclose their information online,

24% said that there were work-related policies to do so, and 11% said that they did so to promote themselves online. The rest said that they had no contextual influences forcing them to disclose their real information.

The last section wanted the respondents to rank the sensitivity of their different private data that they feared being disclosed. It was seen that most were afraid of their social security number being revealed online. Surprisingly, they were not so much concerned about their purchasing habits being recorded or their political views. However, 77% of them were either very or somewhat sensitive about their emails being read, while 83% were sensitive about their physical location being tracked by either social media platforms, applications, or websites. 75% were sensitive about their phone address books being read off, 66% feared their birth date being collected online, and 65% were sensitive about their browsing habits and searches being collected.

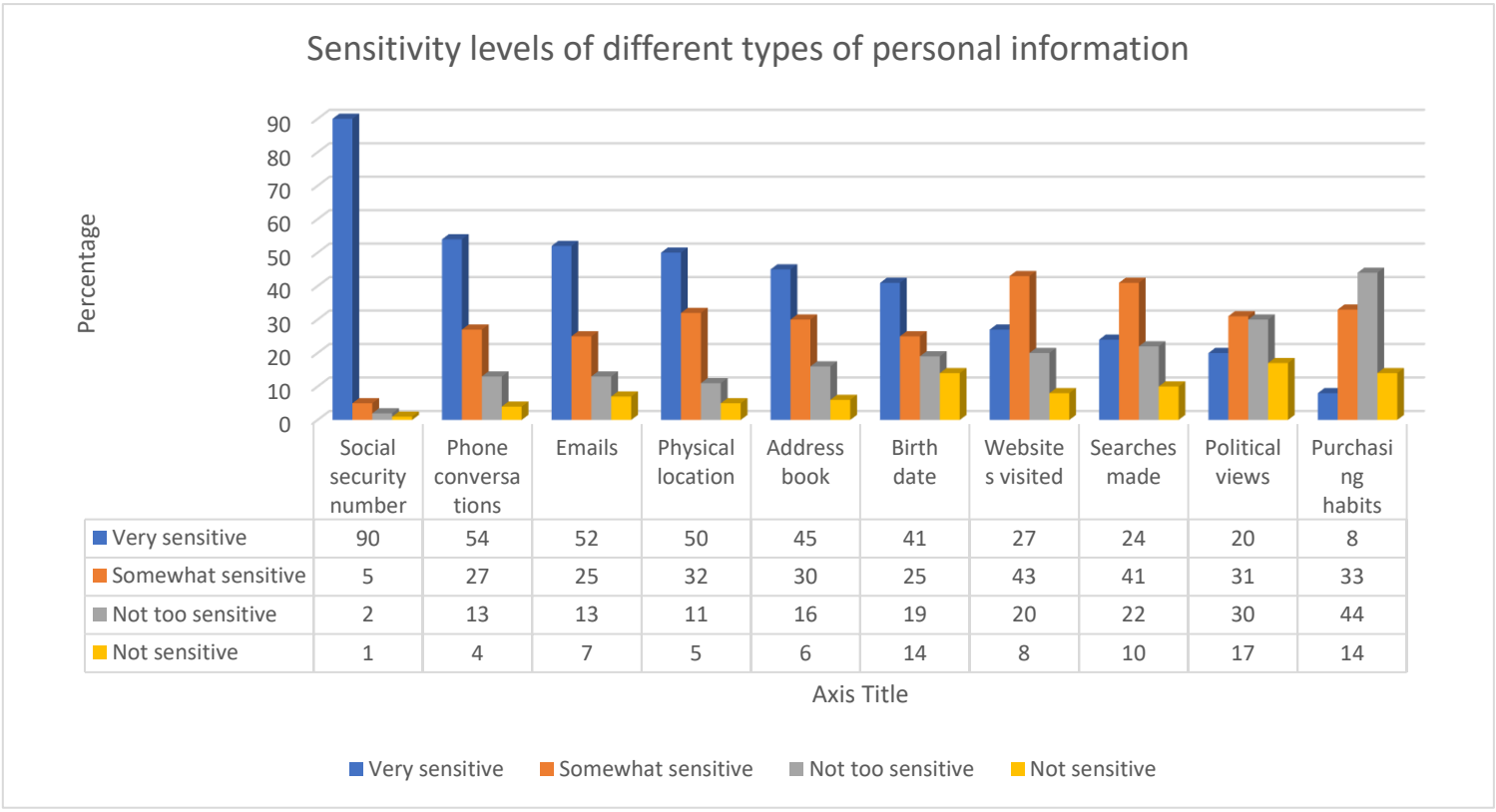

Figure 2: Shows the different sensitivity levels of different types of personal information

Moving on to the next research done by Alawawi, there were quite some important revelations that his study came up with. His research was centered within a certain university, whereby 50 students were selected to do a short questionnaire-based interview concerning social media and privacy (Alalawi, 2015). The students, who were selected, were above 18 years and were taking courses related to journalism and communication. The first part of the questionnaire asked the respondents to give their online privacy concerns and their level of knowledge about the existing privacy issues. 98% of the respondents responded in the general direction that they were highly concerned about their online privacy, while 2% seemed unbothered by their privacy.

In the second part of the interview, the respondents were asked about their attitudes towards social media networking and how they used social media. 18 of the 50 respondents

said that they approximately spent 3-4 hours on social media every day. 12 respondents claimed to spend between 1 and 2 hours on social media. The rest of the respondents claimed to use social media platforms for over 4 hours each day. This showed that there was moderate to high usage of social media in the university, especially for respondents who were between the ages of 18 to 28 years. Concerning the reasons why they were on social media, 50% of the respondents claimed that it was because it was a good avenue for staying in touch with their friends and family. 40% said that it was because it was a good avenue for following up with celebrities and entertainment events. Only 10% said that they used social media for advertising purposes.

The third part of the interview sought to find out the attitudes of the respondents towards privacy policies. The respondents were asked whether they took the time to read privacy policies of different social media platforms. Shockingly, 70% of the respondents had never read even a single line of the privacy policies. This is despite them having agreed to the terms and conditions as they signed up on the social media platforms. Only 30% said that they did read some parts of the terms and conditions of the social media platforms. From this 30%, 5% of them had actually read the entire privacy policies of the social media platforms that they were active on. The major complaint about not reading the privacy policies was because they saw them be too wordy, with 10% claiming that they simply did not have the time to read the policies as they signed up.

The fourth part of the interview asked the users about who they thought the responsibility of ensuring safety on the social media platforms lied on. 31 of the 50 respondents said that they believed that the responsibility of security majorly fell on the social media platforms. This was because they were just mere users and as such it was upon the social media platforms to protect their privacy. 20% of the remaining respondents said that it was upon their government to ensure that they were safe on social media by imposing

the relevant legislations. 18% said that the responsibility of safety fell on them. They attributed this to the failures of the social media platforms and governments to protect the privacy of users and even at times being the enemies of this privacy. 9 respondents claimed that they did monitor whatever they shared on the Internet and particularly on social media platforms.

6.2 Primary data results

To complement the available data from secondary sources, this research saw it fit to conduct a short survey and obtain more updated information from users. Therefore, an online questionnaire was coded and sent to a number of respondents. The online questionnaire that was given to users in the form of a survey got back 100 valid responses within a short time and those were considered sufficient for the study. The recorded responses were converted into percentages for easier analysis. The end results as extracted from the database are in Appendix A.

6.3 Discussion of the results

The following section discusses the results obtained from both the primary and secondary data collection. Logically, the discussion of secondary data has been placed to precede primary data. This is to help form a base of understanding and also to give perspective to the discussion of primary data.

6.3.1 Discussion of results from secondary data

6.3.1.1 From Pew Research Center

The data collected fell within all the privacy concerns that users had with both social media platforms and the government. When the 607 respondents were asked whether they were aware of the US government monitoring their communications, 87% said that they had

heard of that grim reality. This means that most users are aware that their privacy is already being violated. It is rather unfortunate that the entities that people trust to protect their rights are the same that are actively spying on them and breaching their privacy rights. When asked about their level of control over their information that was being collected by various platforms, 91% regretfully confirmed that they believed they had minimal control. This showed that users were becoming aware of the fact that they were not the ones in control of their information online but rather the different social media companies. Users regret this fact that they cannot safeguard their own information and that social media companies are busy brokering deals to sell off their data. When asked about the ability to delete their online data, 88% believed that it was impossible for one to fully delete his/her data. Some social media platforms do not even allow users to delete their accounts; they can only deactivate them. Social media companies support a one-way flow of data and that is to them. Data is hardly withdrawn from them and it is all because of their greedy nature. This is the reality that users have to live with. 80% of the respondents shared their concerns about third parties being able to access the data that they shared. Some platforms, such as Facebook have already been found to be giving out too much data for simple third-party apps on Facebook. Facebook is not the only culprit; it seems that most of them are in this guilt list. They parade user information before advertisers in order to attract fat contracts. Their only concern nowadays, seems to be making money out of personal user information and users are increasingly becoming aware of this. Facebook is in the spotlight because it is doing that to its user base of close to 2 billion users.

The researchers also put the government into the spotlight when they asked the respondents whether they felt concerned about the government collecting social media data. 70% of the respondents felt that they were highly concerned about the government doing this behind their backs. Users are aware that there have been rumors of some governments

forcefully withdrawing user information from their personal account. Some governments have been accused of forcefully requiring some social media platforms to give up accounts of some users without their consent. Governments have already painted bad images about themselves, and it is such a shame that at one point, they turned to snooping around user's private chats. This is why users feel highly concerned about their shameless interference with their personal lives despite not doing anything wrong. The reality is that in this battle of privacy, users have lost confidence in their governments to safeguard their privacy. This is because their previously exposed intrusions of user social media accounts make them and the social media platforms equally crooked. This is why 64% of the respondents felt that their government needed to pull up their socks when it came to regulating online adverts. Social media adverts fall into this category, and a lot of the filth around the lack of privacy has been brought about by unregulated advertising. Advertisers are being sold private data by social media companies and most governments have taken this lying down. 34% of the respondents said that they did not want governments to get involved with the regulation of adverts. This is most likely because governments have betrayed their trust in the past, and they are worried that this regulation may be turned into something else. Governments may use this as an opportunity to pull out more private user information for their own gains or in the name of fighting terrorism.

Social media platforms have pedaled the notion that access to users' private information is used to better the services they access online. The researchers asked the respondents whether they agreed with this, and it turned out that over 90% of them disagreed with it. The respondents were aware of what these platforms actually use their personal data predominantly for. A platform such as Facebook cannot be said to be using personal data to better its services while it is dragging court cases behind it over giving this data to third parties without consent. The respondents seemed to be well aware of the facts about the

cheap lies sold by social media platforms. When asked whether they were willing to share their personal information in order to continue to access the free services, 334 affirmed. While it may seem a bit awkward, it was actually because deep within these platforms were excellent services that users had made to be a part of their lives. Take Facebook, for example; it had been an excellent social media platform for a long period until it started advertising aggressively and giving out private user information without consent. 334 respondents would rather have the little information that they would continue sharing given out to advertisers to continue accessing social media services. It did not, however, mean that they were comfortable or happy about the way social media platforms were using their data.

