THE MANAGEMENT OF SECURITY AND PRIVACY CONCERNS BY SMART PHONE AND SOCIAL MEDIA USERS IN UNIVERSITY OF NAIROBI

GATHUA MERCY NYOKABI

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE AWARD OF MASTER OF ARTS DEGREE IN COMMUNICATION STUDIES IN THE UNIVERSITY OF NAIROBI

2016

DECLARATION

This research project is my original work and has not been presented for any other Master's degree in any other university

_____

GATHUA MERCY NYOKABI

K50/76008/2014

This research project has been submitted for examination with our approval as University Supervisors

_____

Dr. Samuel Kamau

Lecturer

School of journalism and mass communication

University of Nairobi

DEDICATION

I dedicate this work to my husband Titus Watitu and my son Karl Kimani. I would also like to thank both my parents John and Anne Gathua for their love and support. I wouldn't have gotten to the point I am at today without them.

ACKNOWLEDGEMENT

I first would like to praise the almighty God in making all this work possible.

I am extremely grateful to Dr. Samuel Kamau who kindly accepted to be my supervisor and played a major role in the development of this thesis. His guidance, encouragement, support, time and invaluable suggestions formed a useful foundation for this work.

I am also extremely grateful to the following people for all their help, encouragement and support during this project: - Caroline Gathua, Rosemary Gathua, Brenda Odhiambo, Victoria Mbui, Zipporah Mwangi, Dorothy Rutto, and Daniel Njoroge.

ABSTRACT

The purpose of this study to establish what the major security and privacy challenges smart phone users on social media experience and, what if anything, they do to protect themselves. The issue of cybercrime and personal security online is a major threat globally and with the growing numbers of smartphone users and internet dependency in Kenya, people are susceptible to having their private information misused. The studies address this threat by finding out the extent to which smartphone users in Nairobi are aware of security threats lurking online. The researcher employed a mixed methodology approach where a survey questionnaire and Focus Group Discussions were used. The population sample was 160 respondents from the University of Nairobi, aged between 18-35 years who have access to smartphones and are active social media users. Findings show that most people are aware of some of the threats to privacy on social media and smart phones. However, it was evident that some respondents do not safeguard their privacy when accessing social media sites. It was recommended that in order for more Nairobi residents to pay attention, there is a need for more education and awareness of the impact of our digital footprint on financial, personal and professional lives. In conclusion, there is a clear need to keep consumer education on impact of loss of privacy on SNS and smartphones in Nairobi

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 Overview

This chapter will cover the background, statement of the problem, significance of the study, objectives, research questions, scope and limitations of this study.

1.2 Background

In recent times, social networks and other content sharing user-driven technologies have dominated the internet. Smith (2009) observed that with social media technology taking a lead in the world of communication, a massive revolution has occurred in user-generated content, global community and publishing of consumer opinions.

The number of internet users in the country is currently at 29.6 million with mobile data constituting 99% of the total subscriptions. A report gathered from Safaricom, the largest mobile service provider in Kenya and the largest devices retailer occupying over 85 % of the mobile data market share, by CAK (2016) revealed that Consumer purchase of Smartphones is currently at 67 % over the total phone sales. This unprecedented growth in smartphone use means that the number of Kenyans connecting to new media like Twitter, Facebook, WhatsApp, Instagram, twitter and Google+ has also increased. Though there have been numerous studies to gather the statistics from Kenyan organizations such as CAK, Safaricom, Jumia and others; little has been said about privacy and online security.

Globally, some countries have put more emphasis on security and privacy online, mostly to guard against hackings and identity theft. This is perhaps why numerous studies have been conducted in this area, particularly in the developed nations. The gap, however, lies in establishing security and privacy issues and what Kenyans already know. Most

Kenyan studies rely on the statistics such as overall smartphone users and not on their behavior. This study aims at establishing what privacy and security challenges are faced by social media and smartphone users.

In a published article by the US federal government, on Privacy and Security in a connected world, commonly referred to as "The Internet of Things" or (IoT). People from all walks of life should comfortably upload and download data from the internet almost automatically. It is expected that by use of IoTs, people are bound to enjoy life with very few worries with options such as: automatically posting pictures online by use of Internet-connected cameras, home security systems that controls your lights when away or sharing with your close friends your normal sporting activities such biking or running. Rose, Eldridge, & Lyman (2015) defines Internet of Things as a situation where one is able to connect to the internet, GPS and other everyday activities through the use of simple internet-enabled objects far away from computers and with minimal human intervention. It can generally be argued that IoTs, have increased the amount of personal data we upload and share with the world by automating a big percentage of the process of tagging and saving images, routes, likes and predicting trends, this potentially raises the threats to privacy and security online.

The aim of this study is to discern whether Kenyans understand the security threats lurking online due to issues surrounding privacy or lack thereof. Privacy refers to the safeguarding of one's confidential information from unauthorized people (Gibbs, 2008).The author further maintains that privacy limitation should mainly be centred within these three constructs

1. Secrecy: which refers to control of information
2. Anonymity: acting without attention from others and

3. Solitude: limiting physical access to an individual

When thinking of privacy, social media should meet these three conditions but more often than not, all three do not exist on social media and smartphones. This study should help establish how much the average person knows about internet security and what measures, if any, they have taken to preserve their privacy in an increasingly digital society.

1.3 Problem Statement

The uptake of technology and smart phones and or similar devices is at an all-time high in Kenya. The Communications Authority of Kenya (CAK) puts the number of mobile phone subscribers in the country at 37.8 million by the end of the first quarter in the financial year 2015/2016. According to the latest report released by CAK (2016); data/internet subscriptions seen recently have contributed to the immense growth in the Kenyan market telecommunication industry. Okuku et al., (2015) observed that the launching of undersea cables in 2009 created a very high demand for internet in the Kenyan market. The undersea cables brought what can easily be termed as ICT revolution. The increase in Internet bandwidth in the country led to an increased number of people who are dependent on the Internet.

With this rise in mobile penetration and data access, comes a corresponding rise in social media and smartphone use in our society. The uptake in smartphone use in the country has brought out a debate on issues surrounding privacy, largely because the number of personal information new media users freely share on social media and smartphone platforms is astounding. Gercke (2009) observed that the high use of smartphones has shifted cyber threats from desktop computers to these new devices. According to Gercke (2014), there is a need to come up with a system which can oversee the whole issues of

smartphone security through undertakings as many studies have suggested. Kenya Cyber security Report of 2014 indicates that most cybercrimes including mobile malware, identity theft, fraud, data theft are now being conducted through mobile devices. This makes Kenya more vulnerable to cybercrimes now more than ever.

The Norton cybercrime report reveals that 10 percent of all the adults using mobile phones to go online were victims of cybercrime last year. Mobile vulnerabilities have grown as people use their gadgets online more frequently. In January 2012, several Kenyan government websites succumbed to a cyber-attack that left inaccessible. The attacker was an Indonesian hacker who was presumably testing hacking tools and skills acquired from the web. Some 103 government-related websites were affected(Shahonya, 2012).

The fact that the Government has done little to address the issue of cybercrime and personal security online coupled with the growing numbers of smartphone use and internet dependency means that Kenyans online are susceptible to having their private information misused. To this end, this study will seek to find out the extent to which smartphone users in Nairobi are aware of security threats lurking online. It will also attempt to identify the measures employed to safeguard the privacy on social media and smartphones and how effective these measures are.

1.4 Significance of the Study

The rise in security and privacy concerns is undeniable, seemingly, because of the unprecedented growth in the use of social media and smartphones. A Federal Trade Commission staff report dated January 2015 stated that in the past half the internet carried more "things" regarding connectivity more than the actual number of people in

the entire world. The same report projected by the end of 2015, close to 25 billion will be connected to the internet; the number is expected to rise to 50 billion by 2020.

This study will help us to discern the gaps in security on social networks and hopefully increase awareness in the users. Smartphone users will be sensitized on privacy and security challenges, and their behavior will hopefully be influenced. The findings of this study are also important in that they can help curb cybercrimes as well as influence or strengthen policy.

1.5 Objectives

This study is guided by one main objective and three specific objectives, which are:

1.5.1 Main Objective

To establishing the major security and privacy challenges smartphone users face on social media and what they do to protect themselves remains the main aim of this study.

1.5.2 Specific Objectives

This study is guided by three objectives which are:-

1. To establish the level of awareness on privacy and security threats among social media and smartphones users.

2. To identify the privacy and security challenges that Smartphone users on social media are experiencing.

3. To determine the extent to which privacy and security concerns have influenced online behavior smartphone users to grow in the year by 98% to 3.4 million

1.5.3 Research Questions

1. Are respondents aware of any threats to privacy on social media and smart phones?
2. Is the online behavior of the respondents shaped by privacy or security concerns?
3. Which measures have respondents taken to protect their privacy on smartphones and social media?

1.6 Scope and Limitations of the study

Time and monetary constraints influenced the choice of a target population. The study will be conducted at the University of Nairobi; this is mainly because the student body has a diversity that should provide useful insights. The Geographical location of the University also coincides with the parts of the country that has the highest internet and smartphone usage; Nairobi.

This will, however, limit our findings to the perspective of the elites. While this is a limitation, most social media and smartphone users in the country tend to be educated as literacy is needed to actually post and read online and as such our target population would need to be educated and tech savvy.

1.7 Definition of Terms

Internet of Things (IoT)

In a setting where a large number of embedded devices employ communication services by use of Internet protocols is defined as the “Internet of Things”. Rose et al., (2015) also refers to these objects as “smart objects “Another term used to refer to these objects is the "smart objects”. These objects are not operated by people but are mostly automated. However, you will find them in certain sections of buildings, vehicles or spread out through the environment.

Self-disclosure

Jourard and Lasakow (1958) define self-disclosure as the act of enlightening others on what you already know with the aim of passing knowledge. It is commonly known as "making of self-known to others"

Social Network Sites (SNSs)

According to Boyd and Ellison (2007) in Conole, Galley, and Culver (2011) social network are web-based services that permit its users to

1) Come up with public or semi-public profiles in a bounded system

(2) To choose a group of users with whom they share information

(3) Have the power to navigate or view their list of connections and those made by their counterparts in the system

What varies is often the nature and nomenclature of these connections; it may vary depending on site. Some studies will also refer to the same concept as Online Social Networks (OSNs). According to Gummadi, Krishnamurthy, & Mislove, 2013, millions of people are now shifting to OSNs, this dramatic shift has caused a fundamental shift in the patterns of context exchange over the Web (Gummadi, Krishnamurthy, & Mislove, 2013).

For this study, the term SNSs and OSNs will be synonymous with social media and Social Networking sites (SNS).

Smart-Phones

Guo & Wang, (2007) defines a smartphone as a gadget device that combines both telecom and internet services onto one single device that has both computing and networking power of Pcs.

Security

Security in the context of this study will be regarded as safety for SNS and smartphone users against threats such as malware, gray ware, hacking, phishing, loss of privacy, illegal data mining or unauthorized access to private data online.

Privacy

Atheneum, (1967) for an individual, a group or institution to enjoy privacy, they must all be able to determine when, how and to what extent can their information be spread to others.

Cybercrime

A South African law on Electronic Communications and Transactions Amendment Bill, 2012, defined cybercrime as an offense or crime committed using electronic communications, information system by the help of internet enabled devices.

Phishing

Phishing is described by Norton-Symantec as an online con game. These are tech-savvy con artists and identity theft criminals who trick people into exposing or sharing sensitive or private information, using spam or fake sites. (http://us.norton.com/cybercrime-phishing)

Identity Theft

Newman and McNally (2005) assert that this type of theft comes in very different forms. The perpetrators of these crimes can be identified from a wide variety of actions ranging from mail fraud, credit/debit card fraud, cheque fraud, and medical fraud, pickpocketing, robbery, burglary, or mugging to gain a target victim's personal information. Other criminal activities like counterfeiting and forgery to using a stolen identity to commit acts of terrorism also falls in this bracket.

Self-disclosure

According to Bash (2015), self-disclosure is the sharing of previously unknown information with the aim of passing the information to others.

CHAPTER TWO

LITERATURE REVIEW

2.1 Overview

Chapter two is an analysis of literature in areas of cyber security in Kenya and globally, social media and data mining, smart phones and privacy, management of privacy and security on the internet as well as Theoretical framework, that is, Communication Privacy Management Theory.

2.2 Introduction

There are numerous studies and reports such as (Joinson, Reips, Buchanan, & Schofield 2010 who review how the internet and acquisition of sensitive information sometimes illegally, Gacy 2010, who delves into malicious software and Albrechtslund (2013) who examines the ideas of users who know the dangers of privacy loss but seemingly do not care; that look into the major issues we are reviewing, most of them will concern the amount of information shared on social networks and how this impacts security and privacy. Majority of the aforementioned studies and others conducted in the areas of privacy and security online either focuses on social networks or on smartphones but not both of these things in relation to privacy and security and that makes our study unique. I would, therefore, posit, based on both Gacy's and Albrechtslund's statements above that when these two (smartphones and social media) converge the threats to privacy and security escalate. Social networks accessed through any device easily gather huge amounts of data about the users, but once accessed through the most personal devices: smartphones, the threat rises significantly. These devices are seemingly used far more frequently than P.Cs and may hold more data such as contacts, location data, emails, apps, e-banking information and varied social networks.

