EFFECTS OF MOBILE APPLICATION SECURITY STRATEGIES ON PRIVACY INVASIONAMONGMOBILE SHOP OPERATORS INNAKURU EAST SUB-COUNTY, KENYA

ANGELA WANJIKU KIVINDYO

A Research Project Presented to the Institute of Postgraduate Studies of Kabarak University in Partial Fulfillment of the Requirements for the Award of the Master of Business Administration (Management Information Systems Option)

KABARAK UNIVERSITY

NOVEMBER, 2020

DECLARATION

1. I do declare that;
    a) This thesis is my own original work and to the best of my knowledge, it has not been presented for the award of a degree in any other university or college.
    b) That the work has not incorporated materials from other works or a paraphrase of such works without due and appropriate acknowledgment
    c) That the work has been subjected to the process of anti-plagiarism and has met Kabarak university 15% similarity index threshold.
2. I do understand that issues of academic integrity are paramount and therefore I may be suspended or expelled from the university or my degree may be recalled for academic dishonesty or any other related academic malpractices.

Signature ……………………………………… Date……....……………………..

Angela Wanjiku Kivindyo GMB/NE/0208/01/12

RECOMMENDATION

To the Institute of Postgraduate Studies: The research project entitled "Effects of mobile application security strategies on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya." and written by Angela Wanjiku Kivindyo is presented to the Institute of Postgraduate Studies of Kabarak University. We have reviewed the research project and recommend it be accepted in partial fulfillment of the requirement for award of the degree of Master of Business Administration (Management Information Systems Option).

Signature………………………………….. Date………………………….

Dr. Nelson Masese
School of Science, Engineering and Technology (SSET)
Kabarak University Kenya

Signature………………………………….. Date…………………………

Dr. John Kipkorir Tanui
Senior Lecturer, School of Business and Economics
Kabarak University Kenya

COPYRIGHT

@ 2019

Angela Wanjiku Kivindyo

All rights reserved. No part of this Project may be reproduced or transmitted in any form by means of either mechanical, including photocopying, recording or any other information storage or retrieval system without permission in writing form the author or Kabarak University.

ACKNOWLEDGEMENTS

I would like to extend my gratitude to the Almighty God for the gift of life, care and the opportunity to write this project. I also wish to acknowledge and sincerely thank the Institute of Postgraduate Studies, Kabarak University especially my supervisors Dr. Nelson Masese and Dr. John Kipkorir Tanui for their time, unrelenting academic and scholarly support that has led to the successful completion of this research project.

DEDICATION

This research work is dedicated to my family members for their prayers and support.

ABSTRACT

Privacy invasion is an offence perpetrated by availability, access, and use of advanced mobile devices when they land in the wrong hands of people who have the intention of infringing into the space of either individuals or organizations. There have been many incidences of infringement on people's privacy by exposing their personal lives to third parties and the general public, a factor which is associated with detrimental effects. The study sought to integrate mobile application security strategies as a measure towards curbing privacy invasion. The general objective was to evaluate the effects of mobile application security strategies on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya. The specific objectives were; to examine data encryption, advanced software testing techniques, risk analysis, and privacy settings on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya. The study was guided by the technology acceptance model, restricted access or limited control theory of privacy, control theory of privacy, and seclusion theory of privacy. The study adopted a cross-sectional research design, and was carried out in Nakuru East Sub-County, Kenya. The units of observation were mobile shops within Nakuru town, while the units of analysis were operators of mobile shops. According to Nakuru East Sub-County Business Register (20 9), there are 221 mobile shops within Nakuru town. The researcher used Purposive sampling method to select respondents (Operators) from each of the 221 mobile shops. Nassiuma's (2000) formula was used to determine the sample size of 70 operators of mobile shops. The study used structured questionnaires to facilitate data collection. The pilot study was conducted in Eldoret town's Central Business District where questionnaires were issued out to 7 selected operators of mobile shops. The collected data was analyzed with the aid of the Statistical Package for Social Sciences. Descriptive statistics encompassing frequencies, percentages, means and standard deviations were used in the analysis. In addition, inferential statistics such as correlation and multiple regression analysis were used. The results of the study revealed that there was a negative and statistically significant correlation between data encryption and privacy invasion of the mobile users in Nakuru town. The results of the study further revealed that there was a negative and statistically significant correlation between advanced software testing techniques and privacy invasion. The results of the correlation analysis further indicated that better risk analysis reduces cases of privacy invasion of mobile users in Nakuru town. The results of the study revealed that a strong negative correlation existed between Privacy setting and privacy invasion. From the findings the study recommended that mobile shop operators within Nakuru East Sub-County should adopt data encryption security strategy because it allows protection of data that they do not want anyone else to have access to. The study further recommended that mobile shop operators should adopt advanced software testing techniques because they provide stakeholders with information about the quality of the software product or service under test