When asked about their confidence levels with the different communication media, it did not come as a surprise that social media had the poorest confidence level. 80% of the respondents said that it was either totally insecure or not very secure. Social media is more insecure than the outdated text messages they replaced. Social media platforms are ridden with identity thieves, social engineers, stalkers, and most of all, users are not 100% sure that even their private chats are private. The mishandling of the user's private data has also contributed to this low confidence level. People no longer have trust in the confidentiality of whatever they post or even chat on social media.

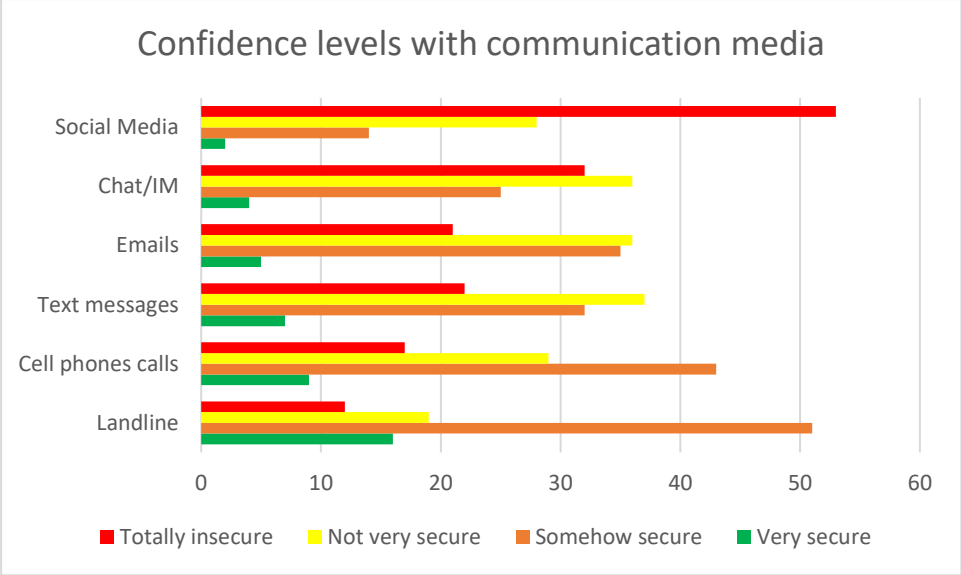

Figure 3: Confidence levels with communication media

Concerning user efforts to secure their data, 61% of the respondents said that they wanted to do more to protect their personal data. Just about the rest of the respondents said that they had done what was possibly enough to secure their private data on social media. This means that it is a general feeling among most users that there is more that they can do to secure their private information, and it is due to this that some people have resulted to removing their personal information from the prying eyes of stalkers, identity thieves, scammers, and social engineers among the rest. Unfortunately, even if they remove some of their personal data, it has already been stored by social media platforms, sold off to advertisers, or used to profile them for advertising. Concerning anonymity, 76% of the respondents said that it was impossible to achieve total anonymity online. These were the respondents that were aware of the dark side of posting anything online and especially on social media. Even if one sets his/her social media account to private so that no one else can see, deep in the databases, this information is sold to third parties. This information is sold in order for the social media platform to make profits for the social media companies. The more

information a company can scoop from its users, the more its revenues grow. That is why they will ensure that users cannot control the privacy of their data in the back end. There is no setting that users can adjust to prevent the social media companies from extracting their information. What they are given to control is just a mere tip of the iceberg of privacy. The big chunk of data is left unregulated, uncontrolled, and in the hands of the social media companies.

Concerning remaining vigilant on one's online personality, 62% of the respondents said that they searched for their own names on the Internet. This was the group of users that was very vigilant of their online personalities. With the advent of crimes such as identity theft, it was wise to search for one's name on the Internet so as to nab fake accounts or get inaccurate information posted about one. That is why 6% of the respondents said that they had put in place a sophisticated alerting system to notify them that their names were mentioned online. This might seem to have been a bit of a stretch, but probably it was for people whose online identity mattered a lot. These could be distinguished people in the society or people who hold high moral authorities.

Concerning the ways people disclosed their information online, it was found that 58% people posted on social media using their real names or rather they used their real names on social media. 42% of the respondents said that they preferred not using their real names on social media. This is quite understandable; 58% can be assumed to be quite aged or have had their accounts created with their real names initially. With the current privacy issues, people have had to rely on other ways such as minor deceptions to protect their real identities. Social media is not a safe playground anymore, where one only connects with friends and family; it is a dangerous world and people will not feel safe to use their full names. Commonly, users will have one real name combined with other names or phrases. However, this does not fool

social media because they can unearth one's identities using emails and besides this, they profile users for adverts based on the information provided in their accounts, not their names.

Concerning sensitivity of data, it turned out that users were more concerned about the revelation of their social security numbers. This was followed by their phone conversations and emails. Inbox messages on social media platforms fell in this category. Users were actually not concerned about their purchasing habits being recorded online. They were totally fine with their shopping habits being collected for suggestions because that is not aggressive at all. Social media platforms, on the other hand, actively participate in aggressive and intrusive advertising. They do not want to study a consumer's shopping habits, that is too shallow of information to sell at a profit. They want to spy on their consumers' lives to see what they talk with others about, where they live, where they work, their marital status, and thus have resulted to stalking them to get this information. 65% of the respondents thought that it was somewhat sensitive to gather their online searches and 75% thought the same about the websites they visited. 67% felt sensitive about their birth dates being collected. Companies such as Google have already collected this data and use it for advertising purposes or to sell to third parties. Social media platforms want to know someone's birth date of all other things in order to refine adverts. This is information that ought to be treated as private. However, social media platforms have been observed to disregard user privacy when they (organizations) stand to benefit. That is why users cannot opt not to have this information accessible by the social media companies. They can only restrict it from being accessed by their friends who probably know nothing about intrusive advertising.

This is the era that the world is in, the one where privacy does not exist. The research done by Pew Research Center proves that privacy is almost a non-issue to social media companies and people cannot trust their governments. It can be said that the research was conducted on a more knowledgeable group of people as it can be seen from their responses.

They were aware of the dirty tricks used by these social media companies and were aware of the poor regulations. They were conversant with the fact that they carried the burden of protecting their own privacy. They might not accurately represent the typical user who is still oblivious to the privacy issues on social media.

6.3.1.2 From Alawawi

The research done by Alawawi was in a college and most of the participants were students. This is a group of users that are not yet entangled with other life responsibilities and have more time to spend on social media. About their concern for privacy, 98% said that they were concerned about their online privacy. Again, this affirms that most users are increasingly becoming aware of their privacy. 60% of these students said that they used up between 2 to 4 hours on social media and the rest spend over 5 hours on social media. Therefore, this is a group that is vulnerable, because it spends a lot of time exposing more information about themselves to strangers. When asked the main reason for being on social media, half of the respondents said that it was in order to connect with friends and family. That can be translated to almost 80% of social media users who only join to stay in touch. This is the most critical group in social media as it generates the most content. The quotes, motivations, baby videos, cat photos, and hiking photos among other exciting content is what keeps users coming back to social media. Social media is only alive because users keep generating content and thus they ought to have their privacy respected. Instagram cannot start posting its own pictures, Facebook cannot update its own status, Snapchat cannot send its own clips, and LinkedIn will not connect a user to itself. These social media platforms exist solely due to the users who create and post content. 10% of the respondents said that they use it for advertising purposes. This is the group that social media platforms accord a little respect just to make money out of them. The real laborers, the ones who tirelessly create content and are not paid a dime are not accorded any respect. Instead, their privacy is violated, their

accounts are ransacked, private chats opened, and their information is collected and sold without their consent. It is the harsh reality of social media, always biting the hand that feeds it.

The respondents were also asked about their knowledge of terms and conditions of the various social media platforms. 70% of them confirmed that they had never read the terms and conditions, especially the privacy policies of these platforms. This represented the average social media platform user. It is unfortunate but not surprising to find out that users do not actually read the terms and conditions of social media platforms. This seems to be what social media platforms count on, their users being uninformed of the contents of the privacy policies or the entire terms and conditions. This is why the terms are flashed to users uncomfortably during setup and they are told to agree to them in order to continue with the account setting up process. They are strategically placed at that point because they are wordy and complex, thus most users will quickly click on agreeing to the terms. What they do not know is that that is the point they sell their rights. That is the point where social media platforms are given the rights to own a user's information. Social media platforms know that what they do is not totally good and thus they come up with long or complex worded privacy policies to discourage users from reading them. In the United Kingdom, the MPs said that the social media platforms used complex terms and conditions for the average user who has never stepped in a law class to understand. This is exactly why the average user will not know what happens to his/her data when he/she signs up with a social media platform. This research shows that a majority of users simply agree to terms and conditions that they are not knowledgeable of.

Concerning the security of social media platforms, 62% said that it was the burden of social media platforms to ensure that they were safe. 20% of them said that the responsibility lay with the government to ensure that their privacy was not violated. The last 18% said that

the responsibility fell on them. This is a clear illustration of how normal users think about their online privacy when it comes to who should enforce it. 62% of these respondents were of the opinion that since the social media companies created these platforms, it was upon them to ensure security and privacy of the users. These views can be viewed as the general feeling of quite a substantial number of social media users. They know that these companies had developers build these systems from scratch and within the development process, the companies ought to have ensured that total security was provided for users. This security must have included protection from privacy invasion from other users and third parties. It seems that these platforms only made the platforms for one-sided privacy. Users can, up to a certain level, protect themselves from other users. They can change their social media accounts to be private thus inaccessible to others, and they can block users that they find annoying or with malicious intentions. On the other side, the users cannot enforce their privacy from the prying eyes of the social media companies and the third parties that are given extensive access to user private information (Krishnamurthy and Wills, 2009). There are no restrictive settings that users can deploy to prevent these two intruders from collecting and using their data.

Another group believed that it is upon their governments to fight for their social media security and privacy. This is doable by laying down certain policies and establishing strict legislations. To the surprise of this group, some governments have been in cahoots with these social media companies to give them the private user information that they ought to be protecting. Other governments are simply not getting involved, probably quieted by some monetary rewards from these platforms for their silence. There are a few organizations such as the EU that are highly vocal concerning its citizens' privacy. Lastly, there was a group that believed that their online security and privacy fell majorly upon them. These are the users that are aware of the existing security threats on social media, especially stalkers, and identity

thieves (Krombholz, Merkl, and Weippl, 2012). They know that the more personal information they share on social media, the more danger they put themselves in. This danger can be extended to their family and friends too as has been seen previously when identity thieves start asking for money from frequently contacted people by their victim. These users are also aware that their information is being collected by the social media platforms and thus have reduced the amount of personal information that they share or have reduced posting on social media. There is quite a number of users that are opting not to post on some rather insecure platforms such as Facebook and this is why the company has started reposting a user's old posts. This is the group that most users ought to be in but unfortunately, not all are informed enough to make this decision.