There are numerous schools of thoughts on privacy on social media ranging from 1.SNS users simply do not care about privacy(Sarah Lynch, Allee Manning, 2016), 2.it has also been argued that privacy settings are too complex and users are not fully aware of the terms they agree(Zhao, Binns, Kleek, & Shadbolt, 2016) 3. It could also be that social media and smartphone users may share content intentionally but do not really want to their information mined and used they do not want to be under surveillance (Rainie, Kiesler, & Madden, 2013). 4. Another viewpoint could be that smartphone and the corresponding applications have been deeply integrated with data mining capabilities and keep prompting us to upload information and acting as IoTs to surreptitiously saving and uploading our information(Rose et al., 2015).

One cannot deny the fact that social, political, moral, epistemological, and cultural landscapes in which we live have immensely shaped by the whole concept of internetworking. Koopman (2008) observed that given the huge potential on how the internet can bringing changes to both political and epistemological surrounding, people have no choice but to accept the internet as their daily life companion. It is therefore paramount that we study this phenomenon as a reality in our society. It is only due to technological advancement that we are able to enjoy collection, storage, and exchange of sensitive information using very simple means (Petronio & Durham, 2008).We should all appreciate the whole aspect of computers as it has acted as the backbone to all these advancements. A government can even gather illegal information thanks to these prime connectivity features (Joinson, Reips, Buchanan, & Schofield, 2010)

2.3 Internet Use and Cyber Security

According to (Chennamaneni & Taneja, 2015) Social networking sites and applications have grown astronomically most recently. Druggan & Brenner (2013) conducted a survey in 2012 to identify the means of interaction used by people. Their study results

revealed that social media accounted for 67 % of all internet users. Among all the new media Facebook takes the lead, a report released on December 31, 2014 revealed that Facebook enjoyed a massive turnaround of close to 1.39 billion in 2015. Despite email remaining a common hotspot for cyber criminals, this trend seems to be shifting swiftly to the social media platform. A report released by Internet Security Threat Report in 2015 showed that close to about 70 % of social media scams were manually scanned. Considering that these scams have the ability to spread rapidly, they often present perfect opportunities to cybercriminal to strike as most people just click thinking it's a common post from their friend.

This report by Symantec further illustrates the need to conduct this study on the concerns posed by social networks to our privacy and security online. People need to revise the perception that cyber security measures are only viable for PCs, criminals have taken advantage of this and are causing devastating effects to many smartphone users who remain ignorant on the security risks.

This increase in the use of the internet has left users exposed to a rise in instances of cybercrimes. A 2013 report by Symantec Corporation notes that cybercrimes are alarmingly on the rise in Africa than anywhere else in the world. Close to about 80 % of all African continent computers are infected with viruses and other malicious software (Gacy, 2010). Due to very weak network and weak information security Africa is seen as a perfect place for cybercrime perpetrators.

According to a report released by Norton Cyber-Crime, 18 adults are victims of cybercrime every second, which means that there are more than 1.5 million cybercrime victims globally per day. South Africa is the country with the highest cybercrime victims

in Africa, at 80 per cent, which puts it third globally behind Russia which stands at 92 per cent and China at 84 per cent.(The International Telecommunication Union, 2015)

2.3.1 Cyber Security Threats Facing Kenya

Kenya has not been left out on the whole issue of cyber insecurity. Each day organizations continue reporting of system breach and exploitation of their computer networks. According to Serianu (2014), most of these frequent and targeted attacks are caused by sophisticated hackers who seem to be exploiting the weak cybercrime regulations in the country.

In the recent years, there has been a substantial rise in cyber security incidents and cybercriminal activity targeting both public and private organizations in Kenya(Ephraim, 2003).

The fastest growing threats to Kenya's cyber security can be put into three main categories: malware attacks, social media attacks, and cyber fraud. Malware is any malicious software that brings harm to a computing system and its users.(Shahonya, 2012) An example of social media attack was on 21st July 2014, the Kenya Defence Forces' Twitter account @kdfinfo, was hacked into by a Latin-American based anonymous group that goes by the name of 'Ano_oxo3' who left a series of misleading and abusive tweets(Kiboi, 2015)

In Kenya, great strides in the incorporation of ICTs into various industry sectors have been made. As of 2013, Mwenesi (2014) noted that ICTs contributed to 12.1 percent of the country's GDP. Admittedly this is a significant achievement but, it is watered down by the lack of legislation governing cyberspace, which leaves us at the mercy of cybercriminals. An example of this was seen when 77 foreigners — one Thai national and 76 Chinese — were arrested in Nairobi in December 2014 after they were found in

possession of equipment capable of a massive cyber-attack, such as infiltrating Safaricom's M-PESA, cash machines and bank accounts (Agence France-Presse 2014). The suspects, according to the Kenya Police were to be charged with operating an unlicensed telecommunication facility, meaning that they could have faced a maximum of 15 years in jail or have to pay a 5 million Kenyan shilling fine (US$54,000), with more charges pending (Nzwili 2015).

2.4 Social Media and Data Mining

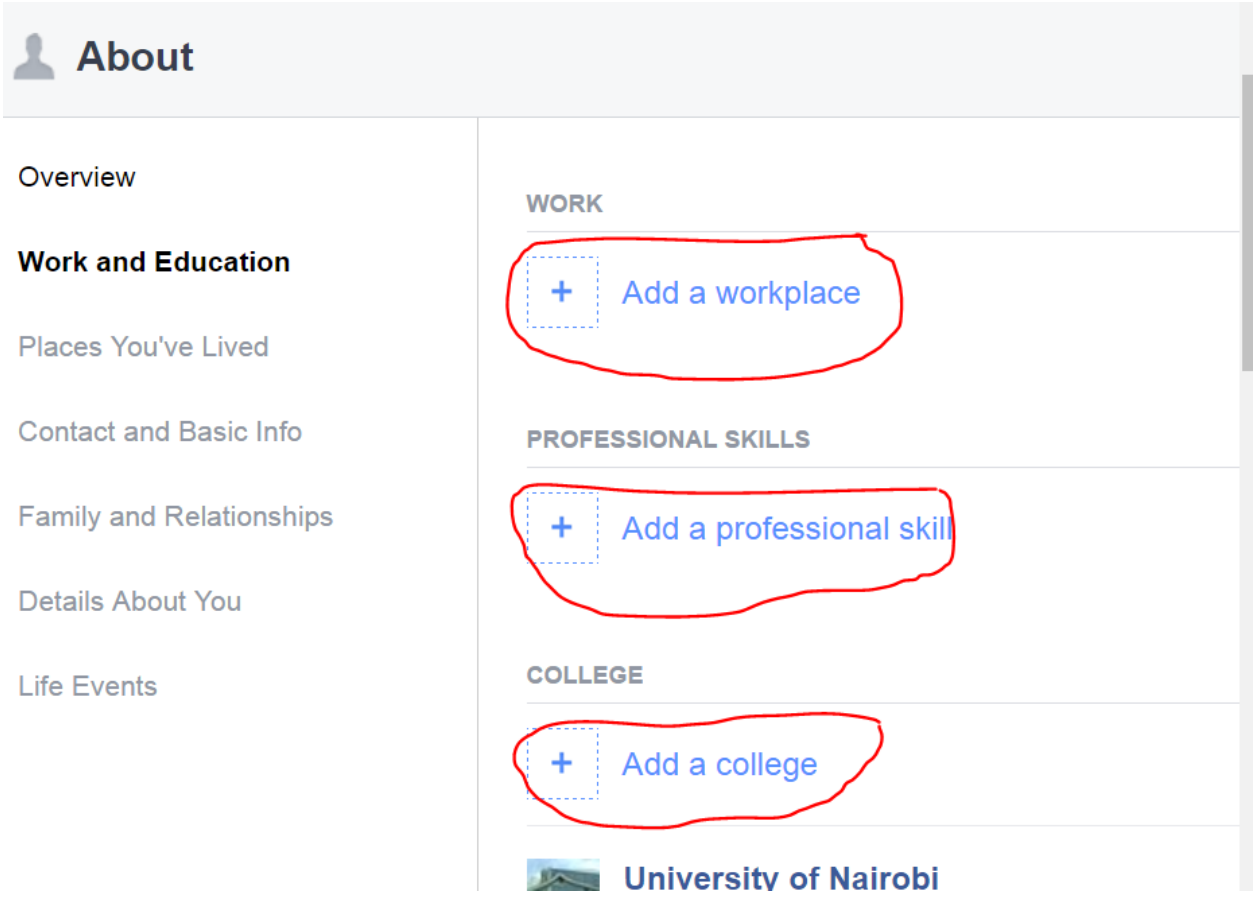
Social media "mining" has become the standard industry practice, especially among insurance and human resource companies. People are combing through social networks accounts for employment and legal purposes and this is why oversharing on social media can be dangerous (Trend Micro E-guide n.d. 2012). With this statement, we see some evidence that information we share in profiles and updates on social networks and via IoTs is actively gathered and commercialized. It will be useful to investigate how aware social media and smartphone users are about this.

While it is often assumed that the recording of user data on SNSs and in smartphone applications leads to the violation of privacy via the surveillance techniques used to obtain this data, Albrechtslund (2013) notes that many users tend to know what they have agreed to. On the other hand, even those users who are more conversant with the data mining on Facebook tend to be less informed about its use of offsite activity. For instance by introducing 'like' buttons on numerous other online sites, Facebook has significantly spread data mining reach (Leaver, 2013).

In 2010, Google reported that 96 percent of its revenue was derived from advertising on its own sites and on sites that use its advertising products. Facebook's global advertising revenue was also slated to rise by an estimated 104 percent in 2011 to US$3.8

billion(Trend Micro E-guide n.d. 2012). This further illustrates the need for social networks to gather data from information posted by the users to customize advertising based on the likes and habits of social media users.

Social network sites are communication podiums that are networked. Here, users have unique and distinguishable profiles comprising material provided by the user, the system or fellow users (Ellison & Boyd, 2013). Going by these characteristics of SNSs, it is no wonder social networks seem to prompt users to share a growing amount of personal information with pointed questions regarding hobbies, institutions attended, jobs held, and family members / relationships and demographics in order to customise activities /content and stay competitive and keep audiences interested. See image below of sample prompts on a Facebook profile.



If social networks by definition must have individual profiles that build connections and interactions, it therefore stands to reason that they will prompt, encourage and convince users to keep sharing. The more users share the more successful a social networking site is deemed.

2.5 Smart Phones and Privacy

‘'Our mobile devices have become a critical part of our daily lives. Even in Africa, where Internet penetration is still limited, the majority of people who own these devices use them to access information of some kind online. In fact, many entrepreneurs run their businesses solely from their trusty mobile device without giving it a second thought. Some might argue that the only way you can keep your mobile device (and data) completely safe is to ensure that it never leaves your sight. Even if you have security software installed on your mobile device, you have to assume that all the data on it is compromised when it goes missing. This means that you have to change all your online passwords, including your banking login details, to ensure that the potential damage is limited’’(Opil, 2014,p. 8).

On 5th March 2015, Forbes published an article essentially meant to create awareness on privacy or lack thereof was borne of our over-dependence on smart phones. ‘If most IoT devices are controlled from our smart phones, which in turn gather data from all our various profiles ranging from social networks, online banking, shopping sites and apps, it is therefore conceivable that smart phones ‘spy’ on their users.

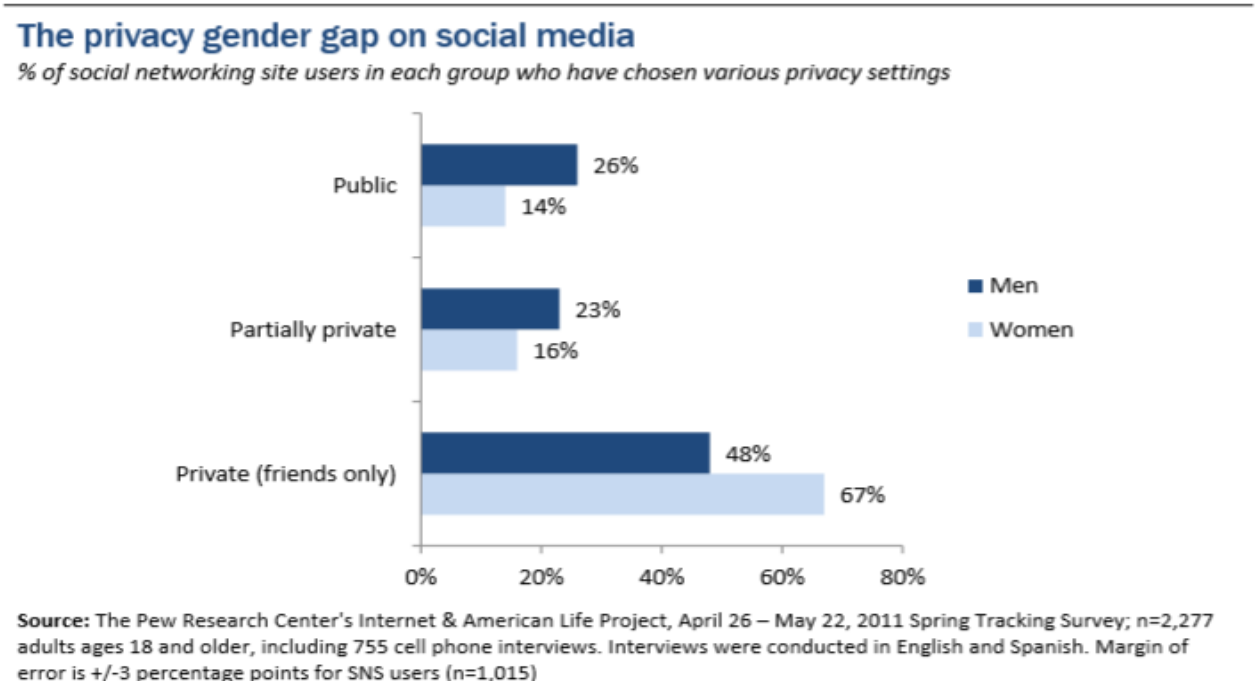
The details and patterns of your everyday life from banking, health conditions, habits, location, and bio-data are out there and you have no actual control on how it may be used. The number of devices that can be classified as IoT are on the rise; smart devices including a smart phone, tablet, smart watches, game consoles, GPS enabled cars/bikes and smart work out gear. (Rose et al., 2015)

2.6 Privacy versus Convenience

The term privacy has grown to be a prevailing keyword. Every individual user has different levels of concern about his or her own privacy ‘‘based on that person's own perceptions and values" (Joinson et al., 2010). This is probably why voluntary disclosure on social networks varies vastly from one person to another. There is no privacy policy offered by social networks and smartphone that will be a blanket solution for its millions of users. The users therefore need to be aware and empowered to pick and choose the security options that fit their privacy needs.