Key Words*: Advanced software testing techniques, data encryption, mobile application security strategies, privacy invasion, privacy settings, risk analysis*

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS AND ACRONYMS

AES	Advanced Encryption Standard
APPS	Applications
CBD	Central Business District
CTP	Control Theory of Privacy
DES	Data Encryption Standard
ENISA	European Union Agency Network
iOS	iPhone Operating System
KHRC	Kenya Human Rights Commission
MDS	Module Directory Services
MIS	Management Information Systems
MiTM	Man in the Middle
NACOSTI	National Commission of Science, Technology and Innovation
NCIC	National Cohesion and Integration Commission
NWCCC	National White Collar Crime Center
OS	Operating System
PAF	Principle Axis Factoring
RALC	Restricted Access and Limited
RSA:	Rivest-Shamir-Adleman
SPSS	Statistical Package for Social Sciences
TAM	Technology Acceptance Model

OPERATIONAL DEFINITION OF TERMS

Advanced Software Testing Techniques : These are tools or measures that are employed to gauge the capacity of a mobile device to mitigate privacy invasion (Agangiba & Agangiba, 2013). With regard to this study, advanced software testing techniques include identification test scenarios, experience-based testing, automated testing, and use case-based testing.

Challenges in combating privacy invasion: These are obstacles that users of mobile devices encounter in their attempt to maintain their solitude and confidentiality of the data or files held in their devices (Sampat & Prabhakar, 2017). In this context it implies to the problems mobile user face in ensuring that their confidentiality is maintained.

Mobile Applications: These are software designed to run on hand-held devices such as mobile phones, tablets, ipads, (Fouchier, 2016). In this context it refers to program installed in a mobile phone.

Mobile Application Security Strategies: It is a comprehensive security solution for mobile applications which run on mobile devices like tablets and smart phones56866 (Park, 2012). In this context it refers to the measures put in place to ensure the safety of application installed in mobile phones and tablets.

Privacy Invasion: This is described as infringement of an individual's right to personal information through intrusion of their solitude, publicizing of their personal issues, and also creating false information about them in an offensive manner (Parker, 2012) In this context it refers to unauthorized access of a mobile user personal information without his/her consent

Privacy Invasion Prevention Strategies: These are measures put in place with the view of putting intruders of personal data or information at bay. Such measures include encryption of data or files, and use of secure connections (Liu & Yao, 2017). The strategies include data encryption, advanced software testing techniques, risk analysis, and privacy settings.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Privacy invasion is a problem that affects millions of people and organizations globally. With the advent of mobile technology applications, the public all over the world are prone to privacy invasion. This is informed by the security of mobile applications which is sometimes infringed by external forces. Mobile applications (apps) are software designed to run on hand-held devices such as mobile phones and tablets of different caliber. The applications aid in sporting activities, gaming, social networking, combating crime and agriculture among others. According to Moore (2008), privacy is defined as a moral claim or condition on others to desist from certain activities. It is also perceived as a derivative notion which is founded on basic rights like liberty or property. Arguably, privacy is contested. This is premised of the assertion that, it is transformable due to the ever changing technological and social conditions (Mulligan, Koopman & Doty, 2016).

Privacy invasion is characterized by four distinct yet related torts. These are intrusion, private facts, false light, and appropriation. Intrusion involves infringing, physically or otherwise, on the solitude of another in a significantly offensive manner. Private facts are evidenced by publicizing of highly offensive private information of a certain person in spite of it not being of legitimate concern to the public. False light is publicizing false and highly offensive impression of another person. Lastly, appropriation is impersonating by use of another’s name or likeness with the view of getting some advantage without their consent (Moore, 2008).

Mobile application security strategy is defined as a comprehensive security solution for mobile applications which run on mobile devices like tablets and smartphones (Park, 2012). The object of mobile application security is to safeguard data of individuals and organizations that are stored in the aforementioned devices. The security of mobile applications entails how well the applications are protected from compromise by crackers, hackers and criminals. The developers of mobile applications use technologies and production practices that shield mobile apps from being hacked. Nevertheless, it is in the public domain that various applications have been hacked and the right to privacy breached. The rationale of hacking this software is to decrypt information and illegally obtain data for purposes of defamation or carrying out crime. Park (2012) adds that in reference to the attack points, attackers to access credentials, personal data, cardholder data, and also to sniff to the victim’s connections. Attack points include data storage, binary, and platform, which though not independent, they are interrelated.

1.1.1 Global Perspective of Mobile Application Security Strategies and Privacy Invasion

The security of mobile applications is paramount especially to users who transact online. If a mobile application is not properly encrypted, there may be breach of privacy with such information as credit card, passwords and other crucial company data being accessed by unauthorized persons. Indeed, Trust wave 2012 Global Security report affirms that there have been 300 data breaches in 18 countries around the world. It is further stated that most mobile platforms are targets for what is called banking Trojans. Statistics indicate that 29.6%, 10.5% and 7.6% of the mobile applications attacks are noted to come from the Russian Federation, the United States of America and Eastern Europe respectively (Park, 2012).