6.3.2 Discussion of results from the primary data

Moving on to the research carried out by this paper, there were many people invited to take a lengthy online questionnaire that spanned over a number of issues and the first valid 110 responses were taken for analysis. The first question aimed at establishing the age brackets of the users and it turned out that there were many respondents on social media aged between 18 and 28 years. This is the age that has most social media users as these young people try to explore various exciting social media platforms. They are great content generators because some are in school and others are very young in their adult lives and do not have many other responsibilities. They are early adopters of online shopping and thus online ads suit them more. Next, most of the respondents had an education level of up to an undergraduate degree and a few had a Master's degree and PhDs. There seemed to be a close link between education levels and age brackets. The respondents at the bottom of both age and education pyramids are the most active on social media and thus the most important content creators.

Age groups of the respondents

Table 2:Age groups of the respondents

Age group	Number of respondents
18-23	50
24-28	33
29-33	11
34-39	10
40-45	6

The pie chart below is a representation of the data in table 2. As can be observed, most of the respondents were in the age groups of 18-23 and 24-28.

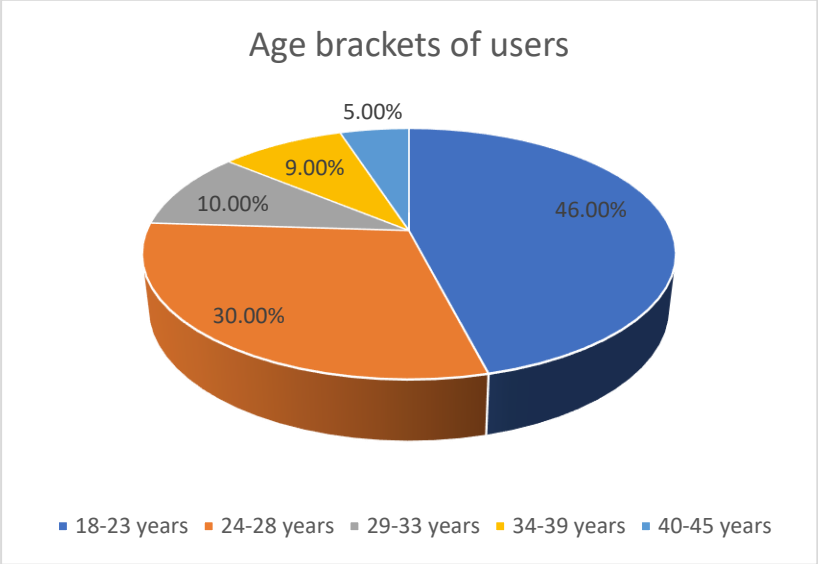

Figure 4: Age bracket of users

Table 3: Literacy levels of the respondents

Literacy level	Number
Undergraduate and below	66
Masters	28
PhD	16

The pie chart below represents the data from the table above. As can be observed, most of the respondents were literate only up to an undergraduate level of education.

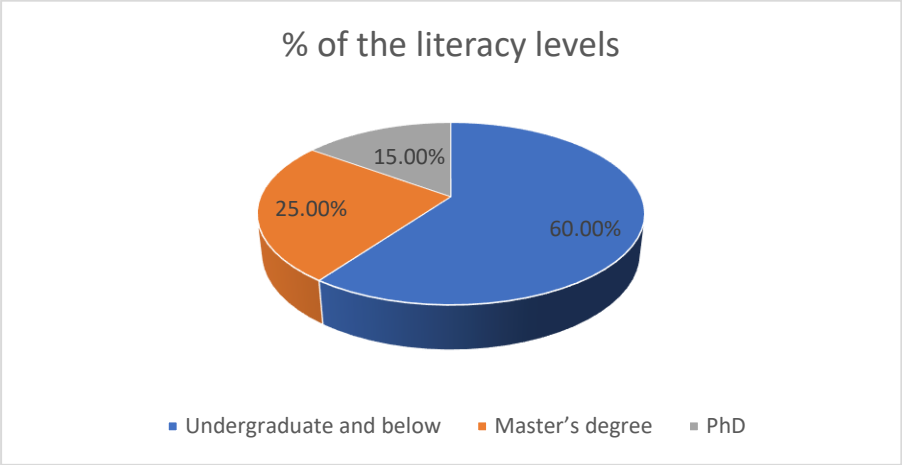

Figure 5:shows the % of the literacy levels

It was also established that 95% of the users did not have an amateur level of computer literacy. This means that they did not study courses related to IT up to advanced levels. 45% humbly ranked themselves as having a beginner level of computer literacy. These could be said to be the most vulnerable because they mostly lied low when it came to age and education level. This was the group that was more prone to being oblivious to the security and privacy issues in social media. This was the group that ought to receive more protection and advice concerning their online security. 50% of the respondents claimed to be at a

professional computer literacy level, meaning that a substantial number of respondents were aware of these online security and privacy issues.

The respondents were asked to select their most favorite social media platforms. It came as no surprise when they ranked Google Plus and Facebook to be their least favorite social media platforms. Facebook has of late being receiving its fair share of criticisms due to its intrusive approach to advertising at the cost of users' privacy. That is why it was rated the second least favorite social media platform after Google Plus. Many people have a general dislike for Google Plus probably due to its unsocial like and unfamiliar appearance (Magno et al., 2012). It is easy for a Twitter user to use Instagram because some metaphors and labels are shared by the two. The same holds true for Facebook. Coming to Google Plus, it has an unfamiliar appearance, it stacks posts in a different way, it uses unfamiliar terms such as circles, and it is not easy to use for new users. Secondly, people hate the way that Google has been forcing its adoption using dubious ways such as forcing people to sign in to leave comments on YouTube. This is such a poor strategy; users do not want to be forced to sign into multiple platforms to accomplish a small task such as saying 'thank you' on a YouTube clip. Another reason why Google Plus is ranked as the least favorite is because most people know that it was launched just after Facebook to offer competition, and it failed miserably. Unlike Facebook, it did not receive adoption and anyone who tried to use it would find that his/her friends were not on it. Users are the critical ingredients in social media platforms without which the platforms would simply crumble due to lack of exciting user-generated content. Facebook is headed in that direction too; people are posting less and less each passing day. The user base is almost at a stagnant with a decline in new sign ups. Twitter and Instagram were ranked the most favorite because they are mostly used by the youth. It is a safe hiding place from parents who opened Facebook accounts over 9 years ago. LinkedIn is

mostly preferred by professionals; the network stands out as the most professionally organized platform.

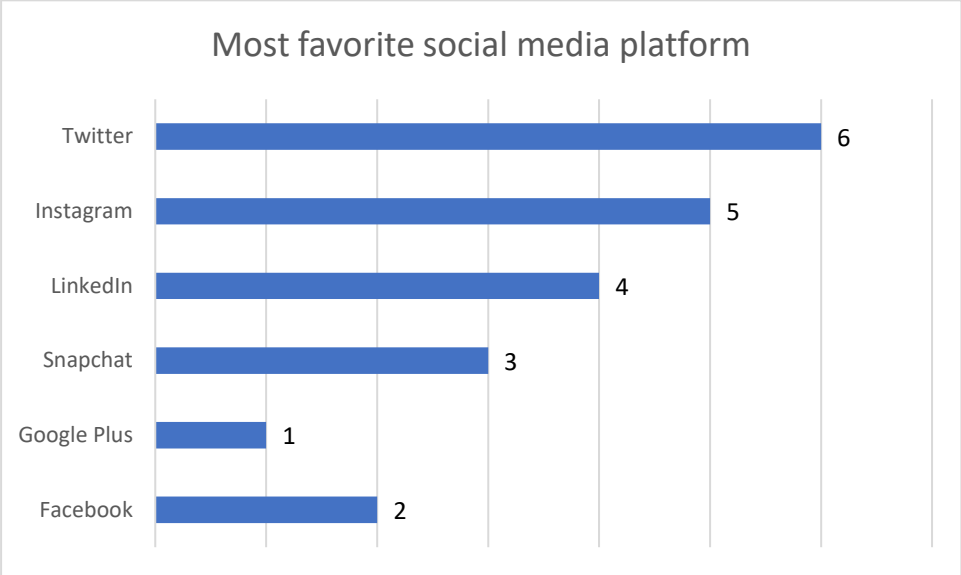

Figure 6: Ranking of social media platforms by respondents

Users were asked about the social networks that had the most privacy issues; of course, Facebook came leading the pack. This platform has been outed already; users know the dirty things that are happening in the back. They are aware that their privacy has been sold off to third parties and advertisers; they are aware that this is a platform that has transformed to be hostile to its users. Facebook spoiled its own platform the moment it decided to make money over advancing the platform as a social place for people to meet and connect. This is why it has been dragged to court several times over gross violations of user privacy. LinkedIn was selected to be the second platform with privacy issues. This is because users do not have the full trust on LinkedIn. Once it is given access to one's email, it is said to be collecting a lot of information, more than the contacts it says that it is discovering. The platform has also been accused of automatically sending connection invitations at times without a user's consent. It is also accused of being big mouthed in that; it keeps disclosing a lot of information to users. It keeps alerting the user's connections whenever one makes even

a subtle change to his/her profile. Twitter, Instagram, and Snapchat were said to have the least privacy issues. This is mostly because Twitter is disciplined when it comes to advertising, it has not been accused of reading chats or third parties access a user's private information. A few years back, however, hackers were able to break into the platform and access a lot of private data and this is why users ranked it third on the list of platforms with privacy issues.