Most studies conducted seem to imply that most people say they care about privacy but their online behave our does not necessarily reflect these concerns. There are many demographic factors that Smart-phone is the trend of unified a person's attitude to privacy on social media or on smart phones.

Figure 2.1 Privacy gender gap on social media



Source: The Pew Research Center's Internet & American Life Project, April 26 – May 22, 2011 Spring Tracking Survey; n=2,277 adults ages 18 and older, including 755 cell phone interviews. Interviews were conducted in English and Spanish. Margin of error is +/-3 percentage points for SNS users (n=1,015)

In a Norton survey, end users reflected concerns regarding how their data is used; one in four SNS users confirmed they were unaware of what they allow access to when downloading an app through their smartphones. Most people readily give up their privacy for free apps or the promise of convenience.

2.7 Social Media, Smartphones and Self-disclosure

Self-disclosure is a fundamental part of social media use. Simply put; we join social networks to make new friends or reconnect with old ones, making self-disclosure inevitable. This study hopes to establish the balance between self-disclosure and over-exposure and possible links to privacy and security online. This study proposes that most social media users will be more negligent with regards to privacy on social networks than they would be in inter-person or in other interactions. Madden (2012) states that people are probably more open with what they share because they don't fully comprehend how their data is stored and used.

We must seek to study actual behaviour online and intent to disclose separately. The people who disclose may do it knowingly or unknowingly (Greene et al., 2006). This study must therefore seek to discern whether privacy is a concern that is overlooked intentionally or whether ignorance is the cause of self-disclosure. Many of the studies of privacy concerns and behaviour have measured reported disclosure or intended disclosure rather than actual behaviour (Joinson et al., 2010). Privacy and security, it would seem are influenced by the complexity of user agreements. Modern day users fail to realise the consequences of what they do. We frequently see ads on social media pages corresponding to our recent searches on Google or our calls logs on smart phones.

This information derived from 'spying' on us is used to customise ads and to suggest people we may know or pages we may like. The promise of like our page/ join a group or

fill in online questionnaire for a chance to win some giveaway is the easiest way to lure traffic and grow popularity of a social networking site or smart phone app. The volume of information we share freely on social media and with smart phone apps will only continue increasing.

There amount of self-disclosure seen on social networks surpasses interpersonal self-disclosure, given the size of possible audience every post reaches and the countless times it could be reposted. According to (Chennamaneni & Taneja, 2015), interpersonal communication is made richer by tone, body language, pitch, facial expressions, gestures and even timing. All these aspects are not on social media interactions and to compensate people say more information, frequently in order to try and mimic the intimacy and impact of an interpersonal encounter.

2.8 The Management of Privacy and Security on the internet

The on-going progression of Internet, as a virtual world made up of unified networks similar to the physical environment, is symbolized by huge amounts of information. As Internet information keeps growing, there is also increased value of the information to government, companies and individuals with bad intentions.

Since disclosure on social media is among the key factors that leave us vulnerable to cyber-attacks via avenues like identity theft (Ellison et al., 2011), we must become more cautious of the information we put online. This is because there is an intricate link among social and privacy capital (Ellison et al., 2011).

The management of security while on the internet is a dynamic process that involves the assessment of key security risks, developing appropriate policies and procedural frameworks to curb these risks, the implementation of said policies and procedures, and finally monitoring processes to assess the effective operation of the established and

implemented framework and procedures Cameron (2014). For this approach proposed by Cameron to help safeguard privacy and security of all users online I would argue that we must create awareness and knowledge of the gaps in this area which is what this study intends to do.

2.9 Theoretical Framework (Communication Privacy Management Theory)

CPM theory is an established communication theory. It explains the self-disclosure procedures both online as well as on social states. It aims to define the how a disclosing persons and recipient handle their privacy boundaries and disclose confidential information. Having a social media profile often puts the users in constant conflict between wanting to share and keeping information private. By virtue of having a profile on social media, users mean to share their lives with their friends, followers and sometimes the general public , they do so via status updates, photos, videos, vines, tweets and events: there is a conflict arising because they want to share the information but some opposing need for privacy still exists. According to (Chennamaneni & Taneja, 2015), it describes self-disclosure as how to reveal information where a person continuously balances the opposing need to reveal and conceal confidential information. This is the balance between wanting to share what is going on with your life and keeping it private. It is harder to maintain collective privacy as the co-owners will have different needs/views/feelings and values.

It can therefore be argued based on Petronio's statements that information starts out as private with thick boundaries but when sharing of this information is done on social networks or on smart phone apps the boundaries become thinner and more porous as more people get access and rights to re-share the same information. It will be interesting to see if this argument holds water with social media and smart phone users and whether this visualisation will influence behaviour.

The following are the five main CPM principle by Petronio:

1. Individuals believe that they have the right to control personal or private information
2. Individuals use personal discretion rules to control their confidential information
3. If an individual tells or gives others access to confidential information, the other party becomes a co-owner of the information.
4. Co-owners of confidential information must have mutual agreement on satisfactory confidential rules about notifying others.
5. If there is no mutual agreement on confidential rules between the co-owners, there arises boundary turbulence.

With regard to social media, Petronio's theory can be applied in that a person obviously owns their individual private information, the privacy boundary thins or becomes significantly more permeable when this information is posted or shared on social networks or on smartphone apps. Once information has been shared with social media friends or followers, the privacy boundaries as well as the information in question are co-owned as any of the co-owners can therefore disseminate said information. You and your social media friends and followers must therefore agree on whether it can be re-posted. We could argue that social media and smart phone connections make the privacy boundary almost non-existent because the number of recipients is usually large and online posts may offer anonymity for anyone who wants to break the boundaries. Smart phones farther complicate issues because your information may be re-posted using features such as screen shots and the share feature that easily offers numerous channels of spreading information at the touch of a button.

Disclosure is a word very common to researchers i.e. different researchers have different meanings. An insightful description of the term describes it as the way to tell or share what was not known before for it to be shared knowledge. This means that there must be a person to receive the information. This theory ties in with this study as it examines the process by which all information transitions from privately owned and how the boundaries can progressively thin until information becomes public. We farther examines how boundary turbulence occurs because the friends we share information with on Social networks and using smartphones are usually not in close proximity and there is rarely any opportunity to agree on privacy boundaries and rules surrounding re-sharing. The study aims to review how aware of the loss of privacy social media and smart phone users are and if they impact behaviour on SNS.

CHAPTER THREE

METHODOLOGY

3. 1 Overview

In this segment, the researcher will discuss the methodological strategies that were adopted in this study .It includes the research design, description of the area of study, target population, sampling design, data collection methods and instruments, procedures for data collection and data processing strategies.

3.2 Introduction

This study relies on primary data obtained from the field through the administration of questionnaires, as well as to focus group discussions.

3. 3 Research Design

A research design refers to how a researcher sets the conditions for collecting and analysing data (Babbie, 2002). This study primarily utilized mixed methodology. It involved using a survey, which is quantitative, and two focus group discussions, which are qualitative data collection method.

The survey, was conducted through the administration of questionnaires, it was beneficial to the study as a tool for assessing the opinions and knowledge held by the target population about privacy on social media and smartphone use. In addition to this, the survey was chosen as it would enable the researcher to measure the attitudes and orientations of larger populations.

Qualitative methodology was included in this study because it is less structured and promotes a longer and more flexible relationship between the researcher and the respondents, which leads to the collection of richer and comprehensive data. The fact

that social media enjoys extensive use in society means that the researcher will have to have an in-depth engagement with the social media users, in order to explore and understand how this constant exposure to the medium has been able to shape their perceptions regarding privacy and online security or lack thereof. The use of a qualitative methodology in conjunction with a quantitative method means that the data collected could be cross-referenced and contextualised hence, less likely to be susceptible to issues of validity and reliability.

3.4 Area of study

The area of study is Nairobi, Kenya's capital city. Consistent with the 2009 census, Nairobi's population stands at approximately 3.2 million people (KNBS, 2010).More specifically, the study was conducted at the University of Nairobi, due to its abundance of a smartphone and social media users. Young adults were chosen as the target population, because according to Östman (2012), it can be assumed that for them, the Internet is not a new phenomenon, but instead has existed most of their lives, meaning that their exposure to it has been frequent as well as sustained and there is usually no novelty to internet use to influence the findings. In addition to this, the University was chosen due to the fact that it would be possible to find a near-accurate representation of the desired population from all parts of the country.

3.5 Target Population

Population is defined as the total group of people, objects or events that all have one noticeable characteristic (Mugenda, 2003). Ephraim (2013) notes that the use of social media in Africa has become popular, especially among the youth. Statistics released by UN-Habitat (2014) show that Kenyan youth below 30 years make up over 77% of the Kenya's population. Out of these, 61% of the youth live in the rural areas; while a mere 39% live in the urban areas (KNBS, 2010).

When it comes to using social media, Kenya is identified to be amongst the leading countries. As Macharia (2015) explains, this is especially about social network sites like Facebook and Twitter. With this regard, because of its vast young population and progresses in technology, reviewing the issue of privacy in the use social networking services will be both relevant and timely. Safaricom, the industry leader reported that in 2014/15, Safaricom registered smartphone users increased to 3.4 million by 98 percent.

The target population of this research will be the youth in the University of Nairobi, aged between 18-35 years who have access to smartphones and are active social media users. The study will focus on students at the University of Nairobi specifically the Main Campus which accounts for 62% of all students at the university. The University was chosen because the student population mostly consists of young adults who extensively use smart phones and social media providing many possible respondents who meet the study's criteria. The student population is diverse and should yield rich data and provide useful insights on the issue. Reuters reported that there are 4.5 Million active Facebook users in Kenya with 95 percent of them logging in via mobiles (Strydom, 2016)

3.6 Sample Design and Sample Size

A Stratified random sampling was conducted in order to select the area of study, which in this case was the University of Nairobi, which is the oldest and largest public university in the country. This type of sampling ensures that specific individual divisions or categories are represented i.e. different faculties, both for undergraduate and postgraduate students. The stratification was done on the basis of the different schools, Faculties and institutes within the college of Humanities and Social sciences. The stratified random sample was used to ensure an equal representation of students across all disciplines offered in the University at the main campus in the study. Seeing as the study seeks a homogenous population with shared characteristics, which in this case will

be the students and faculty with a sustained exposure to social media and smartphones. The focus groups each consisted of 6 Nairobi residents between 18 and 35 years selected using stratified random sampling with some exposure smartphones and social media. Their views provided richer data in regards to matters of confidentiality and online safety and served to enrich the data gathered from the questionnaires while reflecting similar characteristics with the questionnaire respondents. Given that only 3.8 Million out of 26 Million Kenyans using Safaricom have smart phones a total of 14.6% of Mobile phone users (Safaricom Limited, 2016). It is tenable that not all the University of Nairobi student population are smart phone users. With this in mind, the sample chosen was 160 students instead of the 383 that would normally be chosen. The student population consisting mainly of urban youths could be argued to have a higher than average percentage of social media and smart phones users. Therefore, the researcher can use 383 respondents as the sample. 35% of smartphone and social media users are between 18 and 35 years according to a PEW 2014 study (see Appendix 7).

3. 7 Data collection procedures and instruments

The collection of primary data was done through questionnaires and a focus group discussion. Questionnaires were administered through research assistants in the different schools and faculties within Main campus.

3. 7.1. Focus Group Discussions

Kamberelis & Dimitriadis (2005) define focus groups as a collective conversation or collective interview. Neuman (2003) posits that focus group discussions tend to be informal and are done in a setting resonant of a discussion group. In order for a focus group discussion to be successful, its members must be made up of about 6-12 respondents who share certain characteristics relevant to the study (Kombo & Tromp, 2006).

This study conducted 2 focus group discussions among the targeted respondents, which were used to gauge their opinions and attitudes regarding their knowledge and management of privacy concerns when they use smartphones and social media. The data collected from the focus group discussions was used to gauge and explore in depth the beliefs, perceptions and opinions of the participants and the responses helped to enrich the data collected through the questionnaires and provide deeper analysis into respondent's behaviour and knowledge. The Focus groups consisted of 6 students from across the various departments/faculties and disciplines both undergraduate and post graduate.