The rising trend in hacking activities is associated with mobile applications. Mobile applications that are not protected are prone to reverse-engineering, repackaging and republishing. A report filed in the United States posits that one third of mobile devices have medium to high risk of data exposure. Mobile devices with android set-up are twice likely to be attacked than those with iPhone Operating System(iOS) set-up because of the malware that they carry. IOS is a mobile operating system (OS) which was developed by Apple Inc. and was intended for its hardware exclusively. As such, mobile phone applications with android set-up are likely to expose company data that may destroy its reputation or perpetuate financial crime. This implies that mobile applications are not secure due to exposure of network threat that may manipulate the content being sent to or being relayed from the device (Mobile Threat Intelligence Report, 2016).

A global survey shows that the United Kingdom has the least number of mobile apps users such as Facebook and WhatsApp despite being one of the most saturated smart phone markets. The stated apps are used at 91.2% in most countries Fouchier *et al. (*2016). Other applications mostly used are mobile payments, online banking, and professional apps such as LinkedIn at 41.0%, 69.1% and 36.6% respectively. It is reported that the threat of mobile application data breach is real with banking and payment applications being the prime targets. Successful data breach give hackers an opportunity to get financial details, social network logins and mobile account details to the detriment of an organization or an individual. It is, therefore, important to use software development kits to make applications self-reliant and deal with the changing nature of malwares. This strategy would also enable adoption of layered approach to protection of mobile applications in order to avoid crackers and hackers Fouchier, *et al.*(2016).

In the present digital era, data and information is crucial to the survival of firms, military strategies and combating different forms of crime. Data leakage poses threat to financial and violent crimes. Data breaches have been on the rise and preventing data loss has been a daunting task for enterprises and individuals (Liu & Yao, 2017).

Australia has witnessed the upsurge of mobile phone handsets which is an opportunity for privacy invasion which, at times, borders on criminality. It is reported that there is hacking and/or stealing of mobile phones with the motive of accessing sensitive data. Despite the smart phones functioning as computers, security is an issue. These mobile phones are hacked with the intention of committing financial fraud and theft of identity. Indeed a report by Symantec shows that attackers have shifted their focus on mobile devices where they steal data through malware or smashing(Liu & Yao, 2017).

In the United States, hackers create malicious software to infect mobile devices (Mahoney & Pokorny, 2009). According to a report on cybercrime hackers are organized to carry out trans-national crime for profits (Cybercrime Inquiry Report, 2010). In India, it is noted that privacy invasion through cyber mobile increased by 54% in the year 2017. The cyber mobile attacks range from spamming, phishing, malware, network attacks to crypto miners. Some of the notable cyber-crimes on mobile device applications include phishing, which aims at gaining access to personal information using mobile phones and blue jacking whose rationale is to steal personal documents and information. It is further noted that such attacks are prevalent in the United States and China since most people have access to mobile devices such as smart phones and tablets (Mohankumar, Banuroopa & Sreevidhya, 2018).

According to the National White Collar Crime Center (NWCCC) report, the mobile applications used to access social sites have propagated privacy breach, especially in the developed world. The applications allow users to create online profiles regarding their daily chores and professional information. Unwarranted individuals may use the real-time information of the user for financial fraud. In the United States, particularly New Hampshire, thieves were able to steal wares while using Facebook application. Social engineering and phishing has been a gold mine for criminals. The Microsoft company reports that phishing attacks increased by over 1200% in the year 2010, while rogue software were found on 19 million personal computers in 2011. The offences range from impersonation to gain access of information and scam emailing (NWCCC, 2011).

1.1.2 Regional Perspective of Mobile Application Security Strategiesand Privacy Invasion

The advancement of Internet bandwidth to 3G and 4G cellular networks coupled with advanced mobile applications or platforms have enabled detecting and reporting of criminal activities. In Ghana, Agangiba and Agangiba (2013) proposed a mobile application solution to detect and report crime. The app architecture is the client server where on client side is a mobile running application. The information regarding criminal activities and crime perpetrators are fed into the server by the police and the general public using the app. The app would retrieve and provide real-time information about crime and criminal activities. In regard to the security and control of the system, there are restrictions to what information is available to the user category. However, despite the control, the question on data breach by spammers and hackers continue to linger.

It is stated that 8.8 million South Africans experienced cyber-crimes and privacy invasion between the year 2015 and 2016. Further reports indicate that 47% of smart phone users in the country experienced mobile cyber-crime in the year 2013, either by being robbed their money or by privacy invasion. The vulnerability of the mobile device applications and little concern on security put by manufacturers make it cheap for criminals to hack the mobile devices (Symantec Report, 2016).