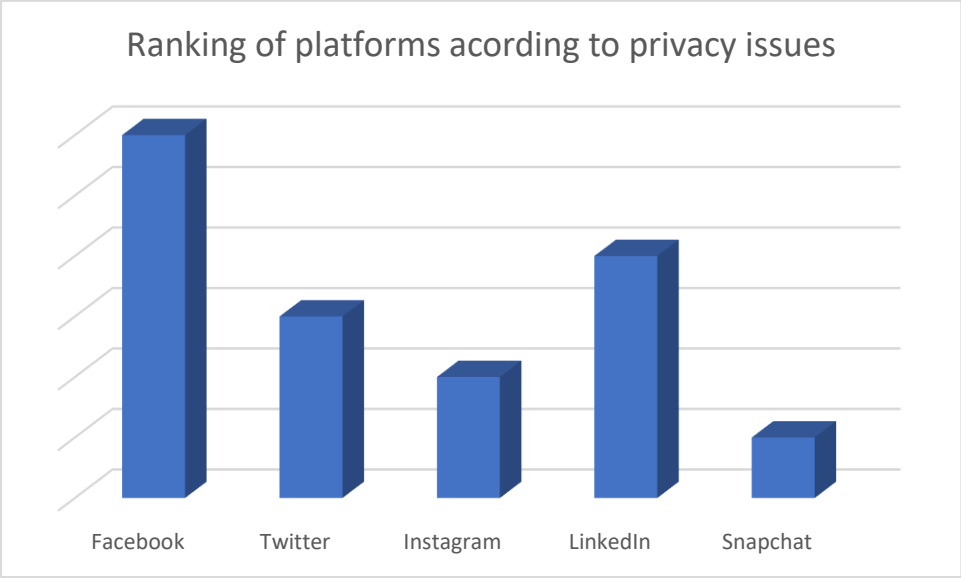

Figure 7: Ranking of social media platforms according to privacy issues

Concerning privacy issues, 99% believed that they faced a type of privacy issue on social media platforms. 80% said that they had been stalked on social media. This is a common threat facing users, stalking and especially girls and prominent people. Stalkers may have weird obsessions with someone or may be gathering a lot of user's information in preparation for a big attack. That is how social engineers do it; they nest around social media platforms and collect the little details that users post about themselves or their families online. Only 20% of the respondents did not feel that they had been stalked by someone on social media. When asked about being bullied on these platforms, 30% confirmed to have been cyberbullied. Cyberbullying is whereby a user is harshly criticized, verbally abused, and

threatened by other social media users (Bonanno and Hymel, 2013). It happens when one makes a certain comment and is seen to behave in a certain way that displeases many people. In other times, it happens because some people have so much anger in them that they feel like discharging at anyone who slightly annoys them. Cyberbullying is a major threat in social media as the verbal attacks do more psychological damage and have even brought about suicidal tendencies in victims (Bonanno and Hymel, 2013).

Due to the ongoing security issues and identity thefts, some users have resulted to not using their actual names on social media. This is so that even if data about them is collected, their real personalities are safe. This research asked respondents whether they were still using their real names on social media and found out that only 40% of them were. The remnants had cleverly either changed one name or resulted to using nicknames instead which are considerably safer than actual names. Social media was seen to be deeply integrated into people's lives. When asked whether they would live without social media, a whopping 75% of the respondents said that they simply could not. This shows that social media has already become a part of people's lives, another reason why it should be made secure. To further confirm that it was an integral part of life, respondents were asked just how many times they posted on social media. 55% said that they posted daily, while 30% said at least every week they made a post. Each time they posted, inevitably they were taking some risks if they shared their personal information. Most of the respondents said that they posted daily, which is good for the platforms while a potential danger for them as they could disclose regrettable information in their posts.

74% of the respondents said that they had between 100 and 500 friends on Facebook. Among these friends were supposedly people with some malicious intentions. Users ought to know that there are more dangers lurking around them on social media platforms; probably one of the 500 friends is a hacker or a stalker. There was an almost fair distribution of how

users set their Facebook privacy settings. 30% had their accounts private with 66% having either public or ‘friends only’ privacy setting. Of course, these platforms were built for social interactions, thus setting them as completely private would have beaten their purpose. This is why most users chose to either have their friends see their accounts or let the accounts to be visible by anyone. Privacy settings are mostly dependent on the sensitivity of the person towards his/her information being disclosed. This is why there is no one-off recommendation for privacy setting, where users ought to set their account. 85% of the respondents had given access to third party applications to some of their social media applications. These third-party applications do a few functionalities such as crafting for friends’ birthday cards on Facebook. However, it has been disclosed that these third-party applications were being given access to too much information than they required. For example, one would find a birthday third party application having access to his/her location, phone number, email address, and other sensitive private information. Concerning the personal data that users shared on social media, 92% gave out their real pictures, 80% their birth dates, 72% their locations, and 63% their email addresses. This is private data that is very sensitive and can be used by hackers, social engineers, identity thieves, and other malicious people. Users are oblivious of the dangers that they put themselves in when they disclose this information on social media. The social media platform will encourage users to spew out this information so that it may use it to profile them for advertising. However, behind the shadows are the malicious people collecting this information so as to use it to attack a user.

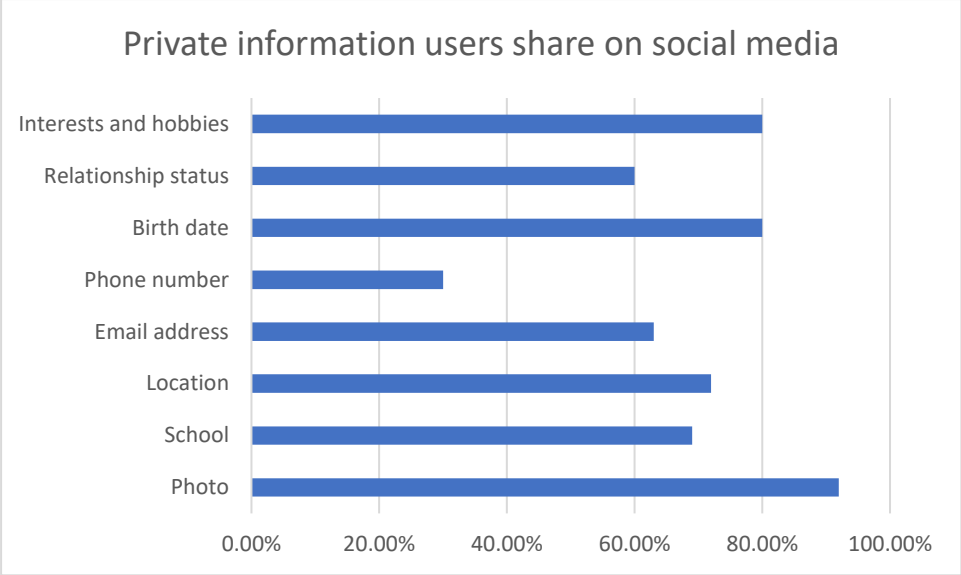

Figure 8: Types of private information that respondents had shared on social media

The research asked respondents questions surrounding the privacy of the leading social networks. First of all, they were asked about Facebook whereby 75% of the respondents disclosed that they never read the platform's privacy policy. This added truth to earlier researches that found out that most users had not read the privacy policies of the platforms they were on. The respondents said that they did not read it because it was too wordy. The 25% that read it said that the recent claims of Facebook collecting a lot of information and disclosing it without their consent were the real motivators. This is generaly the main motivator for users to read the privacy policies of a site or a platform (Milne & Culnan, 2004). They wanted to know what was contained in the privacy policy that made this legal in any way. 76% of the users said that they did not change their privacy settings from their defaults. This is a real concern, social media networks take advantage of updating their services with default settings that allow them to collect user data. Facebook, the usual culprit recently did this to its newly acquired platform, WhatsApp. They pushed an update that allowed WhatsApp to automatically send back user data and this was without obtaining consent. 70% of the respondents said that they found the process of changing privacy settings

was hard and 97% said that they were deeply concerned about the privacy issues on Facebook. The leading privacy issue that respondents reported concerned the level of access that Facebook gave to third party application to user data. This is understandable as the research was done at a period when a student had just uncovered the amount of information that Facebook lets third parties access.

Concerning Twitter, 85% of the respondents did not read the privacy policy because it was presumably long while the 15% that read said that they wanted to know more about Twitter's collection of personal data. 92% of the users did not change their Twitter privacy setting. This is quite explainable, Twitter does not request for too much data like Facebook and user accounts contain very little information that is to be guarded. 99% of the users also said that they did not find Twitter adverts intrusive. Intrusive was in the terms that the platform could have probably mined one's data and shoved a couple of adverts onto a timeline. Twitter is disciplined, it only shows one advert at a time and it makes it look integral to a user's feed. Facebook, on the other hand, will create a train of adverts and scroll them across one's timeline after having spied on their accounts to know what they liked or talked about. 75% of the respondents were of the opinion that Twitter protected the user data adequately. This percentage would have been higher were it not for the single breach that hackers once did into the platforms and thus stealing a lot of private data.

Concerning the WhatsApp messenger, 85% of the respondents said that they were alerted of the new setting that Facebook introduced to fetch data from the platform. The same respondents said that they changed it to prevent Facebook from continuing to draw data from WhatsApp. This is probably the biggest sign of disrespect that Facebook could do to users. WhatsApp creators strictly stayed away from selling adverts and it seems Facebook wants to drag users down that path. That is why 90% of the respondents said that they believed that there would be more privacy violations in future on the platform. This was because it was

Facebook running the show after its acquisition of WhatsApp. The respondents were asked about the other platform that Facebook acquired, LinkedIn. 96% of the respondents said that they were annoyed by the notifications that LinkedIn send them. LinkedIn is fond of finding small things to make noise about and it sends connection notifications that sound too needy. 96% of the users said that the platform is too nosy. LinkedIn will not spare even the least of changes that a user makes or remind a user's former employer to wish them a happy 1-year anniversary at another company. 80% of the respondents had shared their primary email address with LinkedIn probably because it is supposed to be professional. However, 99% of these said that LinkedIn was too intrusive of their private emails.

Concerning Google Plus, the general feeling was that not many people used or were familiar with the usage of the platform. They had also never changed their privacy settings and most of the respondents had never posted or just posted something in 6 months. On Skype, 60% of the respondents said that they were aware of the claims that Skype calls could be intercepted and that Skype had previously given out user data to intelligence agencies. 62% of the users said that they could no longer trust skype with sensitive information. On Instagram, users were protesting the ownership of photos that they uploaded. 95% of the respondents said that they wanted to retain ownership of the photos they posted. In the general questions, it emerged that many users were aware that social media platforms had data mining interests on user data. They also thought that social media platforms did not do enough to secure user data. Social media platforms were said to be violating user privacy rights and others using deceptive tactics to get user data. A company that knows the harsh outcomes of using deceptive tactics to get user data is Google and it seems Facebook wants to go in that general direction. Respondents said that they believed that social media platforms were selling off their users' data to third parties and others simply let third parties have too

much access to user data. Governments were accused of not doing much to protect user data and majority of the users said that advertising was the culprit behind these privacy violations.

Respondents finally said that social media platforms ought to have been subjected to tough privacy rules. They said that the platforms should have been seeking for explicit consent from users in order to collect data from them. This means that they disapproved of methods such as Facebook planting a default setting to allow it to collect user data without requesting for consent. Accessibility of privacy settings on social media platforms was ranked lowly and users complained that even these settings did not give them total control of their privacy. All the respondents said that the fines and punishments that violating social media platforms faced were not adequate. This was because their enormous profits were able to settle the fines without a major effect on the platform's profitability. Users wanted to be in a position to terminate all their social media accounts. This is something that most social media platforms have made impossible.