3. 7. 2. Questionnaires

In this study, questionnaires were used to collect data (appendix 1) due to the fact that the target population is a literate one, and as such, were able to read and fill in the appropriate answers to the questions. They were distributed by the researcher and an assistant. The sample size chosen was 160 questionnaire respondents. Respondents were selected through the use of stratified sampling. Since university students' population is found under various departments, the subjects of the study were chosen at random under every subgroup, that is, department or faculty and various levels (undergraduates, Masters and Doctorate). The questionnaires had a balance of carefully constructed closed and open ended questions, which facilitated the collection of both qualitative and quantitative data.

3. 8 Data Analysis Procedures

Analysis was conducted through the use of data analysis software, namely SPSS, which were used to analyse the data collected from the questionnaires. Data collected from the focus group discussion was used to derive notes which were then coded into various themes, and then assigned to discuss the various research questions.

3.9 Ethical Considerations

The issue of privacy and security is sensitive and requires some precautions and measures put in place to safeguard the welfare of respondents. The study was properly authorised by the University after a research proposal defence with a certificate of field work (appendix 2) . All respondents were duly informed to ensure there were no concerns about informed consent. All focus group respondents also signed a consent form (appendix 3). There was utmost confidentiality in handling the data collected and anonymity was afforded to the respondents. The data collected was strictly used for academic purposes only. The project was duly defended and corrections made, after which a certificate of corrections was issued (appendix 4). The work was checked for plagiarism at the school of journalism and a plagiarism report was issued (see appendix 5). Having passed all these ethical checks the researcher signed a declaration of originality attached as appendix 6.

CHAPTER FOUR

DATA ANALYSIS AND DISCUSSION OF FINDINGS

4.1 Overview

The results/findings from the study were summarized and discussed in this chapter and assisted the researcher to reach some conclusions.

4.2 Introduction

When conducting data analysis, there are three stages in the process: 1) data has to be reduced, 2) data has to displayed, and 3) conclusions have to be drawn and verified (Saunders, Lewis and Thornhill, 2007). Data reduction seeks to condense and transform the data collected into more usable forms. This is usually achieved by simplifying, summarizing and focusing on vital sections of the findings (Kichatov, 2010). The next stage is the data display, this is where the reduced data is organised and assembled into forms that are easier to understand, and it usually include tables and figures. This process is supposed to make the data easier to handle and present (Saunder *et al*., 2007). The final stage of data analysis is drawing conclusions a process that is assisted by the 2 prior stages of data analysis discussed herein.

4.3 Response Rate

Response rate is described as the level to which gathered data comprise every sample member of the target study population. The number or respondents who returned their questionnaires was 150 out of the targeted 160.

4.4 Respondents background information

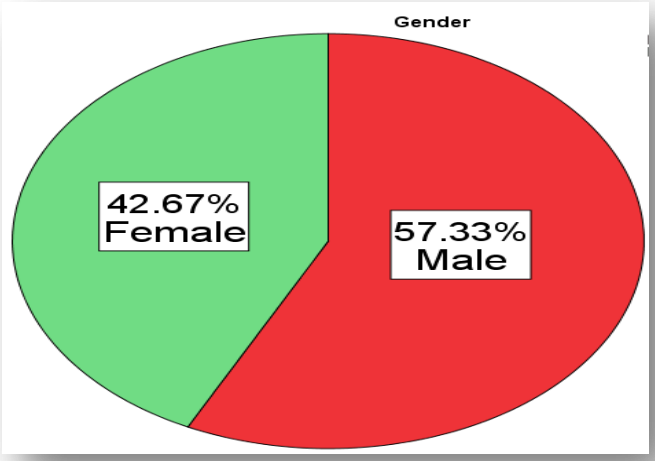
This study aimed to further profile the main demographic groups that the respondents fell into gender distribution, age distribution, and level of education. The findings were

discussed in the following sections. The gender distribution of respondents was along these lines: males made up 57% and females 43%.

4.4.1 Gender

The gender distribution of respondents was in this manner: Males made up 57% females 43%. It was important to get this data because previous studies have shown that females have a higher inclination to secure their SNS profiles. With regard to the basic setting of choosing, females are very conservative. A total of 67% women profile owners limit access contact to friends with only males making up 48%. Madden (2012). Demographic information would be useful in affirming or contradicting those findings. The data was as follows:-

Fig 4.1: Respondents (distributed in gender)



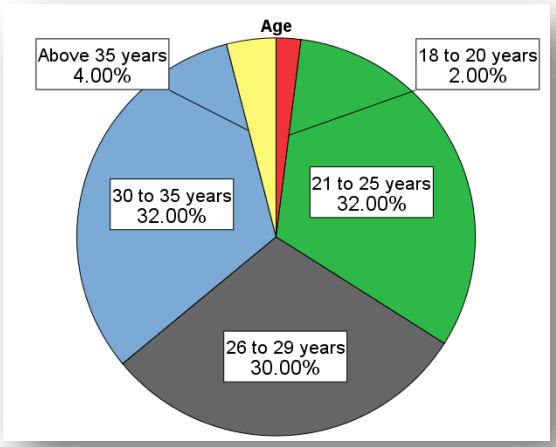
Source: field survey 2016

4.4.2 Age Distribution of Respondents

Although the target population was 18 to 35 years, it was still important to tabulate the exact ranges that ended up in the study. This would help to draw deductions and discern

any patterns and how they might relate to age. The study established that the age ranges of the respondents were as follows:

Figure 4.2: Age Distribution of Respondents

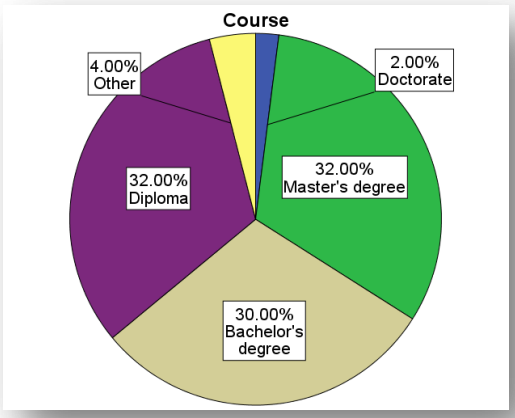


Source: field survey 2016

4.4.3 Level of Education of Respondents

To further understand the background of our respondents, the study analysed the level of education or the programmes they were pursuing, the background information would help see if the proportions of respondents reflected the distribution in UON. The findings were as follows:

Figure 4.3: Course Respondents are taking



Source: field survey 2016

These is consistent with the taget age group where most studnets between 18 and 35 years are pursuig Bachelor's, Diplomas, certificate and Master's courses and more likely to be encountered aound main campus

4.5 Social Networking Habits and Patterns of the respondents

The following section analysed the responses from the respondents of the survey and focus group discussions regarding their general behaviour on SNS and smart phones

4.5.1 Number of Respondents on the Various SNS

All the respondents were on at least one social media site with three quarters of them being on at least 5 social networking platforms with the most popular being: WhatsApp, Facebook, Twitter, YouTube, Google+ and LinkedIn. Out of 150 respondents, the number of respondent per social networks was as follows:

Table 4.1: Number of Respondents on the Various SNS

Social Network (SN)	Number of Respondent on each SNS out of 150
WhatsApp	140
Facebook	130
Twitter	130
Youtube	70
Google+	90
LinkedIn	50
Instagram	100
Pintrest	34
Reddit	24
Flickr	32
Tumblr	22

Source: field survey 2016

These findings clearly show that a majority of SNS users use multiple platforms online. When the issues was raised with the FGD respondents most of them argued that they

needed multiple platforms for varied reasons. WhatsApp was used for direct communication with people close to them family, friends or co-workers; while Facebook was used to keep up with a myriad of people in general ways. Some respondents said that twitter allowed them to be aware of breaking news and the latest occurrences.

4.5.2 Devices Used to Access Social Media (Social Networking Sites)

The respondents were also profiled on the basis of preferred devices on SN access and uploading content. It was found that 55% of the respondents preferred to access the Social Networks on smart phones while 50% used the same smartphones to primarily share content such as photos and videos on social media. The exact findings are presented in below.

Figure 4.4: Devices to Access SNS

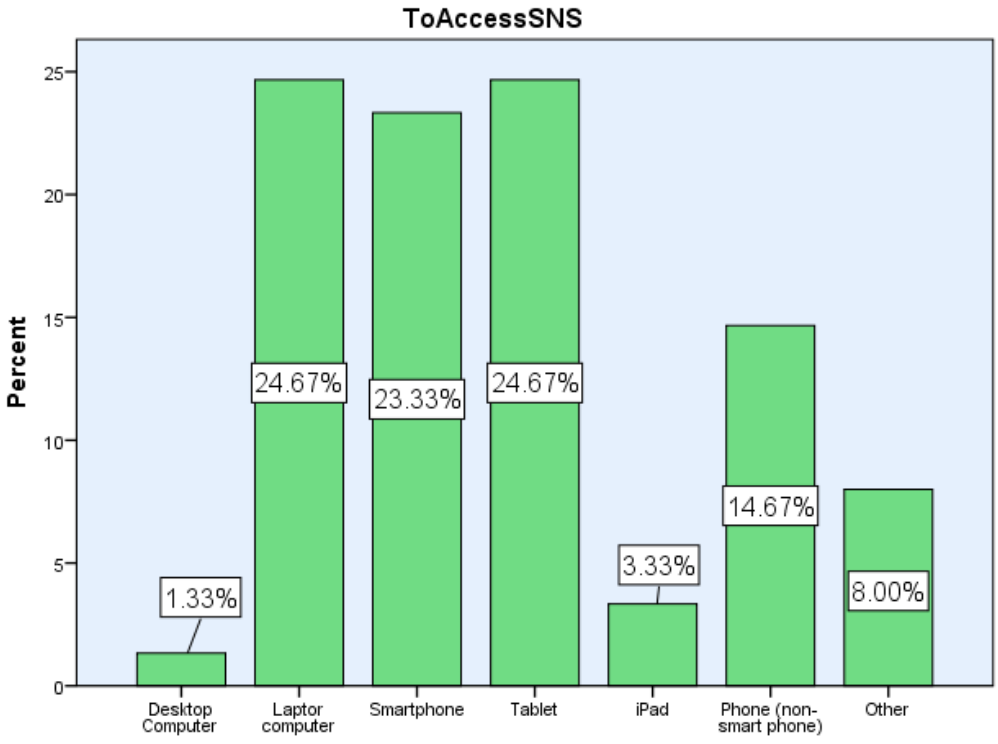
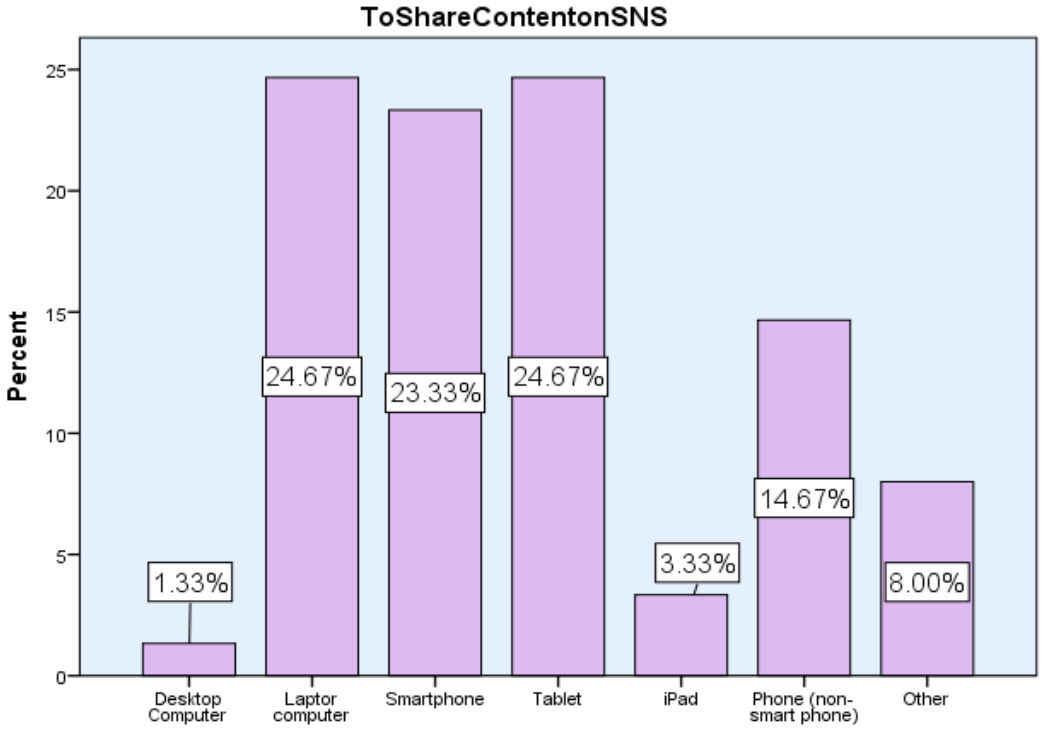


Figure 4.5: Devices to share content on SNS

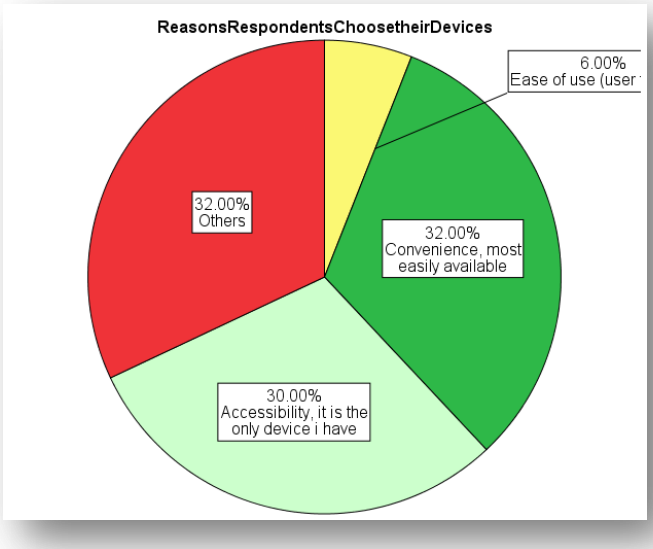


Source: field survey 2016

The devices used to access social networks were compared to devices used to upload content to see if users were consisted in choosing devices and the findings were mostly similar with a slightly higher number choosing computers to share content. The reasons that respondents gave for choosing the device to access social networks were also looked into.