Nigeria has also experienced criminal activities through mobile applications or web-based breaches. The most prominent cyber-crimes in the country include phishing, theft of data and airtime from service providers and email spamming that lead to loss of money and encroachment to privacy (Adebimpe, 2016).

1.13 Local Perspective of Mobile Application Security Strategies and Privacy Invasion

There is high penetration and usage of mobile applications in Kenya with a majority of mobile phone users using mobile banking applications to conduct financial transactions Luvanda *et al.* (2014).The security of mobile applications in Kenya is not different. Despite the mobile banking apps offering convenience in funds transfers, credit card information and withdrawals, there is a security threat from the Man in The Middle (MiTM). The MiTM can intercept messages to and from a mobile device in a public key exchange and then resend the messages using own public key (Chellegati, 2009). With regard to M-Pesa mobile payment platform, there has been public outcry due to fleecing and defrauding of innocent Kenyans via the platform. It is noted that, on average 13% of mobile banking users have lost money through this mobile platform. Most common security breaches come from the Trojan horse and Zeus malware in mobile banking apps (Luvanda*et al.*, 2014).

The security measures of mobile applications such as those that facilitate banking and cash transfer in Kenya are developed in obscurity. As such, these applications are easy target for hackers and crackers especially when they lose their obscurity. The banking and cash transfer applications carry security concerns such as deregistration spoofing, passive and active identity catching, network impersonation by encrypting suppression between the intruder and target user, and user impersonation. The weaknesses in the information security policy may compromise the security of the mobile applications in Kenya. This invokes the need of robust policies governing access to network elements and information assets especially for organizations (Chemwa, 2012).

Mobile device applications are critical in spurring growth of businesses by easing marketing of different goods and services in Kenya. Businesses customize mobile applications to aid in performing specific tasks. Despite these good tidings, mobile applications are prone to attack or breach. A survey conducted by Waithaka and Mnkanda (2017) shows that there are security challenges that affect the use of mobile applications in electronic commerce. The security concerns relate to access of important business information by third parties, loss of money to fraudsters and receiving fake news intended for fraud. The insecurity of mobile applications perpetrated by a clique of fraudsters hinders their effective use in e-commerce.

The value of information held within the information communication technology infrastructure motivates hackers. Though it is impossible to eliminate cyber-crime, organizations attempt to put security measures to deter the vice. Kenyans are obsessed with social media platforms such as Facebook, Twitter and WhatsApp which are rich fishing bays for criminals. Cases propagated by breach of such applications include defamatory postings on social media websites, cyber-bullying, mobile money fraud and hate speech (Kigen *et al.*, 2014).

It is evident from hitherto statistics, that security of mobile applications plays a part with regard toprivacy invasion. This is supported by the statistics that about 300,000 texts were intercepted by the National Cohesion and Integration Commission (NCIC) during the 2013's general election week. In spite of the Commission arguing that the said text contained hate speech, the entire issue bordered on privacy invasion (Kenya Human Rights Commission, 2014).

It is clearly reported that breach of the aforementioned security is a global challenge. The fact that there is a hypothetical link between mobile applications security and privacy invasion necessitates analyzing the extent to which the aforesaid security influences privacy invasion. This would subsequently enable relevant policy makers and practitioners especially in the field of management information systems (MIS) to formulate and implement measures of enhancing security of mobile applications with the view of mitigating privacy invasion.

1.2 Statement of the Problem

Just like the case of personal computers, the operating systems on which mobile devices run have their own risks or vulnerabilities and security issues. The continued ubiquity of mobile devices has obliged security experts to strive to develop mobile application security processes and solutions for the future. Ideally, mobile applications are supposed to be devoid of privacy invasion. However, this has not been the case. According to a global survey on Internet Privacy and Freedom of Expression, concerns have been raised with regard to the potential of invasive information technologies to violate women's privacy for sexual purposes, and also to violate 'enforced privacy' perpetuated by patriarchal cultures on women and girls (Mendel, Puddephatt, Wagner, Hawtin & Torres, 2012). Not only are the rights of women to privacy infringed on, but also those of men. Information technology has acted as a suitable platform through which privacy is invaded. It was reported by the Kenya Human Rights Commission (KHRC) that during the election week in 2013, more than 300,000 text messages per day were intercepted by the NCIC. Though the texts allegedly bordered on hate speech, the fact is, there was privacy invasion especially because NCIC has not clearly defined what hate speech is (KHRC, 2014). The fact that invasion of privacy is an offence punishable by law, makes it imperative to analyze how mobile applications security strategies affect the said invasion. There is hacking of personal accounts running on various mobile applications. This also is tantamount to privacy invasion. It is also imperative to note that past empirical studies have fallen short of adequately examining the subject of mobile application security on one hand, and privacy invasion on other hand, especially in the context of Kenya. In response to the acknowledgement of the problem of mobile application security breach and privacy invasion, and scarcity of empirical evidence to support the same, the present study purposed to examine various mobile application security strategies and how they affect privacy invasion.