All the results can be viewed here.

Chapter Seven: Conclusion

7.1 Preamble

The previous chapter has looked at the threats in cyberspace that are a result of social media. It has reviewed the existing policies in organizations that have been partially able to secure against these threats. It has then come up with its own threat intelligence, a framework to mitigate the threats, user awareness training, and how to recover. It was the last in the many chapters that have delved exhaustively into the issues surrounding social media security. The following section will highlight the contributions by each chapter.

7.2 Contribution of chapters

Each chapter in this thesis has been substantial by touching on key pieces of information. Chapter 1 has introduced the thesis and its subject matter. It has given the overview of cyber threats and then narrowed down to a particular one, user privacy. In user privacy, the chapter has isolated social media privacy issues to be the concern of this thesis. In developing the basis for the choice of this issue, the chapter has explained the motivation. There are two categories of problems that the chapter identifies that form up the discussions in the whole research. It identifies the problems emanating from privacy violations by social media companies and then mentions the issue of attackers that lurk on social media. The wide scope of the research is discussed, the objective stated, and the contributions of the thesis discussed.

Chapter 2 has acknowledged the works done on this topic by other researchers. It has first explained for how long the problem has existed thus leading to research on it. From the

many researches that have been done on the topic, the chapter selects four. These four are of particular importance to this topic; in this, they approach social media privacy from interesting viewpoints. The chapter has, therefore, explained what has been done so that this research can cover some of what has been left out. The discussed literature laid down the foundation of the research in a better way and gave several lenses on how the problem can be viewed.

Chapter 3 has discussed one of the vices that have grown of late due to social media and social engineering. It has introduced the users to social engineering and taken them through some of the key phases in a social engineering attack. Of importance to note is that the discussed phases are not strictly followed during attacks. This is because social engineers capitalize on the chances that avail themselves and also due to the preference of social engineers to remain fluid during an attack. The chapter has established the relationship between social media and social engineering. It has exposed social media as the main avenue through which social engineers are either gathering information about targets or just directly attacking them. After the establishment of this connection, the chapter has looked at the main challenges of social engineering as an attack. It has discussed the invisibility of the threat vector. It has explained that the attacker is hardly known until it is too late and damage has been done. The other challenge that has been explained is that of enterprise security. It has been discussed in the perspective of one user leading to the compromise of the security of an entire enterprise. This chapter has also proposed some solutions to particularly deal with social engineering.

Chapter 4 has been the main meat of the thesis that has gone through the study done in this thesis. It has discussed several things about the study. The collection of data via samples and surveys has been discussed. It has highlighted the optimal number of respondents that were expected to take the survey and those that eventually did. It has then

discussed how the data was processed and analyzed to come up with usable figures. A discussion of what the results say has been given to help put everything into the perspective of social media security and privacy. Based on the results, some recommendations have been made to address the social media privacy and security issues. The study has identified three key points from which these solutions must be implemented. These are users, governments, and social media companies. The recommendations have been duly explained to show their practicality and potential for effectiveness in dealing with the problems highlighted by the research.

Chapter 5 has then looked at more general threats in the cyberspace that have come up due to social media. The chapter has evaluated the existing policies in organizations that have been put up to deal with these threats. To better understand the threats, the chapter has also developed tactical threat intelligence on these threats. Based on this intelligence, a mitigating framework has been developed to help organizations deal with them. Again, the issue of user awareness has been brought to light just to emphasize its importance when dealing with social media threats. Finally, the chapter ends by explaining how a user can recover from unfortunate events where social media threats prevail.

7.3 Recommendations

7.3.1 Users

To begin with, users have to be careful with the sensitivity of the data they post on social media and the amount of information that is visible to others. Some users are victims of their own calamities, whereby they have posted sensitive data on social media thus encouraging malicious persons to exploit their “honesty.” Other than their honesty being exploited, posting some comments or pictures on social media might cost one his/her reputation and even a job. It is estimated that 70% of recruiters do background checks on

one's social media account and reject a candidate based on his/her posts. Some of the data that users should be wary of when sharing online include the names of their banks, workplaces, frequently visited locations, and their homes. This makes it easy for a stalker to follow up on one's every move. Stalking could be made harder if people did not reveal where they were at all times on social media. Unfortunately, users want others to see where they live, work, eat, and spend most of their time. It is safe to assume that there is always someone with malicious intentions actively collecting the data that one posts on his/her social media accounts.

Social media platforms provide a few privacy settings that can enable one to alter his/her visibility online. Some platforms will allow a user to block off everyone except their friends from being able to view what they post. Facebook was found by several researches to be the platform faced by most privacy issues. That is why the platform includes 101 privacy settings to help users protect their account and information. It is good for users to be wary of strangers who try to message them asking for some favors. It is upon users to learn how to use these privacy settings; they have been put there for a reason. The best recommendation as concerns this is to make a social media account not visible to people other than friends and family whenever possible. Almost all social media platforms support this and it could be the setting that keeps stalkers, hackers, and social engineers at bay. Unfortunately, these settings are not designed to prevent the social media companies from collecting one's data in the background. The advantage is that even if they collect one's data, they will not follow up a certain person to rob them off or rob him/her when not at home.

It is advisable for users to enable two-factor authentication into their accounts whenever possible. This will go a long way into stopping hackers who might get hold of one's password. A two-step authentication is basically a multi-factor verification whereby one is authenticated into his/her account after two checks have confirmed the legitimacy of

his/her identity (Oder, 2008). One of the factors is obviously the password but the second factor could be a code or pass that is sent via SMS or email. The second layer of authentication makes it harder for a hacker or someone who has stolen credentials from getting through the login process. They might have the correct username and password but since they do not have the second code, they cannot log into an account. This has stopped many hacking attempts, fraud, data theft, and identity theft. Most social media accounts have support for this multiple factor authentication, and it is just a matter of one activating it.

Users should be wary of third party applications within and out of social media platforms. These apps are reportedly able to access one's list of friends, entire account information of users, posts, and even private messages. These third-party applications are used to do various functionalities based on the platform. For Twitter, they are used to easily unfollow people who do not follow back and some claim to help users get more followers. In Facebook, they are used to send birthday wishes, record people that look at one's profile, and some have some useless functionalities. When one connects to them, it has been found out that they are given more than necessary access to one's data. Facebook is said to give them almost an entire access to one's account. Compared to what they do, it is not worth it to let them access this kind of data. They could be masquerading as apps to help one catch by surprise stalkers, but in the background, they could be exporting his/her messages and posts to their websites. This is information that could be used for malicious purposes. Social media platforms do come with settings for one to remove these apps. Users are strongly advised to remove them so as to protect their accounts.

Lastly, it never hurts for users to change their passwords regularly. Changing passwords is effective at ensuring that, even if one's password is stolen, the malicious person will have a small window of opportunity to use it. It is surprisingly easy to steal passwords, especially when users are willing "free" premium software. Free software, especially when

downloaded from torrent sites, comes with many malicious programs and codes. This is normally the cost of using the illegally downloaded software. They come full of keystroke loggers, ransomware, and some malware used to steal passwords saved on browsers. This is yet another important point; users should not save their passwords on their browsers. It is better to use a password manager software. There are many tools that can be used to copy all the saved passwords in a computer. One of the easiest tools runs from a USB flash disk, and all a malicious person needs to do is plug it into the victim's computer. Users should also never reuse the same passwords for each of social media platforms. This makes it hard for a malicious person that has been able to hack into one account to be able to hack another. Hackers know that users are lazy, and they will, therefore, tend to repeat the same passwords for all the social media platforms they use. Easy-to-guess passwords or information that can easily be found out such as birthday dates should also never be used.

7.3.2 Social media platforms

To begin with, social media platforms should put in place settings that can enable users to limit the amount of data that third-party applications can access. Social media platforms just give automatically ticked options of what these apps can access. Not only are these options non-extensive on the amount of data the apps can access, there is no choice of opting out of some options. It would be good if users are given a say such that they can prevent these apps from reading some type of information from their accounts. Surprisingly, these apps can still function without some of the data that they are given such as access to one's messages. It is rather unfortunate when a Facebook third party app used to post happy birthday messages on friends' timelines are allowed to read off messages. They simply have no business with messages yet Facebook has given them access to read them. This is a major privacy flaw. This is why it is upon the likes of Facebook to give users the ability to deny these apps access to some data.

Social media platforms ought to respect their users' privacy. They must, therefore, stop collecting and selling off their user's personal data. There have been several allegations that some social media platforms, such as Facebook collect, profile, and sell off user data to third parties. This is done without obtaining consent from users. Facebook has solely been accused of going overboard and collecting additional user data without informing the users. It was accused of collecting faceprints of users with the intention of being able to automatically tag them in pictures (Roberts, 2015). Users were not informed about this sort of collection. What Facebook did, a common trick used by social media companies, was to add a clause in its privacy statement allowing it to collect the faceprints. This was absurd since it was not among the terms that users agreed to when signing up for a Facebook account. This amounted to a total disrespect of user's privacy. Again, Facebook pushed an update to WhatsApp after it acquired it that forced it to share its user data with Facebook servers. Users were again not notified and the update was made mandatory. Another great disrespect to the privacy of users. This has to come to a stop; social media platforms must accord their users the respect that they deserve. At the end of the day, it is the users that generate content that brings other users on the platforms. This, in turn, makes a platform grow and be able to leverage its user base for money via advertising. It is disheartening when a social media company is taken to court over illegally collecting some data, illegally sharing out some data, or not seeking user consent for some operations. These platforms play a cat and mouse game with existing laws, whereby they find tiny holes to justify clearly illegal practices. This is aimed mostly at Facebook; it has been found guilty of heinous crimes concerning collection and sharing of user data.

In addition, these platforms need to come up with ways to educate users on how to change their privacy settings. There have been claims raised by some users that the process is a bit complex and filled with uncertainties, especially for new users. There are undoubtedly

some difficulties in the management of privacy controls that have been given by social media platforms (Madden et al., 2013). They have been termed as poor interfaces when compared to the human-centered design principles (Liu et al., 2011). Controls that ought to be easily accessible have been found hidden under sub-menus of other menus. Sometimes, these controls do not have an explanation of what they prevent against. Users are left to learn all these on their own. It is a punishment that one has to endure in order to change privacy settings. Social media networks are instead supposed to make the process of managing privacy controls easy and make the users knowledgeable of it. It is advisable that during sign up, a user should be taken through the available controls, what they do, and what one can do to access and adjust them. Currently, users are hardly told that these controls even exist and new users really suffer before they are familiar with the controls.