Figure 4.6 Reasons Respondents choose their devices

The respondents were asked for the exact reasons they chose the device they preferred. The findings were as follows:



Source: field survey 2016

It was found that 32% of them chose their preferred device because it was the most convenient 30 % agreed it was due to ease of accessibility to them. 9% said they chose their device because it was users friendly and 32% gave other reasons such as:

- Large screen
- The device was very secure
- The content was already on the device
- The device that allowed them more editing options/features for their content

These findings imply that social media access is done spontaneously as an overwhelming majority (over 92%) gave reasons for choosing their devices as availability, accessibility and convenience. This is probably why only 4% of the respondents will use a desktop computer as it is not a device you have on the go.

The reasons the sharing of content was slightly higher on computers were ease of editing and more stable internet access for heavier files. The implication is that fixed data is still more reliable for larger content sharing tasks that mobile networks. It also implies that most people will alter. Edit and manipulate the information they post and need more computing abilities for this.

4.5.3 Time Spent Online versus Time Spent on Social Media Sites

32% of the respondents said that they spent at least 4 hours online every day but only 18% spend under an hour on social media sites per day. This means that more than half the respondents were online daily.

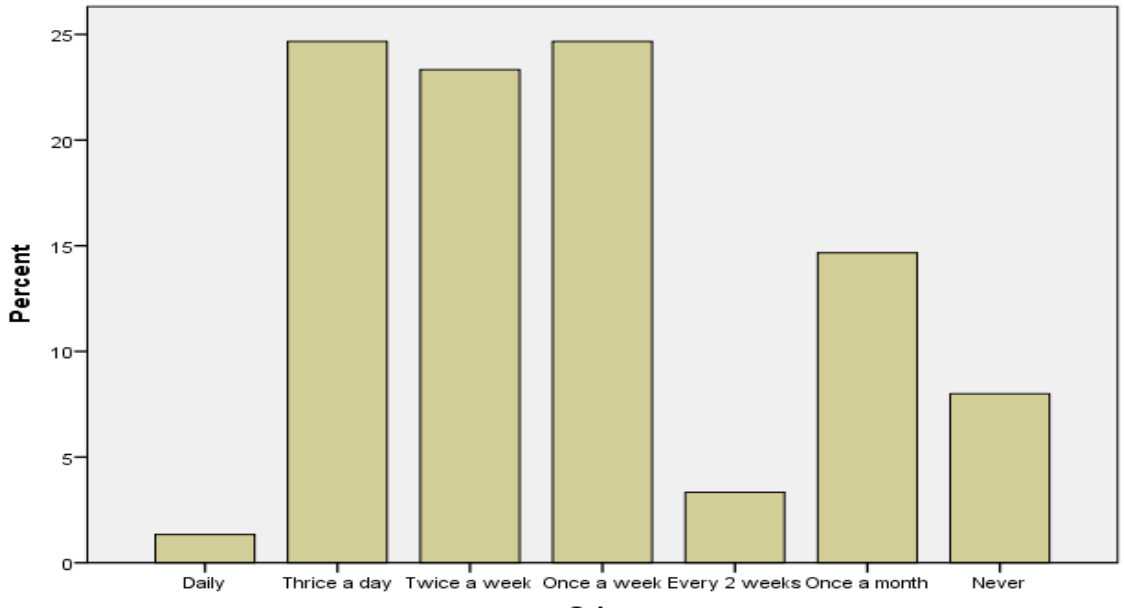
Table 4.2: Time Spent on Social media sites or Apps

Time Spent on Social media sites or Apps	Percentage of respondents
More than 4 hours a day	32%
Varies from day to day	23%
0-1 Hour Daily	18%
1-2 Hours 5%	5%
2-3 Hours Daily	14%
3-4 Hours	9%

Source: field survey 2016

Only about a quarter of the respondents said their access varied from day to day, while three quarters were online daily. The implication is that there is potential to disclose some information about your life, activities, likes, location and opinions multiple times a week and there ought to be a corresponding urge to learn about how that information is shared, viewed or sold. In comparison less than 5% of the respondents were on social media daily but a majority logged on to some social media platform every week.

Figure 4.7: Frequency of Social Media Access



Source: field survey 2016

The implication is that there is potential to disclose some information about your life, activities, likes, location and opinions multiple times a week and there ought to be a corresponding urge to learn about how that information is shared, viewed or sold

4.5.4 How Respondents use their Social Media Account

The respondents said they used social media for a variety of reasons including: - keeping up with friends that I actually know well in person, staying connected with people with interests similar to mine (known and unknown), staying in touch with family and friends who are not always nearby, share and follow issues of social-political significance, conducting business online, sharing content that they created and to keep up with trends.

The findings are tabulated below

Table 4.3: Reasons why people use social Networking Sites

Reasons why people use social Networking Sites	Percentage of Respondents
To keep up with friends that I actually know well in person	64%
To stay connected with people with interests similar to mine (known and unknown)	73%
To stay in touch with family and friends who are not always nearby	64%
To share and follow issues of social-political significance	50%
To conduct business online	27%
To share content that I have created	23%
To keep up with trends and news	68%

Source: field survey 2016

Over two thirds or 64%, of the respondents used social media for friends, family and people they knew personally. The impact of this can be explored further as some scholars have argued that Schouten et al. (2007) and Walther et al. (2008) argue that contrasting face-to-face interface, which can convey various non-verbal gestures and social signals, it is not possible for social media to do the same.

4.5.5 Are respondents aware of any threats to privacy on social media and smart phones?

When questioned about their concern on internet security, 80% were very concerned, 15% expressed some concern in varying degrees. The only respondents who admitted to not being concerned at all constituted 5%.

Table 4.4: How concerned are the respondents about Security on the internet?

Level of concern	Percentage
Very Concerned	80%
A little Concerned	5%
I know I should be concerned, But I am not	5%
Not at all concerned	5%
Somewhat concerned	5%

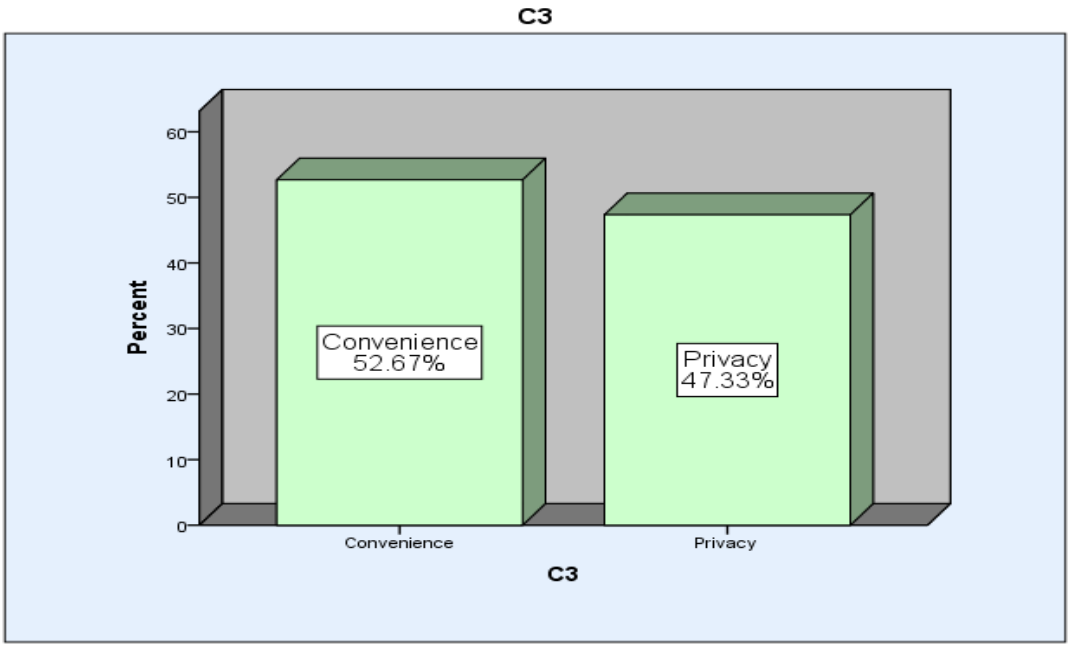
Source: field survey 2016

At least 70% or over two thirds of the respondents were aware of the following threats to online privacy and security:-Identity theft, phishing, smartphone sharing/tracking your online habits and banking fraud. In a seeming contradiction to the responses above, when respondents were asked what was more important between privacy and convenience, majority said privacy as presented in the chart below. At least 82% of the questionnaire respondents admitted that they were very concerned about security on the internet in general. In this regard the focus group respondents were concerned about smart phones 'keeping tabs' on them, and then sharing their habits, likes and history with other apps and SNSs. Over three quarters % of all respondents knew of the following threats to online privacy and security: unauthorised access to their accounts by 3rd parties, phishing, smartphones keeping track and sharing their profiling data with other apps as well as profiles being cloned. The focus group respondents expounded on these issues and said that access of their devices and SNSs activities was likely to be used to spy on them by spouses. One respondent had an account of how WhatsApp can be activated for the same phone number but on 2 devices that mirror each other.

4.5.6 Privacy versus Convenience

The respondents were asked if they prioritised privacy or convenience while on social networks and using the internet in general and 77% of the respondents said that privacy was their priority.

Figure 4.8: Privacy versus Convenience

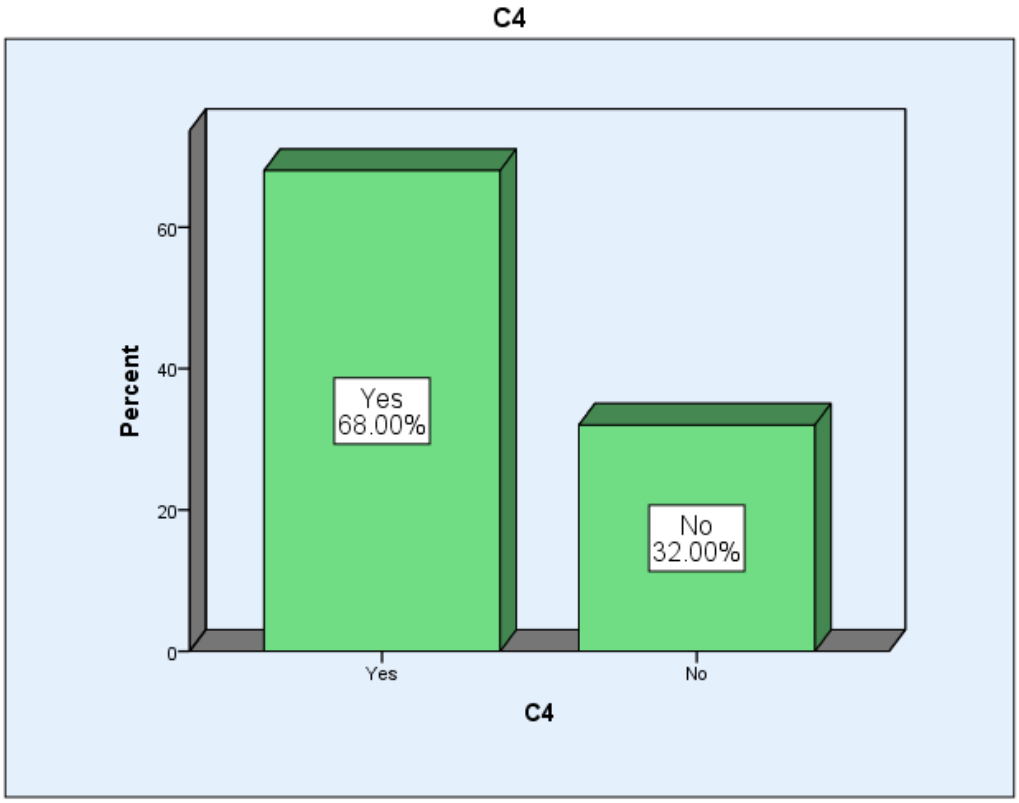


Source: field survey 2016

The findings tell us that most people would choose privacy over convenience but it remains to be seen whether these sentiments are actually reflected in their online behaviour with the responses to the terms and conditions questions negate these sentiments.

Figure 4.9: Do you like/share or join pages on social media for a chance to win giveaways?