1.3 Purpose of the Study

The general objective was to evaluate the effects of mobile application security strategies on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya.

1.4Objectives of the Study

i. To examine the effect of data encryption on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya.

ii. To analyze the effect of advanced software testing techniques on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya.

iii. To analyze the effect of risk analysis on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya.

iv. To assess the effect of privacy settings on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya.

1.5Research Hypotheses

H_{01}: There is no significant effect of data encryption on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya.

H_{02}: There is no significant effect of advanced software testing techniques on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya.

H_{03}: There is no significant effect of risk analysis on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya.

H_{04}: Thereis no significant effect of privacy settings on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya.

1.6Justification of the Study

The rise of crime especially using sophisticated channels is a threat that is being taken very seriously especially in government circles. Fraudulent activities and privacy invasion targeting public and private entities and also individuals have aggravated the dire online and mobile insecurity in Kenya. Founded on these factors and unprecedented numbers in the country of advanced mobile devices exemplified by tablets and smart phones, which support diverse applications, it is imperative to establish the link between security of applications running on these devices and privacy invasion.

1.7Scope of the Study

The study was conducted in Nakuru Town specifically, the Central Business District. This is supported by the fact that, the town is cosmopolitan in nature and has vibrant business activities and social life, and that Nakuru East Sub-County is where majority of mobile shops are found. These attributes are associated with extensive use of mobile applications. A cross-section of mobile shop operators and/or operators operating the aforementioned shops was the focus of the study. The study was delimited to a set of variables which include data encryption, advanced software testing techniques, risk analysis, privacy settings, and privacy invasion. The interrelationships amongst these variables were critically examined. The study was carried out over a span of approximately seven calendar months.

1.8 Limitations of the Study

There are likely to be some challenges that the study faced particularly during data collection. The study focused on uses of smart phones, tablets and other devices which allows the installation and use of mobile applications. This limitation was addressed by having a smaller sample size which was determined using Nassiuma's (2008) formula.

Some respondents were unwilling to divulge information pertinent to the study. The researcher informed them about the purpose for which the study was conducted and the benefits of participating in the study.

It was delimited to a set of independent and dependent variables. Independent or explanatory variables encompassed various constructs that are definitive of mobile applications security strategies. These include data encryption, advanced software testing techniques, risk analysis, and privacy settings. Privacy invasion constituted the outcome or dependent variable.

1.9 Assumptions of the Study

The study considered the following assumptions: The scope of the study (Nakuru East Sub-County)was assumed to be appropriate in conducting the study with regard to the operators of devices that support mobile applications such as cell phones, tablets, and iPads, just to mention a few. Another assumption is the feasibility of the replication of the study findings to other parts of the country. This was based on the assumption that residents of Nakuru East Sub-County are similar to residents of other parts of Kenya in respect of mobile application security strategies and privacy invasion. It was further assumed that, the researcher would not encounter substantial limitations in accessing pertinent data from the projected respondents.

1.10 Significance of the Study

The findings of this study, conclusions drawn and suggested recommendations anticipated to be informative to relevant stakeholders in formulating policies, strategies, and/or measures of improving mobile application security. By so doing, level of criminal activities and privacy invasion perpetuated via these applications, is likely to be reduced. The study expected to guide practitioners in both the MIS and security fields in dealing with security breaches occasioned by use of mobile applications. In addition, the study is hoped to increase the body of knowledge relative to management information systems and security. Thus, scholars in these areas will find the results of this study being reliable reference materials for their research and other scholarly works.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter covers literature on key study variables, empirical studies and theories that explain mobile application security strategies, and privacy invasion. Reviewed empirical studies are summarized, critiqued and identified. A conceptual framework linking the study variables diagrammatically is also discussed in this chapter.

2.2 Literature on Mobile Application Security Strategies and Privacy Invasion

A study carried out by Enck, Octeau, Mcdaniel and Chaudhuri (2011) assessed the android application security in the United States. The object of the study was to determine the security of smart-phone applications. It centered on 1100 free android applications. The study further introduced decom-piler, a program that recovers android application source code from its installation image. A static analysis of 21 million lines of recovered code was done. The findings indicated that there was wide misuse of privacy sensitive information such as location and phone identifiers. The authors further discovered that there was no evidence of malware or exploitable vulnerabilities in regard to security in the studied android applications.

A study was conducted by Mirzoev, Brannon, Lasker and Miller (2014). The authors looked into the mobile application threats and security in United States of America. The purpose of the study was to assess the existing security risks and threats and to provide solutions for such threats. The study considered Android and Apple iOS market. The findings showed that mobile devices and applications do not have standard security software and users fail to install security applications. It was further noted that users can unknowingly install malicious programs that steal important information. It was concluded that security applications need to be integrated into mobile systems during development to prevent cyber-crime.