Lastly, social media accounts should make it possible for users to delete their accounts permanently. Some platforms, such as Facebook only allow a user to deactivate his/her account. Deactivation is not the same as delete since data about that profile is still accessible. Deleting should allow a user to completely wipe off his/her data from a social media platform. As users age and privacy issues become more, they are opting to just get out of the social media platforms once and for all. It seems that social media platforms see that this is bad for business, and thus they only allow a user to deactivate his account so that they can still boast of having a big user base. Very few platforms such as LinkedIn are willing to allow a user delete an account. This is the last form of defense that users have when it comes to their privacy, and they should be allowed to use it. Therefore, there should be an easy-to-access control that all users have to be notified of that can enable them to delete their accounts on social media.

7.3.3 Governments

Governments ought to come up with strict regulations to protect user privacy. A good trendsetter is the European Union, which is vocal concerning the collection and sharing of the data of users in the region. The EU was quick to react to Facebook's addition of a certain setting in their newly acquired platform, WhatsApp. The setting that came auto enabled made WhatsApp send back user data to Facebook. The EU protects the privacy of the data of users in its region. However, outside the EU, everything changes. Entire governments seem to be unconcerned about the suffering of their citizens on social media platforms. Governments sit back and watch as the data of their citizens is sold off without their consent. It is the responsibility of any government to protect its citizens. Therefore, they should protect them from the dangers they face when they are online. One of these dangers is the infringement of their privacy by social media companies. Governments need to follow the example of the EU and put in place very strict regulations designed to discourage social media platforms from unethically collecting and using the data of their citizens. Key changes to EU regulations on user data have been provided in appendix B of this document.

Governments have the power to call for a total ban of a platform that does not abide by its data privacy rules in their countries. Shutting of some social media platforms is possible and has already been demonstrated in countries such as China and Iran (Papic and Noonan, 2011). This is very effective since a significant loss of revenues is felt by the social media platforms. If the governments in an entire region decide to ban any social media platform that does not play by the rules, it is guaranteed that the platform will willingly or unwillingly have to play by the rules. A total ban from an entire region would mean that the revenues received from advertisers in that region are lost and also the reputation of the platform becomes soiled. Governments can also call for the removal of some clauses on social media privacy policies that degrade the capabilities of users in securing their data. It

should not be up to someone in Facebook to wake up and think about what to add or remove from privacy policies. The government should intervene in situations such as these and call for the removal of such additions. Governments should also introduce severe punishments and fines to platforms that violate users' privacy. Current fines and punishments seem to be too lenient and these platforms can simply break rules because they can afford to pay the fines. Social media platforms simply do a calculation of the expected fine against what they stand to gain from a particular violation. If they have a lot to gain from a violation, they do it and just pay the fine. Fines should be so high such that these platforms cannot dare to violate some rights.

Lastly, governments ought to work in collaboration with users to ensure that identity thieves, spammers, scammers, and social engineers are apprehended and their accounts are permanently shut down. It is easy to do this as users can be told to report such people to a government account. Currently, users only have the option of reporting such people to the social media companies. Robots put in place by the companies determine whether or not to block the reported account. If there was an option to report such an issue to the government, the culprit would be followed up and put behind bars. This would make social media platforms safer.

7.4 Future Research Directions

This research tried to extensively cover the existing privacy and security threats in social media. It went on to look at other existing works of literature on the topic and tried to add more knowledge to the topic. This had been outlined by the previous researchers in their works. The research would, therefore, like to lay out some areas that future researchers can dig deeper into and probably bring a ton of more knowledge to the topic. One of the things that future researchers should look at are the legislations that governments should lay out to

protect user data and how they can cooperate as unions to ensure that there is privacy. Secondly, future researchers should examine the specific third-party apps that are extensively collecting user data. The researchers should look at the exact ways these apps collect, store, and use the data that they collect and how they can be limited in terms of what they can access. Thirdly, future researches should look at how social media platforms and governments can collaborate to curb social media crimes. These crimes are on the rise and someone ought to research on how they can be ended. Lastly, future researchers should aim at exploring different world regions when it comes to collecting primary data. The data that was sampled cannot be said to depict the opinions of all the types of users as it was collected from a rather limited demography.

7.5 Limitations of this research

The greatest limitation to this research was the data used. This research utilized data from both primary and secondary sources. First of all, from the questionnaires sent to respondents, it is worrying that some respondents may have given untrue data. This is because the questionnaire was online, was long, and there was no type of monetary compensation given to the respondents. From the secondary data used, it is also feared that some of the data may have been biased or modified by the original researcher to suit his/her intentions.

The second limitation was the budget and time constraints. The research was done within a fixed budget and schedule, and there were some delays experienced especially in receiving feedback from the respondents. The questionnaire was online and the users had the freedom to fill them at their comfort in terms of time. There was also the challenge of having to do many other things apart from research and as such balancing between school work and another occupation. Therefore, the time to do this research was considerably little but the

most was made out of the opportunities available. Secondly, due to monetary constraints, the data analysis was not done using premium tools, and thus some substantial findings and patterns may not have been identified. The primary data collection tool was an online questionnaire to make the costs even less for conducting the research.

The third limitation to this research was the sample selected. It was actually hard to find respondents who were willing to take this 20-30 minute questionnaire online. Only volunteers were given the link to fill the questions. Also, not all the volunteers filled and submitted back their responses to the questionnaires. However, even with all this, a significant number of responses were received and they were just enough for meaningful findings and patterns to be drawn from them.

The last limitation encountered by this research was self-reporting. It is rather hard for one to present the arguments about a certain problem objectively. It might seem an easy thing to do but the mind slowly starts becoming more biased as more and more information is available and new discoveries are made. Therefore, it was quite a challenge even though biasedness was avoided for the major part of the research.

References

Alalawi, N. (2015). Social Networks and Privacy. Management Science and Engineering, 9(4), 46-55.

Albrecht, C., Albrecht, C., & Tzafrir, S. (2011). How to protect and minimize consumer risk to identity theft. Journal of Financial Crime, 18(4), 405-414. http://dx.doi.org/10.1108/13590791111173722

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of facebook. European Journal of Information Systems, 26(6), 661-687. http://dx.doi.org/10.1057/s41303-017-0057-y

Alkhalisi, Z. (2018). IRS scam alleged ringleader arrested in India. CNNMoney. Retrieved 15 February 2018, from http://money.cnn.com/2017/04/09/news/tax-scam-india-arrest-ringleader/index.html

Bakhshi, T., Papadaki, M., & Furnell, S. (2009). Social engineering: Assessing vulnerabilities in practice. Information Management & Computer Security, 17(1), 53-63. http://dx.doi.org/10.1108/09685220910944768

Bamberger, K. A., & Mulligan, D. K. (2010). Privacy on the Books and on the Ground. Stan. L. Rev., 63, 247.

Bonanno, R. A., & Hymel, S. (2013). Cyber bullying and internalizing difficulties: Above and beyond the impact of traditional forms of bullying. Journal of Youth and Adolescence, 42(5), 685-97. doi:http://dx.doi.org/10.1007/s10964-013-9937-1

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of experimental criminology, 11(1), 97-115.

Burgess, M., Canright, G., & Engø-Monsen, K. (2004). A graph-theoretical model of computer security. International Journal of Information Security, 3(2), 70-85. http://dx.doi.org/10.1007/s10207-004-0044-x

Cao, J., Li, Q., Ji, Y., He, Y., & Guo, D. (2016). Detection of forwarding-based malicious URLs in online social networks. International Journal of Parallel Programming, 44(1), 163-180. http://dx.doi.org/10.1007/s10766-014-0330-9

Castelluccio, M. (2002). Social engineering 101. Strategic Finance, 84(6), 57-58. Retrieved 11 February 2018, from https://search.proquest.com/docview/229746623.

Drake, J. R. (2016). Asking for facebook logins: An egoist case for privacy. *Journal of Business Ethics, 139*(3), 429-441. http://dx.doi.org/10.1007/s10551-015-2586-4

Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. Computers & Security, 69, 18. Retrieved 17 February 2018, from https://search.proquest.com/docview/1942191702.

Employee Training is the Only Way to Prevent Social Engineering. (2018). BAI Security. Retrieved 8 March 2018, from http://www.baisecurity.net/2017/04/employee-training-is-the-only-way-to-prevent-social-engineering/

Endicott-Popovsky, B., & Lockwood, D. L. (2006). A SOCIAL ENGINEERING PROJECT IN A COMPUTER SECURITY COURSE. Academy of Information and Management Sciences Journal, 9(1), 37-44. Retrieved 7 January 2018, from https://search.proquest.com/docview/214628148.

Gan, D., & Jenkins, L. R. (2015). Social networking privacy-who's stalking you?dagger]. Future Internet, 7(1), 67-93. http://dx.doi.org/10.3390/fi7010067

Goldman, D. (2018). Hackers siphon $47 million out of tech company's accounts. CNNMoney. Retrieved 15 February 2018, from http://money.cnn.com/2015/08/10/technology/ubiquiti-hacked/index.html

Gordhamer, S. (2018). 5 Ways Social Media is Changing Our Daily Lives. Mashable. Retrieved 8 March 2018, from https://mashable.com/2009/10/16/social-media-changing-lives/#B_2H3faDGOqT

Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Retrieved 14 January 2017 from https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

Greavu-Serban, V., & Serban, O. (2014). Social engineering a general approach. Informatica Economica, 18(2), 5-14. Retrieved 9 February 2018, from https://search.proquest.com/docview/1547694667.

Greenberg, A. (2018). The Ransomware Hackers Made Some Real Amateur Mistakes. WIRED. Retrieved 15 February 2018, from https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/

Hammer, B. (2013). The mechanisms of interpersonal privacy in social networking websites: A study of subconscious processes, social network analysis, and fear of social exclusion. University of Arkansas.

Harris, S., Seetharaman, D., & Tau, B. (2017, Sep 06). Facebook identifies $100,000 in ad spending by fake accounts with suspected ties to russia; accounts shared 'divisive social and political messages,' social network says. Wall Street Journal (Online) Retrieved 1 March 2018, from https://search.proquest.com/docview/1935980831.

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails. Online Information Review, 40(2), 265-281. Retrieved 15 February 2018, from https://search.proquest.com/docview/1776786039.

Heartfield, R., & Loukas, G. (2016). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Computing Surveys (CSUR), 48(3), 37.

Heyman, R., De Wolf, R., & Pierson, J. (2014). Evaluating social media privacy settings for personal and advertising purposes. The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 16(4), 18. Retrieved 19 February 2018, from http://search.proquest.com/docview/1660153046

Ivaturi, K., & Janczewski, L. (2013). Social engineering preparedness of online banks: An asia-pacific perspective. Journal of Global Information Technology Management, 16(4), 21-46. Retrieved 15 February 2018, from https://search.proquest.com/docview/1461726484.