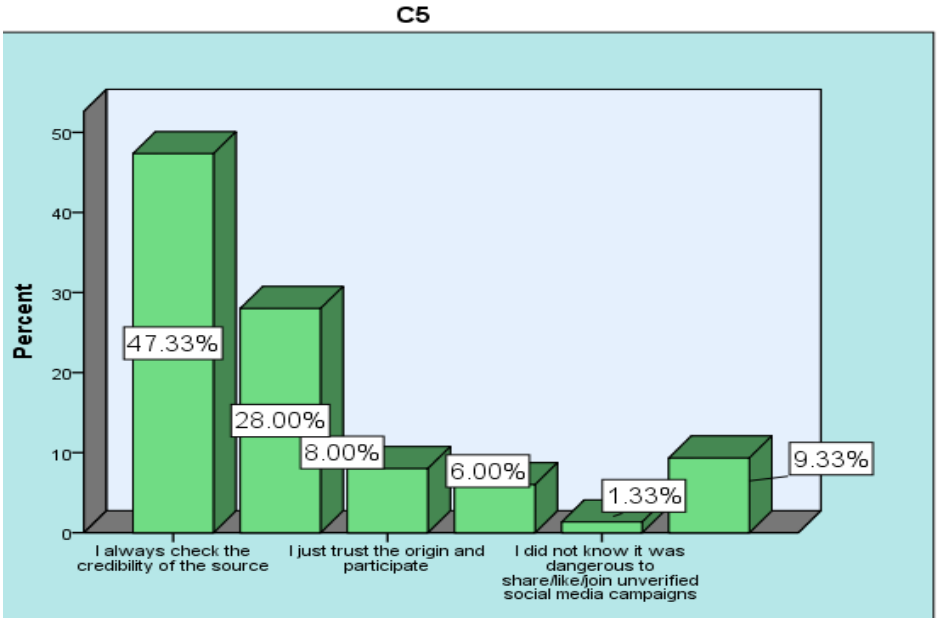
The respondents were asked if they ever joined or liked pages in order to win and if they verified authenticity and the responses were as below.



Source: field survey 2016

A majority said yes, making them highly susceptible to phishing. The reasons they gave were as per figure 4.10 below.

Figure 4.10: Circumstances under which you like/share or join pages on social media for a chance to win giveaways



Source: field survey 2016

Majority of the respondents claimed they checked the source and authenticity of the pages. With very few people saying that they did not know the dangers of not verifying sources authenticity.

4.5.7 Which threats to Privacy and Security online are you aware of?

The respondents could all name some actual threats to security and privacy online, with over three quarters naming at least 4 threats as per table below.

Table 4.5: Type of Security Threats online

Type of Security Threats online	Percentage of respondents who knew them
Identity Theft	77%
Phishing	77%
smartphone sharing/tracking your online habits	77%
banking fraud	73%
Other	5%

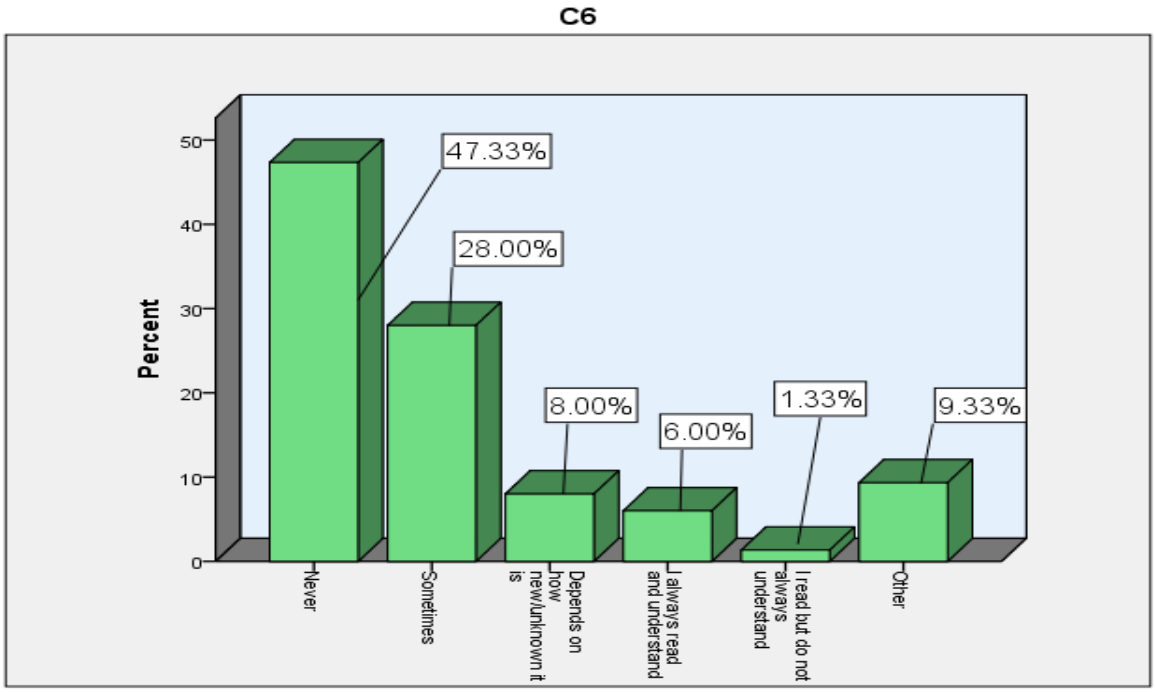
Source: field survey 2016

4.6 Changes in Behaviour of Respondents to Safeguard their Security Online

4.6.1 Do you read terms and conditions before joining a social networking site?

In sharp contrast to the opinions above none of the respondents, when asked, read and understand the terms and conditions of joining SNSs or downloading Apps. Less than half i.e. 45% of the respondents said that they read them sometimes. In the focus group discussions, respondents said that they did not read them because billions of people were already subscribed and they were no different. One respondent specifically said 'what will I do argue with Facebook? I am only one customer out of billions.' Only one focus group respondent had an opposing view saying that if we all read the terms and highlighted concerns, we would be heard by big corporations. The actual responses are as follows:

Figure 4.11: Reading terms and conditions on social networks



Source: field survey 2016

4.6.2 Reacting to Security Threats online

Respondents were asked how they would respond to their social media accounts being breached/hacked or compromised and the responses were as follows:

Table 4.6: Responding to breaches on social media

Change passwords	**55%**
Deactivate account	27%
Contact and inform service provider	9%
inform all you friends on site to create awareness	9%

Source: field survey 2016

Some of the FGD respondents were incredulous as to why anyone would even bother to hack such 'trivial' things as their Facebook account and said their Social Media accounts held nothing highly sensitive. One respondent argued that the worst thing that could happen was they (hackers) may post embarrassing content but nothing very damaging.

4.6.3 Dealing with breached/compromised Smart Phones

Similarly, 45% of the respondents said that if their handsets were breached/ hacked or compromised they would change passwords and 41% wipe device memory. Other reactions are tabulated below. On both social networks and smartphones, the most popular reaction was to change passwords.

Table 4.7: How Respondents respond to Smart phone breaches

Change passwords	**45%**
Wipe device memory	41%
Contact manufacturer	5%
I don't know what to do	3%
Install security Apps	6%

Source: field survey 2016

The focus group discussion further explored the ideas of reacting to a compromised smart phone and several respondents were more concerned about people around them getting access to their messages and Mobile banking history than any virtual access such as hacking. They argued that 'financial information and other material were more dangerous when accessed by spouses, family members and friends around you than by a hacker in China'.

4.7 Change in Social Media Habits derived from Privacy and Security Concerns

There were several things that respondents said they did to protect their privacy. 65% said that they only followed or accepted friend requests from people they personally knew well. Another 35% never post personal photos and their locations on social media. In the focus group, the respondents had varying responses; some maintain 2 profiles on major sites such as Facebook to separate acquaintances from friends and family. Some respondents argued that posting photos or details of their children was totally off limits.

Most of the respondents said they restricted who could view their information to friends only and that they reviewed all posts and tags before they could appear on their profiles. At the focus group one respondent said that all his devices were additionally password protected and he only posted in closed groups on social media.

Table 4.8: Specific Measures Undertaken to ensure Privacy and Security on SNS

Ways in which respondents have changed online behaviour due to security and privacy concerns	Percentage of Respondents
I follow / accept friend requests from people I know well (outside cyber space)	65
I never post personal photos/events/details on social media	35
I simply view / read / follow posts but never post anything myself	30
My social media accounts have strict security settings and my profile cannot easily be seen	25
I am friends with anyone who sends me a request	25
I am not sure what my security settings on social media are	5
I have not secured my profiles and anyone who searches can view all my posts	5

Source: field survey 2016

These findings show that security measures among social media and smart phone users are still lax in comparison to how much they know about the threats to their privacy. The reasons could be carelessness, not knowing the real life impact of these threats as well as trivialising online threats as minor with no actual losses incurred from them. The reasons listed under other measures taken show that a minority have taken strict measures to ensure that their privacy is protected. Only 5% of the respondents, for instance, actually install security Apps on their smartphones with reasons mostly based on possible data loss and not actual concern for breach as per the discussions of the FGD.

4.7.1 Have the respondents taken any measures to protect their privacy on smart phones and social media?

Respondents when asked if they read terms and conditions when downloading or installing Apps and joining Social networks had the following responses:

Table 4.9: Reading Terms and Conditions on downloading Apps

	Smartphone Apps %age	Social Networks %age
Never	36	23
Sometimes	36	32
Depends on how well known it is	28	18
I always read and understand	0	27
I read but don't always understand	0	0

Source: field survey 2016

There are more respondents reading terms and conditions when joining SNSs than there are downloading Apps, implying that either Apps have more complex terms or their impact on security is either not known or is dismissed. The other explanation is that we may be downloading smart phones so frequently that we have become less vigilant while social networks are joined less frequently and a more conscious decision is required to sign up. Respondents were also asked if they read terms and conditions before signing up or joining social networking sites and none of the respondents read terms and conditions all the time. 45% of the respondents said that they read them sometimes.

CHAPTER FOUR

DATA ANALYSIS AND DISCUSSION OF FINDINGS

5.1 Overview

This chapter summarizes key findings of the study and conclusions drawn from those findings. It also gives recommendations that can be employed by the general public, policy makers and other scholars in regards to social media, areas of further academic study and key industry players in smart phones and Social networking.

5.2 Summary

The study sought to find out what security and privacy challenges university students were aware of and how they dealt with them. The study objectives were: i) To establish the level of awareness on privacy and security threats among social media and smart phones users. ii) To identify the privacy and security challenges that Smart phone users on social media are experiencing, iii) To determine the extent to which privacy and security concerns influence online behaviour. The instruments employed to gather data were questionnaires and focus group discussions. Close analysis of qualitative data was done and key data pertaining the objectives of the study derived from responses. The quantitative data collected was coded and keyed in the statistical package for social science (SPSS). The results were later analysed and presented in clear ways to reflect findings of the study. The qualitative data was then used to explain, expound, clarify and justify the answers respondents gave in the quantitative findings. The study showed that all respondents used several social media and that they had some awareness of security challenges. It was apparent that the security measures employed are lax and that most social media users found terms and conditions too complex.

5.3 Summary of Key findings of the Study

Majority of the respondents (over 77%) know that there are threats to their privacy lurking on social networks and smart phone Apps, at least in theory, they however have not done much in the way of attempting to secure their information in that only 45% read terms and conditions sometimes with 0% reading them all the time. This is partly because the legalese is complex and long or because they feel helpless against the sheer magnitude of the Social media corporations, some complacency is just due to negligence i.e. they know they should worry but they do not, because they have yet to see the impact on their lives outside cyber space. Given that the study focused on perceptions of the elite, it is implied that all the findings may vary if the study was repeated and focused on people with even less education and resources. In summary, the study found that:

A majority of the respondents know that there are threats to privacy and security online with over three quarters knowing at least identity theft, phishing and banking fraud.

Most of the respondents also say they prioritise privacy over convenience online but none of them consistently read terms and conditions of any SNS or smart phone Apps. In addition, a significant number of them do not verify authenticity of sites and pages before joining them.

Although three quarters of them have taken small measures to preserve privacy on SNs and smartphones, the changes have been minor (such as restricting friend lists).Only a minority (5%) have actually installed anti-malware or other security Apps to safeguard their information online.

Knowledge of the threats seems hypothetical as all findings point to some knowledge but little or no impact on behaviour of respondents.

5.4 Conclusion of the study

There is a clear need to focus on consumer education on impact of loss of privacy on SNS and smartphones in Nairobi. The largely analogue institutions may mean that our digital foot print has not fully impacted on our day to day lives. Nairobi residents are theoretically concerned about their privacy and security on Social networks but have not actualised these concerns into actual actions. The objectives of the study were: i) to establish the level of awareness on privacy and security threats among social media and smart phones users. ii) to identify the privacy and security challenges that Smart phone users on social media are experiencing, iii) to determine the extent to which privacy and security concerns influence online behaviour.

It comes out clearly that Kenyan social media users are vulnerable to exploitation of private information. There are mainly two reasons for this. First, the Kenyan government has not taken adequate steps in addressing the problem of private online security and cybercrime. Secondly, there is rapid increase of smartphone users and reliance on the Internet. The current study was able to help the researcher close security gaps on social networking sites. Potentially, Nairobi university students and Kenyans at large will be more aware of potential threats through user awareness initiatives. Users of smartphones will be made aware of security and privacy problems and potentially, this study will influence behavior.

In the modern day, using Smartphones and social media sites have grown to be a major part of human lives. Some of the most common sites include Twitter, Facebook, Instagram and Pinterest. Social media is solely based on the model that users do not know the perceived value of the shared information. To be precise, an organization like Facebook generates income since users of Facebook value private information less than offered services. This user's point of view is proportionate to their opinion of privacy.