A study carried out by McCarthy (2013) analyzed consumer data in mobile health applications in California in United States. The study involved 43 health and fitness apps. The findings showed that 74% of the free apps and 605 of the paid apps had a privacy policy. However, only 25% of the free apps and 48% of the paid apps conveyed important information on privacy policy. It was further noted that none of the free apps and few of the paid apps encrypted data that consumers keyed in. The studies concluded that the health applications do not encrypt consumer data and therefore were not secure.

A study by Osho, Yisa, Ogunleke & Abdulhamid (2015) empirically assessed mobile spamming in Nigeria. The purpose of the study was to examine the mobile spamming in the country. Primary data were obtained from selected mobile users. Questionnaires were used to collect data. The results showed that mobile phones were not secure as there was high prevalent of spamming with fraudulent intent. The study suggested that a comprehensive framework for managing mobile spamming in the country should be developed.

A study by Manoti & Odongo (2016) examined the security of mobile banking and payments in Kenya. The general objective of the study was to show the insecurity of mobile banking and payments in Kenyan banks. The study considered six mobile banking applications used by tier I banks. Exploratory research design was used. Primary data obtained from running penetration testing were used. The results indicated that most mobile banking apps used by the banks were not secure. The apps did not adhere to the open web application security project guidelines that are used for development of secure web applications.

A study was conducted by Wambua (2012). The study sought to enhance information system security in the banking services in Kenya. The objective of the study was to enhance information system security in mobile phone banking is Kenya. Descriptive research design was adopted. Questionnaires were used to collect data from the selected staff working with 45 commercial banks in Nairobi. The results indicated that mobile phone banking was not secure and confidential. The authors saw the need for banks to enhance information system security to avoid loss of money and financial fraud. Users of mobile apps can use various techniques to combat mobile application insecurity. For instance, they can use passwords, personal identification numbers, encryption, and also avoid accessing unsolicited data such as spams on their mobile devices.

2.3Data Encryption and Privacy Invasion

Globally, a study conducted by Li (2017) addressed the application of data encryption technology in network security examination in China. The study examined the application of symmetric key cryptographic algorithm and the public key encryption algorithm. The results of the study revealed that the most advanced data encryption techniques such as Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) algorithms are applied. The study also noted that data encryption system combines the key asymmetric algorithm and the public key encryption algorithm to provide a fast, practical and secure mode of transmission of confidential data. The system also provided a perfect computer network security mechanism.

A study conducted by Basharat, Azam and Muzaffar (2012) examined data security and encryption in Pakistan. The study sought to identify the issues and threats in database security and how encryption is used at different levels to provide security. The study uses the analysis of past empirical literature to draw its findings. The results of the study were that encryption provides confidentiality, however, fails to give any assurance of integrity unless there is digital signature or hash function. The study also established that the use of strong encryption algorithms leads to a reduction in performance of the database system.

In Nigeria, a study conducted by Azeez, Abubakar (2018) analyzed encryption algorithms. The purpose of the study was to conduct a comparative assessment of Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES) and Data Encryption Standard (DES) algorithms in order to identify the best in relation to its reliability, functionality and dependability. The implementation was carried out using C# and the study method used was experimental in nature. The results of the study found out that AES used the lowest time for encryption, RSA uses up the most encryption time. The study also indicated that the performance of RSA and DES algorithms was low. The study, therefore, concluded that AES was the most efficient algorithm.

A study conducted by Asare and Missah (2016) evaluated the Enhanced Triple Data Encryption Standard Algorithm in securing data transfer in level seven health institutions in Ghana. The objective of the study was to identify ways to Enhance Triple Data Encryption Algorithm in order to secure messages and data on transit at level seven health institutions in the country. The study adopted science research methodology and explored in details the steps and processes used in encryption. The study findings indicated that in order to secure information sent on the level seven messaging system there is need to utilize Enhanced Triple Data Encryption Algorithm. The study also established that the algorithm was enhanced by first hashing the key with MDS Crypto Service Provider.

A local empirical assessment conducted by Mutua (2013) investigated implementation of advanced encryption standards in mobile communication. The main aim of the study was to develop a secure mobile messaging application for java enabled mobile handsets and devices. The study used case study method. The study applied symmetric encryption concepts. The modeling of the system was done through the use of sequence, interactive state diagrams and collaborative diagrams. The algorithm was then implemented using generic algorithm approach. The study found out that the system was able to encrypt, decrypt, send and receive text messages without adding or changing the size of the packets. The study also revealed that the application was suitable and was compatible with the various models of phones that run on java.