Kerkstra, G. (2005). Protecting transaction data. Chain Store Age, 81(6), 100. Retrieved 15 February 2018, from https://search.proquest.com/docview/222086812.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. Information Management & Computer Security, 22(1), 115-126. http://dx.doi.org/10.1108/IMCS-01-2013-0005

Krishnamurthy, B., & Wills, C. E. (2009, August). On the leakage of personally identifiable information via online social networks. In Proceedings of the 2nd ACM workshop on Online social networks (pp. 7-12). ACM.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

Krombholz, K., Merkl, D., & Weippl, E. (2012). Fake identities in social media: A case study on the sustainability of the facebook business model. Journal of Service Science Research, 4(2), 175-212. doi:http://dx.doi.org/10.1007/s12927-012-0008-z

Larson, S. (2018). *Facebook's new security settings speak a simple language*. *CNNMoney*. Retrieved 21 February 2018, from http://money.cnn.com/2017/05/31/technology/facebook-new-security-settings-page/index.html

Lior, J. S. (2005). A social networks theory of privacy. The University of Chicago Law Review, 72(3), 919-988. Retrieved 23 February 2018, from https://search.proquest.com/docview/214807827

Liptak, A. (2018). The WannaCry ransomware attack has spread to 150 countries. The Verge. Retrieved 14 February 2018, from https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011, November). Analyzing facebook privacy settings: user expectations vs. reality. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference (pp. 61-70). ACM.

Locklear, M. (2018). *Facebook clarifies its security settings to curb confusion*. *Engadget*. Retrieved 21 February 2018, from https://www.engadget.com/2017/05/31/facebook-clarifies-security-settings/

Loeffler, C. (2012). Privacy issues in social media. The IP Litigator : Devoted to Intellectual Property Litigation and Enforcement, 18(5), 12-18. Retrieved 1 February 2018, from http://search.proquest.com/docview/1082016549.

Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. Information Resources Management

Journal, 24(3), 1. Retrieved 5 January 2018, from https://search.proquest.com/docview/892604242.

Madden, M. (2016). Public Perceptions of Privacy and Security in the Post-Snowden Era. Pew Research Center: Internet, Science & Tech. Retrieved 3 November 2016, from http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media, and privacy. Pew Research Center, 21, 2-86.

Magno, G., Comarela, G., Saez-Trumper, D., Cha, M., & Almeida, V. (2012, November). New kid on the block: Exploring the google+ social graph. In Proceedings of the 2012 ACM conference on Internet measurement conference (pp. 159-170). ACM.

Malik, A., Hiekkanen, K., Dhir, A., & Nieminen, M. (2016). Impact of privacy, trust and user activity on intentions to share facebook photos. Journal of Information, Communication & Ethics in Society, 14(4), 364-382. Retrieved 13 December 2017, from https://search.proquest.com/docview/1844292056.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics*, *137*(3), 551-569. http://dx.doi.org/10.1007/s10551-015-2565-9

Milne, G. R., & Culnan, M. J. (2004). Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. Journal of Interactive Marketing, 18(3), 15-29.

Mital, M., & Sarkar, S. (2011). Multihoming behavior of users in social networking web sites: A theoretical model. Information Technology & People, 24(4), 378-392. http://dx.doi.org/10.1108/09593841111182250

Mouton, Francois & Leenen, Louise & Venter, H.s. (2016). Social engineering attack examples, templates and scenarios. Computers & Security. 59. 186 - 209. 10.1016/j.cose.2016.03.004.

Mouton, F., Malan, M. M., Kimppa, K. K., & Venter, H. S. (2015). Necessity for ethics in social engineering research. Computers & Security, 55, 114. Retrieved 25 February 2018, from https://search.proquest.com/docview/1733195513.

Musthaler, L. (2006). How social engineering sinks security. Network World, 23(39), 45. Retrieved from https://search.proquest.com/docview/215993673.

Nemati, H., Wall, J. D., & Chow, A. (2014). Privacy coping and information-sharing behaviors in social media: A comparison of chinese and U.S. users. Journal of Global Information Technology Management, 17(4), 228-249. Retrieved 28 February 2018, from http://search.proquest.com/docview/1674426345

Oder, U. T. (2008). Two-factor authentication. Hoboken, NJ: John Wiley and Sons.

Papic, M., & Noonan, S. (2011). Social media as a tool for protest. Retrieved 15 February 2018, from https://www.stratfor.com/weekly/20110202-social-media-tool-protest

Parker, D. (2002, Dec 16). A fraudster's tricks of the trade: BOOK REVIEW THE ART OF DECEPTION: An ex-con reveals how clever manipulation can make employees the weakest link in a company's security, writes D: Financial Times Retrieved 3 March 2018, from https://search.proquest.com/docview/249487841.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. Information Systems Security, 15(5), 13-21.

Perri, F. S., & Brody, R. G. (2012). The optics of fraud: Affiliations that enhance offender credibility. Journal of Financial Crime, 19(4), 355-370. http://dx.doi.org/10.1108/13590791211266359

Roberts, J. J. (2015). Who owns your face? Weak laws give power to Facebook. Retrieved 15 September 2016, from http://fortune.com/2015/06/17/facebook-moments-privacy-facial-recognition/

Robertson, S. (2018). Digital ‘totalitarian marketing’ threatens privacy and security, former advertising executive says. The Globe and Mail. Retrieved 24 February 2018, from https://www.theglobeandmail.com/report-on-business/industry-news/marketing/digital-totalitarian-marketing-threatens-privacy-and-security/article37009003/

Russell, R., & Stutz, M. (2014). SOCIAL MEDIA: WHAT EMPLOYERS NEED TO KNOW. Journal of Internet Law, 17(8), 3-6. Retrieved 25 February 2018, from https://search.proquest.com/docview/1501615784.

Sableman, M. (2017). Social media privacy: It's a reasonable expectations game. *Copyright & New Media Law Newsletter, 20*(4), 5-7. Retrieved 27 February 2018, from https://search.proquest.com/docview/1852966940.

Savage, M. (2003). Former hacker mitnick details the threat of 'social engineering'. Crn, (1043), 58. Retrieved 8 March 2018, from https://search.proquest.com/docview/227563346.

Sayers, G. G. (2005). Take steps to reduce risks of data theft. Business Insurance, 39(28), 9. Retrieved 6 February 2018, from https://search.proquest.com/docview/233518484.

Schaab, P., Beckers, K., & Pape, S. (2017). Social engineering defence mechanisms and counteracting training strategies. Information and Computer Security, 25(2), 206-222. Retrieved 9 January 2018, from https://search.proquest.com/docview/1908738518.

Schwartz, M. J. (2012). Facebook social engineering attack strikes NATO. Informationweek - Online, Retrieved 15 February 2018, from https://search.proquest.com/docview/927676612.

Seda, L. (2014). Identity theft and university students: Do they know, do they care? Journal of Financial Crime, 21(4), 461-483. Retrieved 14 February 2018, from https://search.proquest.com/docview/1660751510.

Shane, S., Perlroth, N., & Sanger, D. (2018). Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core. Nytimes.com. Retrieved 14 February 2018, from https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html

Sisk, M. (2008). Social engineering: Plugging the holes in human firewalls ; the intense school's one-week e-course helps banks make sure staffers are following security procedures. Bank Technology News, 17(6), 46. Retrieved 13 January 2018, from https://search.proquest.com/docview/208140513.

Snyder, C. (2015). Handling human hacking: creating a comprehensive defensive strategy against modern social engineering.

Storm, D. (2018). 17 exploits the NSA uses to hack PCs, routers and servers for surveillance. Computerworld. Retrieved 14 February 2018, from https://www.computerworld.com/article/2474275/cybercrime-hacking/17-exploits-the-nsa-uses-to-hack-pcs--routers-and-servers-for-surveillance.html

Talmadge, E. (2018). North Korea announces blocks on Facebook, Twitter and YouTube. the Guardian. Retrieved 21 February 2018, from https://www.theguardian.com/world/2016/apr/01/north-korea-announces-blocks-on-facebook-twitter-and-youtube

Tannam, E. (2018). *EU warns Facebook, Google and Twitter that they must respect consumer rules*. *Silicon Republic*. Retrieved 21 February 2018, from https://www.siliconrepublic.com/companies/facebook-google-twitter-consumer-eu

Tarnoff, B. (2018). How the internet was invented. the Guardian. Retrieved 8 March 2018, from https://www.theguardian.com/technology/2016/jul/15/how-the-internet-was-invented-1976-arpa-kahn-cerf

Thompson, S. T. C. (2006). Helping the hacker? library information, security, and social engineering. Information Technology and Libraries, 25(4), 222-225. Retrieved 5 February 2018, from https://search.proquest.com/docview/215828364.

W32.Koobface | Symantec. (2018). Symantec.com. Retrieved 15 February 2018, from https://www.symantec.com/security_response/writeup.jsp%3Fdocid%3D2008-080315-0217-99

Workman, M. (2008). A test of interventions for security threats from social engineering. Information Management & Computer Security, 16(5), 463-483. http://dx.doi.org/10.1108/09685220810920549

Young, R., Zhang, L., & Prybutok, V. R. (2007). Hacking into the minds of hackers. Information Systems Management, 24(4), 281-287. Retrieved 15 February 2018, from https://search.proquest.com/docview/214129274.

Appendix A: Results of the interview

1. What is your age bracket?					
18-23				46.00%	
24-28				30.00%	
29-33				10.00%	
34-39				9.00%	
40-45				5.00%	
2. What is your level of education?					
Undergraduate and below				60.00%	
Master's degree				25.00%	
PhD				15.00%	
3. What is your computer literacy level?					
Beginner				45.00%	
Professional				50.00%	
Amateur				5.00%	
4. What is your gender?					
Male				59.00%	
Female				50.00%	
Other				1.00%	
5. Of the given platforms below, which is your most favourite social media platform?					
Facebook				5	
Twitter				1	
Instagram				2	
LinkedIn				3	
Snapchat				4	
Google Plus				6	
6. Which of these is your least favourite platform?					
Facebook				1	
LinkedIn				3	

Google Plus				2	
7. Which of these do you think has most privacy issues?					
Facebook				1	
Twitter				3	
Instagram				4	
LinkedIn				2	
Snapchat				5	
8. Have you encountered any privacy issues on social media?					
Yes				99.00%	
No				1.00%	
9. Do you think stalking can be minimized with proper controls					
Yes				80.00%	
No				20.00%	
10. Do you think bullying is happening in Social Media					
Yes				30.00%	
No				70.00%	
11. Do you use your real names on social media?					
Yes				40.00%	
No				60.00%	
12. Could you live without any social media account?					