The current study findings are vital since they can assist in controlling cyber-crimes and impacting or reinforcing policy.

The conclusions were that there is a fair amount of awareness of the privacy and security threats by at least 75% of the respondents they know there are threats to privacy and security online. This should be examined further in future studies to see if users follow through on their convictions with corresponding actions.

The major threats known to respondents are: identity theft, banking fraud and phishing but there has been no major impact on behaviour Of SNS and smartphone users. Three quarters of all the respondents said they would prioritise privacy over convenience online but subsequent questions in the focus group discussion contradicted these claims. This supports Rainie & Janna Anderson, (2014) who found that humans have showed that they can compromise on giving away private info for even a free cup of tea.

There are no major changes to respondents' behaviour with only 6% installing security apps to safeguard their devices, in spite of the reports by Norton-Symantec highlighting that 36% of Android Apps are greyware and another 17% being malicious. None of the respondents consistently read terms and conditions on either installing Apps or joining social networks.

The study could neither confirm no contradict findings of a PEW internet research that established females were more conservative with Social media security settings as the sample was fairly gender balanced. But having 75% of the respondents on multiple social networks and none of the respondents saying they were not on any SNS is in line with another PEW 2014 study that argued that younger, higher educated English speaking Kenyans were more likely to be on social media and use smart phones. (Strydom, 2016)

5.5 Recommendations from the study

In order for more Kenyan residents to pay attention, there is a need for more education and awareness of the impact of our digital footprint on financial, personal and professional lives. They know that privacy and security threats online are bad but have not really seen or felt the impact in our lives except maybe on mobile money fraud.

The industry players in smart phones and Social networking should work to raise awareness for users and to simplify terms and condition, our college educated members of society have difficulty interpreting and it could be much worse for those with even less education.

The main stream media could raise awareness by highlighting incidents of cybercrime linked to lax security measures online and the legal implications of any persons caught committing cybercrimes. The authorities in cyber security could be engaged on this issue.

Policies should be put in place to ensure Social Networks and App manufacturers openly disclose data mining and sharing practices. There is also a need to simplify terms and conditions for all users to understand.

The law enforcement agencies in the country should be more open to following up cybercrimes and treating cybercrime just as seriously as they do other crimes. If citizens were to see these issues as real crimes they might take the threats more seriously.

5.6 Suggestions for further research

I. Since the study sought to assess awareness of security and privacy concerns for social media and smartphones in Nairobi a future study should integrate more Nairobi residents as this views were limited to college educated young adults.

II. Another area of study could assess the impact or harm that has actually occurred due to loss of privacy on social media perhaps a case study of actual victims/cases.

III. There is also a need to study this issue from the perspectives of experienced cyber security experts with in depth knowledge of the subject and to use this to create awareness and educate the public.

IV. Future studies could incorporate an aspect of cross-checking user opinions with their social media profiles to assess the level of discrepancy more accurately.

REFERENCES

Albrechtslund, A. (2008). Online Social Networking as Participatory Surveillance. First Monday, 13(3). doi:10.5210/fm.v13i3.2142Analysis, M. (2016). FIRST QUARTER SECTOR STATISTICS REPORT FOR THE FINANCIAL YEAR 2015 / 2016, *2016*(September 2015), 1–28.

Bash, E. (2015). No Title No Title. *PhD Proposal*, *1*, 1–34. http://doi.org/10.1017/CBO9781107415324.004

Chennamaneni, A., & Taneja, A. (2015). Communication Privacy Management and Self-Disclosure on Social Media - A Case of Facebook, 1–11.

Conole, G., Galley, R., & Culver, J. (2011). Frameworks for understanding the nature of interactions, networking, and community in a social networking site for academic practice. *International Review of Research in Open and Distance Learning*, *12*(3), 119–138. http://doi.org/10.1111/j.1083-6101.2007.00393.x

Communications Authority of Kenya. (2014). Quarterly Sector Statistics Report. First quarter of the financial year 2014/15. Retrieved 4February 2016 from http://www.ca.go.ke/images/downloads/STATISTICS/Sector%20Statistics%20report%2 0Q1%202014-2015.pdf

E-guide, D. L. (n.d.). How To Claim Your Certificate, 2014.

Ellison, N. B., & Boyd, D. M. (2013). Sociality through social network sites. *The Oxford Handbook of Internet Studies*, 151–172. http://doi.org/10.1093/oxfordhb/9780199589074.001.0001

Ephraim, P. . (2003). African youths and the dangers of social networking: a culture-centered approach to using social media. *Ethics and Information Technology*, *15*(4), 275.

Ephraim, P. E. (2013). African youths and the dangers of social networking: a culture-centered approach to using social media. Ethics and Information Technology, 15(4), 275-284.

GoK-CCK. (2010). Quarterly Sector Statistics Report - Kenya. *Communications Commission of Kenya*, *4th Quarte*, 1–17.

http://doi.org/10.1109/TPAMI.2004.1265723

Gummadi, K., Krishnamurthy, B., & Mislove, A. (2013). Addressing the privacy management crisis in online social networks. *WWW (Companion Volume)*. Retrieved from https://www.iab.org/wp-content/IAB-uploads/2012/01/alan_mislove.pdf

Guo, C., & Wang, H. J. (2007). Smart-Phone Attacks and Defenses. *Microsoft Research*, 1–6. Retrieved from research.microsoft.com

International Telecommunication Union. (2015). INTERNET SECURITY THREAT REPORT INTERNET SECURITY THREAT REPORT 2015, 20(April). *ISTR*, *20*(April).

Joinson, A., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, Trust, and Self-Disclosure Online. *Human-Computer Interaction*, *25*(1), 1–24. http://doi.org/10.1080/07370020903586662

Kelly, H. (2014). Survey: Will we give up privacy without a fight? Retrieved from http://edition.cnn.com/2014/12/18/tech/innovation/pew-future-of-privacy/

Kiboi, B. N. (2015). CYBER SECURITY AS AN EMERGING THREAT TO KENYA ' S by, (May).

Kichatov, V. (2010). MASTER ' S THESIS Social Media as a Promotional Tool - a Comparison between Political Parties and Companies. *Case Analysis*, 47. Retrieved from http://epubl.ltu.se/1402-1552/2010/055/index-en.html

Koopman, C. (2008). Networked Publics: Publicity and Privacy on the Internet, 125–134. Retrieved from http://publicsphereproject.org/events/diac08/proceedings/11.Networked_Publics.Koopman.pdf

Limited, S. (n.d.). Democratising Data, 41. Retrieved from https://www.safaricom.co.ke/annualreport_2015/downloads/DEMOCRATISING-DATA.pdf

Kamberelis, G., & Dimitriadis, G. (2005). Focus groups: strategic articulations of pedagogy, politics, and research practice. Handbook of qualitative research, 875-895.

KNBS, ICF. (2010). Macro: Kenya Demographic and Health Survey 2008-09.Calverton, MD: Kenya National Bureau of Statistics and ICF Macro, 430.

Kombo, D.L. and L.A. Tromp, (2006).Proposal and Thesis Writing: An Introduction. Pauline Publications. Nairobi, Kenya.

Macharia, M. (2015). Kenya leads the way in technology adoption. Retrieved 22 February 2016 from http://cajnewsafrica.com/2015/01/29/kenya-leads-the-way-in-technology-adoption/

Madden, M. (2012). Privacy management on social media sites. *Young*, 20. Retrieved from http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx Managing internet security. (n.d.).

Neuman, W. Lawrence. 2003. Social Research Methods: Quantitative and Qualitative

Approaches. New York, NY: Ally and Bacon.

Östman, J. (2012). Information, expression, participation: How involvement in user-generated content relates to democratic engagement among young people. New media & society, 14(6), 1004-1021.

Opil, B. (2014). Cyber crime – protect yourself. *MSAFIRI*. Retrieved from http://www.msafirimag.com/wp-content/uploads/CyberCrime.png

Petronio, S. (n.d.). Communication Privacy Management Theory, 168–180.

Petronio, S., & Durham, W. T. (2008). Communication Privacy Managment Theory: Significance for Interpersonal Communication. *Engaging Theories in Interpersonal Communication*, 335–347.

Rainie, L., & Janna Anderson. (2014). Digital Life in 2025: The Future of Privacy: the future of privacy. *PEW Research Center*, (December). Retrieved from http://www.pewinternet.org/2014/12/18/future-of-privacy/

Rainie, L., Kiesler, S., & Madden, M. (2013). Anonymity , Privacy , and Security

Online.

Rose, K., Eldridge, S., & Lyman, C. (2015). The internet of things: an overview, (October), 53. Retrieved from http://www.internetsociety.org/doc/iot-overview

Sarah Lynch, Allee Manning, and L. M. (2016, January). Americans Willing To Give Up Privacy Online For Convenience. *VOCATIV*. Retrieved from http://www.vocativ.com/271029/pew-survey-digital-privacy-online/

SHAHONYA, E. (2012, March 27). CCK considers monitoring to curb rising cybercrime. *Daily Nation NATION*. Nairobi. Retrieved from http://www.nation.co.ke/lifestyle/smartcompany/CCK-considers-monitoring-to-curb-rising-cybercrime-/-/1226/1373996/-/443y1lz/-/index.html

Smith, T. (2009). The social media revolution. *International Journal of Market Research*, *51*(4), 559–561. http://doi.org/10.2501/S1470785309200773

Strydom, T. (2016). Facebook rakes in users in Nigeria and Kenya, eyes rest of Africa. Retrieved from http://www.reuters.com/article/us-facebook-africa-idUSKCN0RA17L20150910

UN-Habitat. (2014). State of African Cities 2014. Retrieved 23 February 2016 from http://unhabitat.org/the-state-of-african-cities-2014.

Westlake, E.J. "Friend Me If You Facebook: Generation Y and Performative Surveillance." TDR: The Drama Review 52.4 (2008): 21–40.

Zhao, J., Binns, R., Kleek, M. Van, & Shadbolt, N. (2016). Privacy Languages : Are we there yet to enable user controls ? Expression of Privacy Preferences, 799–806. http://doi.org/http://dx.doi.org/10.1145/2872518.2890590

APPENDICES

APPENDIX 1: ONLINE PRIVACY AND SECURITY QUESTIONNAIRE

This is a questionnaire for an academic study on the management of security and privacy concerns by smart phone .The information that you provide here will be held in utmost confidentiality and will be used for purposes of this academic study only. Please tick in the box or fill in your response where applicable.

SECTION ONE: DEMOGRAPHICS

1. Gender

Male		Female	

2. Age

(a) 18 to 21 years **(b)** 21 to 25 years **(c)** 25 to 29 years **(d)** 30 to 35 years

3. What faculty/school/department/institute are you in?_____

4. What course/programme are you pursuing?

(a) Bachelor's degree **(b)** Master's Degree (**c)** Doctorate (**d)** Other_____

SECTION TWO: PATTERNS OF GENERAL SOCIAL MEDIA USAGE

1. Which of the following social networking sites are you on? (Tick all that apply)

(a) Facebook **(b)** Twitter **(c**) WhatsApp (**d)** Instagram **(e)** Google+ **(f)** Pinterest

(g) YouTube **(h)** LinkedIn **(i)** Tumblr **(j)** Reddit **(f)** Flickr **(g)** Vine

(h) Other _____

2. What is your primary access channel for accessing social networking sites

(a) Desktop Computer **(b)** Laptop Computer **(c)** Smartphone **(d)** Tablet **(e)** iPad

(f) Phone (non-smart phone) **(g)** Other _____

3. What device do you often use to share/post or upload content

(a) Desktop Computer **(b)** Laptop Computer **(c)** Smartphone **(d)** Tablet **(e)** iPad

(f) Phone (non-smart phone) **(g)** Other _____

3 *(ii)* Why is this preferred device/channel for sharing/uploading content, such as photos, videos?

(a) Ease of use (user friendly) **(b)** Convenience, most easily available **(c)** Accessibility it is the only device I have **(d)** Other (explain)

_____

_____

____

4. How often do you use social media sites/apps?(Tick where applicable)

Daily		Thrice a day	Twice a week	Once a week	Every 2 weeks	Once a month	Never

5. How much time do you spend online in a typical day whether through desktop, home or laptop computer and mobile devices?

0-1 Hours	1-2 Hours	2-3 hours	3-4 hours	More than 4 hours	Never	Varies from day to day

6. How many hours do you spend on social networking sites on a typical day? (Tick where applicable)

0-1 Hours	1-2 Hours	2-3 hours	3-4 hours	More than 4 hours	Never	Varies from day to day

7. What do you use your social media accounts for (select all that apply)

(a) To keep up with friends that I actually know well in person

(b) To stay connected with people with interests similar to mine (known and unknown)

(c) To stay in touch with family and friends who are not always nearby

(d) To share and follow issues of social-political significance

(e) To conduct business online

(f) To share content that I have created

(g) To keep up with trends and news

SECTION THREE: AWARENESS OF SECURITY ONLINE

1. In general, how concerned are you about security on the Internet? (e.g unauthorised people reading your email, finding out what websites you visit, etc.) Keep in mind that "security" can mean **privacy**, **confidentiality**, and/or **proof of identity** for you or for someone else.