A study conducted by Kazungu (2015) assessed information security and performance at Kenya power. One of the objectives of the study sought to establish the extent to which Kenya Power has secured its information assets. Descriptive research design was used for the study. The study sample comprised of 97 employees from Kenya Power who were selected using simple random sampling technique. Questionnaires were used as sources of data. The findings of the study revealed that the organization engages in encryption and protection of passwords.

2.4 Advanced Software Testing Techniques Privacy Invasion

A study was carried out by Muccini, Di Francesco and Esposito (2012) in Italy. The study addressed software testing for mobile applications with an inclination towards the challenges and future research directions. The rationale was to investigate the new research directions on mobile application testing automation. The study reviewed past literature on the stated issues. It was noted that in software testing for mobile apps, there were challenges such as security testing and hence privacy concerns for mobile apps. There were also challenges in graphic user interface testing that is testing whether different devices could provide adequate rendering of data, and whether native applications were correctly displayed on different devices. It was concluded that there is need for automation in testing mobile apps while in cognizance of cost implication and the need to alleviate the interoperability problems. In tandem, there is emphasis for adoption of cost-effective software testing metrics (Lazic & Mastorakis, 2008).

A study by Kulesovs (2017) analyzed mobile applications testing in Latvia. One of the objectives of the study was to provide a systemized overview of the software testing field. The study conducted reviews of academic and multi-vocal literature, documentation analysis, static and dynamic analysis, and visual modeling techniques among others in data collection. The Apple iOS applications were considered. It was established that developers carry out testing to ensure usability, functionality and security among others. In security testing, it was noted that advanced functional security testing involved checking the existence of development setting file entries. Other software testing tools were black-box and white box testing and in-operational testing in software development and system run-time. This is line with the acknowledgement of challenges in testing of mobile applications, Patel & Patel, 2017). It was further noted that there are solutions for mobile user interface test automation. The solutions included original equipment manufacturer and third party automation tools (Kulesovs, 2017).

A study carried out by Temkar *et al.*, (2015) addressed cloud-based testing technique for mobile applications in India. The study was based on the daunting task of testing mobile applications due to a variety of different operating systems. The past literature was reviewed. The authors established that there are various testing tools and techniques such as usability testing that test the functionality of the mobile apps, compatibility testing that gauges whether an app is compatible in different mobile devices, operational testing, performance and services testing among others. It was discovered that cloud based testing offer comprehensive test capabilities such as performance testing, load testing, stress testing, security testing, risk and compliance testing among others. According to Temkar, Gadekar & Shah (2015), cloud testing technique provides crucial solutions with regard to addressing challenges faced during mobile testing.

Another study was conducted by Amen, Mahmoud and Lu (2015) in the United Kingdom. The study focused on the mobile app testing matrix and challenges. The objective was to provide a solution on mobile application automated and manual testing limitations. The authors reviewed literature on the stated issue. It was revealed that mobile app testing require agility and physical testing, that is detecting bugs through automated tools and ensuring that an application runs on a mobile operating system respectively. It was further established that automated testing is ideal in mobile app testing in that it reduces human errors and is efficient in detecting bugs as compared to manual testing which has limited user-interface.

A survey study was carried out in Kenya by Chepchieng (2006). The study surveyed the software testing processes used by software developers. The study attempted to establish the tools and processes used in software testing by information and communication technology developers in Kenya. A survey research design was adopted. The information communication technology firms were targeted where managers and project managers were sampled. It was noted that the information communication technology consultants performed software testing when developing software which was observed to be important. This was in line with Temkar*et al., (*2015) assertion that mobile application testing is very difficult due to its diversity and associated different operating systems.

The firms, at various degrees followed the internally defined rules and procedures, the locally set standards and international standards such as ISO 9001in testing software. It was however, noted that software testing was hampered by the inadequacy of software testing skills by consultants. Some of the most commonly used software testing techniques include experience-based testing, automated testing, and decision table testing. Software testing techniques include control flow testing, data flow testing, path testing, and branch testing. Other techniques are black box testing, white box testing, gray box testing, agile testing, and ad hoc testing (Chepchieng, 2006).

2.5 Risk Analysis and Privacy Invasion

According to Rostami (2016), identification of risk is important in both success and risk management. This means anything short of risk identification is likely to result in inadequacy in the entire process of risk management. On the same vein, it is stated that tools and techniques aid in the process of identifying risks, and ought to be embraced subject to the entity's characteristics. When there are difficulties encountered in recognizing tools and techniques which are applicable, this becomes a barrier which inhibits risk management practice.

Risk analysis techniques become imperative in the wake of malicious applications being endeared to the features and functionality of the various mobile devices (Deshmukh & Patil, 2016). There exists an array of risks present in recent mobile apps. In view of the foregoing, android's permission system was engineered with the intent of informing users the potential risks associated with installing certain apps. Prior to installation of an app, the user is granted an opportunity to re-evaluate the application's permissions requests and cancel the installation given the imprudence or unacceptability of the permissions.