Yes				25.00%	
No				75.00%	
13. How often do you post on social media?					
Daily				55.00%	
Weekly				30.00%	
Every fortnight				15.00%	
Monthly				5.00%	
Rarely					
14. How many friends do you have on Facebook					
1-100				10.00%	
100-500				74.00%	
500-1000				9.00%	
Over 1000				7.00%	
15. What is your privacy setting for your Facebook account?					
Private				30.00%	
Only friends can view				36.00%	
Public				34.00%	
16. Have you allowed any third party applications to access your social media account?					
Yes				85.00%	
No				15.00%	
17. What is your experience with social media platforms in terms of connecting with people					
Excellent				70.00%	
Good				25.00%	
Bad				3.00%	
Awful				2.00%	
18. Have you shared the following on your social media platforms?					
Your photo				92.00%	

Your school				69.00%	
Your location				72.00%	
Your email address				63.00%	
Your phone number				30.00%	
Your birth date				80.00%	
Your relationship status				60.00%	
Your interests and hobbies				80.00%	
19. How many followers do you have on Twitter					
Less than 100				10.00%	
100 – 500				64.00%	
500 – 2500				24.00%	
Over 2500				16.00%	
20. Are your tweets private or public					
Private				60.00%	
Public				30.00%	
Not sure				10.00%	
21. Have you ever deleted content you posted on social media?					
Yes				88.00%	
No				12.00%	
22. Have you ever blocked another user on social media?					
Yes				95.00%	
No				5.00%	
Facebook					
23. Have you ever read the Facebook					

privacy policy? Why?					
Yes				25.00%	
No				75.00%	
				The leading reason for those who read was due to allegations that Facebook was collecting their information without their knowledge. Those that did not read said that the policy was too long.	
24. Have you ever changed your privacy settings?					
Yes				24.00%	
No				76.00%	
			25. How did you find the process of changing your privacy settings		
Easy				30.00%	
Hard				50.00%	
Complicated at first				20.00%	
26. Have you ever received spam messages or tagged involuntarily on a post made by a stranger?					
Yes				90.00%	
No				10.00%	
27. Have you ever reported a user or a post?					
Yes				92.00%	
No				8.00%	
28. Are you concerned about your privacy on Facebook?					
Yes				97.00%	
No				3.00%	
30. What are your privacy concerns on Facebook					

Account is insecure				3	
Third party applications can access private account information				2	
Facebook gives out account information to third parties				1	
Twitter					
31. Have you read the privacy policy of Twitter? Why?					
Yes				15.00%	
No				85.00%	
				Those that read claimed that they wanted to know more about the information that Twitter collects. Those that did not read say that it was long and they did not have time for it.	
32. Have you changed your privacy settings of Twitter?					
Yes				8.00%	
No				92.00%	
33. Have you faced any security or privacy issues on Twitter					
Yes				1.00%	
No				99.00%	
34. If yes, which ones?					
				The respondents claimed that they were sent spam messages.	
35. Do you find Twitter ads					

intrusive?					
Yes				1.00%	
No				99.00%	
36. Do you think Twitter has protected your private data adequately?					
Yes				75.00%	
No				25.00%	
WhatsApp					
37. Do you use WhatsApp?					
Yes				95.00%	
No				5.00%	
38. Between WhatsApp and Facebook Messenger, which one is more secure?					
WhatsApp				1	
Facebook Messenger				2.00%	
39. Are you aware of Facebook fetching user data from WhatsApp?					
Yes				85.00%	
No				15.00%	
40. Have you changed the setting that allows Facebook to collect your private data from WhatsApp?					
Yes				85.00%	
No				15.00%	
41. Do you think that Facebook's acquisition of WhatsApp means that might be violations on the future?					
Yes				90.00%	
No				10.00%	
42. Are WhatsApp privacy settings easy to access?					

Yes				45.00%	
No				55.00%	
LinkedIn					
43. Do you have an account with LinkedIn?					
Yes				87.00%	
No				13.00%	
44. Are you annoyed by LinkedIn notifications?					
Yes				96.00%	
No				4.00%	
45. Do you feel that LinkedIn is too nosy with user information?					
Yes				96.00%	
No				4.00%	
46. Have you shared your main email address with LinkedIn?					
Yes				80.00%	
No				20.00%	
47. If yes, do you feel that LinkedIn is too much intrusive into your email address?					
Yes				99.00%	
No				1.00%	
48. Are LinkedIn's privacy settings easy to change?					
Yes				30.00%	
No				70.00%	
Google Plus					
49. Are you					

signed up on Google Plus?					
Yes				65.00%	
NO				35.00%	
50. When was the last time that you posted on Google Plus?					
Less than a week ago				4.00%	
Less than a month ago				6.00%	
Less than 6 months ago				25.00%	
Less than a year ago				30.00%	
Never				35.00%	
51. Have you ever read the Google Plus terms and conditions?					
Yes				23.00%	
No				77.00%	
52. Have you ever changed your privacy settings on Google Plus?					
Yes				1.00%	
No				99.00%	
53. If yes, is it easy for one to access and change the privacy settings?					
Yes				10.00%	
No				90.00%	
Skype					
54. Are you an active user on Skype?					
Yes				70.00%	
No				30.00%	
55. Are you aware of claims that Skype gave access to user data to intelligence agencies?					
Yes				60.00%	
No				40.00%	

56. Are you aware of claims that Skype calls could be intercepted by third parties?					
Yes				60.00%	
No				40.00%	
57. With all these claims, can you trust to communicate sensitive information over Skype?					
Yes				38.00%	
NO				62.00%	
Instagram					
58. Do you have an active account on Instagram?					
Yes				70.00%	
No				30.00%	
59. Do you think that Instagram should take ownership of your personal photos once you upload them?					
Yes				5.00%	
No				95.00%	
60. Is your Instagram account public or private?					
Public				85.00%	
Private				15.00%	
61. How accessible are privacy settings on Instagram?					
Easy to access				20.00%	
Fairly accessible				55.00%	
Difficult to access and change				25.00%	
General					
62. Are you concerned about the data mining interests of social media platforms on their users?					
Yes				98.00%	
No				2.00%	

63. Do you think that social media platforms have not done enough to protect their users' data?					
Yes				99.00%	
No				1.00%	
64. Do you think that Facebook has become too aggressive and intrusive on its users?					
Yes				90.00%	
No				10.00%	
65. Do you believe that most social media platforms are violating their users' privacy rights?					
Yes				97.00%	
No				3.00%	
66. Do you believe that social media platforms are using deceptive tactics to get users to give up the ownership of their data?					
Yes				90.00%	
No				10.00%	
67. Do you believe that social media platforms such as Facebook have poor customer support?					
Yes				98.00%	
No				2.00%	
68. Do you believe claims that social media platforms have been selling off user data to third parties?					
Yes				99.00%	
No				1.00%	
69. Do you believe that social media platforms have been letting third party applications access too much user data?					
Yes				99.00%	
No				1.00%	
70. Do you believe that governments are doing enough to protect their user data?					
Yes				25.00%	
No				75.00%	
71. Do you believe that advertising services have been the major cause of privacy violations?					
Yes				97.00%	
No				3.00%	

72. Do you believe that social media platforms should be subjected to tough privacy laws?					
Yes				90.00%	
No				10.00%	
73. Have social media platforms been actively seeking for user consent before using/collecting/selling their data?					
Yes				1.00%	
No				99.00%	
74. Should all social media platforms allow their users to have an option of deleting their accounts?					
Yes				98.00%	
No				2.00%	
75. Are you satisfied with the accessibility of privacy settings that social media platforms give?					
Yes				17.00%	
No				83.00%	
76. Do you think that these privacy settings availed by users control all the privacy aspects of their data?					
Yes				0.00%	
No				100.00 %	
77. Have the fines and punishments imposed on some social media platforms been adequate? Why?					
Yes				0.00%	
No				100.00 %	Respondents said that these platforms were not heavily affected by the punishments/fines since their profits were enormous.
78. Do you wish that some governments would sensor some social media platforms?					
Yes				45%	
No				55%	
79. Can you voluntarily terminate all your social media accounts?					
Yes				0.00%	
No				100.00 %	
80. Do you wish that you were in a position to terminate all your					

social media accounts?					
Yes				100.00 %	
No				0.00%	

Appendix B: EU GDPR Changes

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

Increased Territorial Scope (extra-territorial applicability)
Arguably the biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the Union, regardless of the company's location. Previously, territorial applicability of the directive was ambiguous and referred to data process 'in context of an establishment'. This topic has arisen in a number of high profile court cases. GDPR makes its applicability very clear - it will apply to the processing of personal data by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU. Non-Eu businesses processing the data of EU citizens will also have to appoint a representative in the EU.

Penalties
Under GDPR organizations in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements e.g.not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement.

Consent
The conditions for consent have been strengthened, and companies will no longer be able to use long illegible terms and conditions full of legalese, as the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Data Subject Rights

Breach Notification

Under the GDPR, breach notification will become mandatory in all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access

Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to data transparency and empowerment of data subjects.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17, include the data no longer being relevant to original purposes for processing, or a data subjects withdrawing consent. It should also be noted that this right requires controllers to compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

Data Portability

GDPR introduces data portability - the right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.

Privacy by Design

Privacy by design as a concept has existed for years now, but it is only just becoming part of a legal requirement with the GDPR. At its core, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition. More specifically - 'The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects'. Article 23 calls for controllers to hold and process only the data absolutely necessary for the completion of its duties (data minimisation), as well as limiting the access to personal data to those needing to act out the processing.

Data Protection Officers

Currently, controllers are required to notify their data processing activities with local DPAs, which, for multinationals, can be a bureaucratic nightmare with most Member States having different notification requirements. Under GDPR it will not be necessary to submit notifications / registrations to each local DPA of data processing activities, nor will it be a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs). Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences. Importantly, the DPO:

Must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices
May be a staff member or an external service provider
Contact details must be provided to the relevant DPA
Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
Must report directly to the highest level of management
Must not carry out any other tasks that could results in a conflict of interest.

All changes can be accessed here.

List of Publications from the Thesis

Papers

1) Privacy issues in Social Media, ATCS Conference (2017)
2) The use of Social Media for terrorism (Social Media issues), NATO Defense Against Terrorism Review (2017)
3) Privacy Issues in Social Media -Fake News and SM, CSU HDR Symposium 2017
4) Cybersecurity: Privacy issues in Social Media, CSU CSS Symposium (2017)

Books

1) Title: Cybersecurity Attack and Defense Strategies, Erdal Ozkaya, Yuri Diogenes, Publisher: Packt Publishing, 2018, ISBN 978-1-78847-529-7
   Packt Publishing
2) Title: Learning Social Engineering, Erdal Ozkaya, Publisher: Packt publishing, 2018,
3) Title: Hands on Cyber Security for Finance Publisher: Packt publishing, 2019
4) Title: The Dark Web, Erdal Ozkaya, Publisher: Packt Publishing, 2019
5) Title: Incident Response: Fundamentals of Cybersecurity, Erdal Ozkaya, Publisher: Packt Publishing, 2019, I

3 certifications approved by ANSI

1) Cybersecurity First Responder Certification (US DoD 7570 complaint, ANSI approved)
   http://logicaloperations.com/certifications/1/CyberSec-First-Responder/

2) Cybersecurity Certification via Logical Operations
   To be released