(a) Not at all concerned **(b)** A little concerned **(c)** Somewhat concerned

(d) Very concerned **(e)** I know I should be concerned, but I'm not

2. Which threats to online privacy and security are you aware of?

(a) Phishing (***the activity of defrauding an online account holder of financial information by posing as a legitimate organisation***.) **(b)** Identity theft **(c)** Profile cloning **(d)** Banking fraud **(e)** Smart phones sharing/recording/tracking your online habits **(f)** Other _____

3. In general, which is more important to you: CONVENIENCE or PRIVACY?

(a) Convenience **(b)** Privacy

5. Do you like/share or join pages on social media for a chance to win giveaways?

(a) Yes **(b)** No

6. If yes, to question 4 above, under which circumstances?

(a) I always check the credibility of the source **(b)** I verify the origin/source

(c)I just trust the origin and participate **(d)** I don't care about origin/authenticity

(e) I did not know it was dangerous to share/like/join unverified social media campaigns

(f) Other _____

8. Do you read terms and conditions before joining a social networking site

(a) Never **(b)** Sometimes **(c)** Depends on how new/unknown it is **(d)** I always read and understand **(e)** I read but do not always understand **(f)** Other_____

9. Please provide a reason for your answer in question 7 above_____

10. Do you read terms and conditions before downloading/installing apps into your smartphone

(a) Never **(b)** Sometimes **(c)** Depends on how new/unknown it is

(d)I always read and understand **(e)** I read but do not always understand

(f) Other _____

11. Please provide a reason for your answer in question 9 above_____
____

---

11. Do you read/are you concerned about permissions that apps require to work on your smart phone?

(a) Yes **(b)** No **(c)** I don't know what this means **(d)** Sometimes

12. Have you changed/modified your behaviour on social networks in any way to preserve your privacy and safeguard your security?

(a) Yes **(b)** No

13. In which ways has your online behaviour been influenced by privacy and security concerns/fears

_____

_____

_____

14. To what extent are security features a factor in your choosing whether to join/like/follow a social networking site or download an app on your smartphone?

(a) No extent at all (**b)** To a small extent (**c)** To a significant extent (**d)** To a very great extent

15. What specific issues have you experienced/observed on social media or smart phones that were a threat to your privacy or security?_____

_____

__

16. Which specific measures would you undertake to preserve you privacy and safeguard your information on social media and smartphones_____

_____

_____

_____

17. How would react/ respond if your social networking accounts were breached/attached/hacked/compromised.

(a) Deactivate account **(b)** Change passwords **(c)** Contact and inform service provider

(d) Inform all you friends on the site to create awareness **(e)** ignore the issues

(f)I don't know what to do **(g)**
Other_____

18. How would you respond/react if your smartphone was breached/attacked/hacked/compromised,

(a) Wipe device memory **(b)** Change passwords **(c)** Contact and inform service provider or manufacturer **(d)** Switch off device **(e)** Install security apps

(f)I don't know what to do **(e)**
Other_____

19. Which of the following statements best describe your online behaviour in regards to social networking sites

(a) I carefully read and understand the terms and conditions as well as information sharing policies of all sites I join

(b) I follow/accept friend requests from people I know well(outside cyber space)

(c) I am friends with anyone who sends me a request

(d) I never post personal photos/events/details on social media

(e) I simply view/read/follow posts but never post anything myself

(f) My social media accounts have strict security settings and my profile cannot easily be seen

(g) I have not secured my profiles and anyone who searches can view all my posts

(h) I am not sure what my security settings on social media are

(i) Other_____
_

APPENDIX 2: CERTIFICATE OF FIELD WORK

UNIVERSITY OF NAIROBI
COLLEGE OF HUMANITIES & SOCIAL SCIENCES
SCHOOL OF JOURNALISM & MASS COMMUNICATION

Telegram: Journalism Varsity Nairobi
Telephone: 254-02-3318262, Ext. 28080, 28061
Director's Office: 254-02-2314201 (Direct Line)
Telex: 22095 Fax: 254-02-245566
Email: director-soj@uonbi.ac.ke

P.O. Box 30197-00100
Nairobi, GPO
Kenya

REF: CERTIFICATE OF FIELD WORK

This is to certify that all corrections proposed at the Board of Examiners' meeting held on 15/06/2016 in respect of M.A/Ph.D final Project/Thesis defence have been effected to my/our satisfaction and the student can be allowed to proceed for field work.

Reg. No: K50/76008/2014

Name: GATHUA MERCY NYOKABI

Title: THE MANAGEMENT OF SECURITY AND PRIVACY CONCERNS BY SMART PHONE AND SOCIAL MEDIA USERS IN NAIROBI

SUPERVISOR	SIGNATURE	DATE 25/7/16
ASSOCIATE DIRECTOR Dr Sam Sunigi	SIGNATURE	DATE 27/7/16
DIRECTOR	SIGNATURE/STAMP	DATE 11/11/2016

UNIVERSITY OF NAIROBI DIRECTOR 11 NOV 2016 SCHOOL OF JOURNALISM & MASS COMMUNICATION

APPENDIX 3: CONSENT TO PARTICIPATE IN FOCUS GROUP

You have been asked to participate in a focus group sponsored by a UON postgraduate student in the School of Journalism. The purpose of the group is to try and understand the security and privacy concerns that social media and smart phone users have and how they deal with them purely for academic purposes. The information learned in the focus groups will be used for academic purposes to further understand social media and smart phone use and how they relate to issues of privacy and security. You can choose whether or not to participate in the focus group and stop at any time. Although the focus group will be tape recorded, your responses will remain anonymous and no names will be mentioned in the report. There are no right or wrong answers to the focus group questions. We want to hear many different viewpoints and would like to hear from everyone. We hope you can be honest even when your responses may not be in agreement with the rest of the group. In respect for each other, we ask that only one individual speak at a time in the group and that responses made by all participants be kept **confidential.** We will also require a brief demographic overview of all our participants.

Gender

Male		Female	

Age

- 18 to 21 years
- 21 to 25 years
- 25 to 29 years
- 30 to 35 years

What faculty/school/department are you in?

_____

What course/programme are you pursuing?

- Bachelor's degree
- Master's Degree
- Doctorate
- Diploma
- Certificate

I understand this information and agree to participate fully under the conditions stated

above: Signed: _____

Date:_____

APPENDIX 4: CERTIFICATE OF CORRECTIONS

UNIVERSITY OF NAIROBI
COLLEGE OF HUMANITIES & SOCIAL SCIENCES
SCHOOL OF JOURNALISM & MASS COMMUNICATION

Telegram: Journalism Varsity Nairobi
Telephone: 254-02-3318262, Ext. 28080, 28061
Director's Office: 254-02-2314201 (Direct Line)
Telex: 22095 Fax: 254-02-245566
Email: director-soj@uonbi.ac.ke

P.O. Box 30197-00100
Nairobi, GPO
Kenya

REF: CERTIFICATE OF CORRECTIONS

This is to certify that all corrections proposed at the Board of Examiners meeting held on M.A in respect of M.A/PhD. Project/Thesis Proposal defence have been effected to my/our satisfaction and the project can now be prepared for binding.

Reg. No: K50/76008/2014

Name: Mercy Nyokabi Gathua

Title: The Management of Security and Privacy Concerns by Smart phone and Social Media Users in UON

SUPERVISOR	SIGNATURE	DATE 12/11/2016
Dr Samuel Siringi ASSOCIATE DIRECTOR	SIGNATURE	DATE 11/11/2016
DIRECTOR	SIGNATURE/STAMP	DATE 11/11/2016

UNIVERSITY OF NAIROBI DIRECTOR 11 NOV 2016 SCHOOL OF JOURNALISM & MASS COMMUNICATION

APPENDIX 5: PLAGIARISM REPORT

Turnitin Originality Report

THE MANAGEMENT OF SECURITY AND PRIVACY CONCERNS BY SMART PHONE AND SOCIAL MEDIA AMOUNG UNIVERSITY STUDENTS IN NAIROBI by Mercy Nyokabi

From Mass media and Technology (MA Comminication theory)

- Processed on 03-Nov-2016 18:10 EAT
- ID: 731469972
- Word Count: 11247

Similarity Index
3%
Similarity by Source

Internet Sources:
1%
Publications:
0%
Student Papers:
2%

sources:

1 1% match (Internet from 26-Apr-2016)
https://ourinternet-files.s3.amazonaws.com/publications/no15.pdf

2 1% match (student papers from 27-Nov-2014)
Submitted to University of Pretoria on 2014-11-27

3 < 1% match (student papers from 19-Apr-2013)
Submitted to Corinthian Colleges on 2013-04-19

4 < 1% match (student papers from 29-Feb-2012)
Submitted to University of St. Gallen on 2012-02-29

5 < 1% match (Internet from 30-Sep-2014)
http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2011.01559.x/full

6 < 1% match (Internet from 07-Jul-2010)
http://www.wickedlocal.com/brewster/news/lifestyle/health/x362986744/LIVING-50-Networking-sites-keep-boomers-socially-active

7 < 1% match (Internet from 15-Aug-2012)
http://www.dit.ie/media/newsdocuments/2011/4%20O'Brien.pdf

UNIVERSITY OF NAIROBI
DIRECTOR
10 NOV 2016
SCHOOL OF JOURNALISM & MASS COMMUNICATION

APPENDIX 6: DECLARATION OF ORIGINALITY

UNIVERSITY OF NAIROBI

Declaration of Originality Form

This form must be completed and signed for all works submitted to the University for examination.

Name of Student Mercy Nyokabi Gathua

Registration Number K50/76008/2014

College Humanities and Social Sciences

Faculty/School/Institute Journalism and Mass Communication

Department _____

Course Name M.A. Communication Studies

Title of the work The Management of Security and Privacy Concerns by Smart Phone and Social Media Users in the University of Nairobi

DECLARATION

1. I understand what Plagiarism is and I am aware of the University's policy in this regard
2. I declare that this _____ (Thesis, project, essay, assignment, paper, report, etc) is my original work and has not been submitted elsewhere for examination, award of a degree or publication. Where other people's work, or my own work has been used, this has properly been acknowledged and referenced in accordance with the University of Nairobi's requirements.
3. I have not sought or used the services of any professional agencies to produce this work
4. I have not allowed, and shall not allow anyone to copy my work with the intention of passing it off as his/her own work
5. I understand that any false claim in respect of this work shall result in disciplinary action, in accordance with University Plagiarism Policy.

Signature _____

Date 11/11/2016

UNIVERSITY OF NAIROBI
DIRECTOR
11 NOV 2016
SCHOOL OF JOURNALISM & MASS COMMUNICATION

APENDIX 7: PEW 2014 FINDINGS

Young, Higher Educated and English Speakers More Likely to Access Internet

Adults who access the internet at least occasionally or own a smartphone

		By age:			By education:			By English language ability:		
	Total	18-34	35+	Diff	Secondary or more	Less than secondary	Diff	Speak or read English	Cannot speak or read English	Diff
	%	%	%		%	%		%	%	
Chile	**76**	98	62	+36	87	18	+69	96	64	+32
Russia	**73**	95	61	+34	--	--	--	92	63	+29
Venezuela	**67**	84	54	+30	91	55	+36	92	59	+33
Poland	**63**	95	51	+44	77	22	+55	96	43	+53
China	**63**	87	45	+42	88	42	+46	91	53	+38
Lebanon	**62**	94	41	+53	84	30	+54	90	31	+59
Argentina	**62**	85	48	+37	89	50	+39	91	44	+47
Colombia	**57**	80	44	+36	83	35	+48	89	42	+47
Malaysia	**55**	81	35	+46	72	19	+53	73	20	+53
Ukraine	**53**	84	39	+45	--	--	--	85	39	+46
Brazil	**51**	72	35	+37	78	28	+50	87	43	+44
Mexico	**50**	73	36	+37	81	26	+55	78	33	+45
Egypt	**50**	64	34	+30	81	30	+51	84	37	+47
Jordan	**47**	62	27	+35	75	16	+59	86	27	+59
Peru	**46**	70	31	+39	69	14	+55	85	33	+52
Thailand	**45**	83	27	+56	82	24	+58	71	18	+53
Vietnam	**43**	70	21	+49	75	20	+55	83	20	+63
Tunisia	**42**	66	25	+41	70	17	+53	71	14	+57
Philippines	**42**	64	23	+41	67	33	+34	--	--	--
South Africa	**41**	51	31	+20	64	19	+45	--	--	--
Nigeria	**39**	51	23	+28	51	10	+41	48	6	+42
Nicaragua	**38**	53	24	+29	71	19	+52	72	25	+47
El Salvador	**34**	53	19	+34	77	16	+61	79	22	+57
Kenya	**29**	35	22	+13	51	12	+39	36	3	+33
Senegal	**28**	37	18	+19	74	17	+57	65	12	+53
Indonesia	**24**	41	10	+31	43	11	+32	48	13	+35
Ghana	**21**	30	11	+19	32	5	+27	30	3	+27
India	**20**	30	12	+18	34	9	+25	35	8	+27
Tanzania	**19**	27	10	+17	--	--	--	41	5	+36
Uganda	**15**	20	8	+12	57	9	+48	23	2	+21
Bangladesh	**11**	15	6	+9	24	5	+19	17	5	+12

Note: For internet users, Pakistan excluded due to insufficient sample size. For education, Russia, Ukraine and Tanzania are excluded due to insufficient sample size. For English language ability, the Philippines and South Africa are excluded due to insufficient sample size for non-English speakers. Respondents who replied that they can speak or read some English, or took the survey in English were considered to have English language ability.

Source: Spring 2014 Global Attitudes survey. Q67, Q68 & Q69.