According to Chin *et al.,* (2012), the smartphone ecosystem application vendors, application markets and patterns of usage make applications more prone to malicious attacks. There is a tendency of installing a large number of apps from relatively unfamiliar brands without being keen on privacy policies of such applications. This is bound to occasion mistrust of applications (Felt *et al.*, 2011). Some of the risk analysis techniques which can be employed to address risks of hacking mobile apps include Delphi method, probability analysis, and decision theory (Karanja, 2017). Delphi method involves estimation of the likelihood and outcome of future events (Sayari *et al.*, 2014). Probability analysis is a statistical technique which uses decision trees to assess alternative courses of action where expected values are employed. Decision theory is used in probability risk analysis.

Several empirical studies have been conducted with regard to risk analysis and privacy setting. For instance, a study carried out by Gunnarsson & Ekberg (2003) addressed privacy invasion by making comparison of the United States and European Union. The study considered internet privacy violation. The authors relied on past literature on internet privacy invasion. The authors further performed a spam study and reviewed articles to come up with conclusions. The study noted that privacy violations over the internet were real and a significant problem. Importantly, it was established that privacy breach over the internet posed the risk of stalking to individuals, industrial espionage and spying. In the study, it was noted that privacy invasion posed online and marketing fraud. It was concluded that privacy protection in the European Union was better than in the United States. In addition, it is inferred that privacy violations may occasion whittling down of trust or capacity to trust forthwith (Kirsten, 2018).

A study conducted for European Union Agency Network (ENISA) assessed privacy and data protection in mobile applications (ENISA, 2017). The study obtained data from reviewing past literature, empirical studies and conducting interviews on developers. The target population for the study include: app developers, providers and other parties in app ecosystem. It was noted that risks in mobile applications stem from their nature that is software running on mobile devices, the extended use of third party software and services and the limitations of app developers. It was further stated that it is vital for developers and providers of mobile devices to understand privacy risk management that are the different privacy risks.

A study conducted by Delac, Silic and Krolo (2011) examined the security threats for mobile platforms in Croatia. The study aimed at pointing out the emerging security threats for mobile devices and extant literature on the topic was reviewed. It was established that the privacy of smart phones are at risk of being infringed. It was further noted that the mobile devices can be attacked by malicious programs. The programs collect private data, generate huge network traffic and gain access to critical systems. The lack of isolation in iOS platform compromises the security of mobile devices since the malicious programs pose the aforementioned risks; whenrisk increases, the level of trust declines (Gefen & Pavlou, 2012).

A study was conducted by Waithaka and Mnkandla (2017). The study involved the challenges that face the use of mobile applications for e-commerce in the manufacturing industry. The aim of was to determine the challenges that mobile phone users face in regard to mobile application for e-commerce. The study used semi-structured interviews to collect data from the suppliers, customers and staff of the selected manufacturing firms. The study found out that financial risks such as risk of loss of money, risk of loss of vital data to competitors and criminals, and psychological risks were some of the concerns in the use of mobile applications for e-commerce. The study concluded that security concerns of mobile phone applications for e-commerce posed risks to the users. In the wake of this conclusion, Miltgen *et al*, (2016) underline the importance of trust since it assuages the degree of risks that is perceived by consumers with regard to e-commerce.

Another study in Kenya was carried out by Karanja (2017). The study investigated the risks facing mobile banking in Kenya where the commercial banks were targeted. The aim was to determine the risks associated with mobile banking in commercial banks. Descriptive research design was used. The information technology managers of the selected banks were considered. It was noted that there was a risk of malware attack on mobile banking platform, risk of hackers stealing mobile banking personal identification numbers and codes and stealing organization emails. Furthermore, there was a risk of unauthorized access to mobile banking systems. It was observed that mobile banking carried significant risks of hacking and unauthorized access. This was in concurrence to views of a past study which acknowledged that unauthorized access has become a common concern for users and banks (Alsayed & Bilgrami, 2017).

2.6 Privacy Settings and Privacy Invasion

A study was done by Venkat, Pichandy, Barcla, and Jayaseelan (2014) on Facebook privacy management in India. The study was aimed at finding out whether Facebook was safe and secure and also whether users were aware of the privacy settings that existed on the site. A sample of 407 Facebook users was taken for the study. The findings revealed that majority of the users were unaware of the privacy settings and that those who were aware of the settings were poor at privacy management on Facebook. Further, the study found out that most of the users' personal data was open to the public opposite to their belief that their data was not public. Majority of the users were also not aware of the privacy concerns that were associated with the popular social networking website. The study hence concluded that, users unknowingly revealed personal information that wicked attackers could take advantage of and commit privacy breach.

A study was carried out by Alsaleh, Alomar and Alarifi (2017) on understanding how security mechanisms are perceived and new persuasive methods by smart phone users in Saudi Arabia. The study aimed at investigating how smart phone users' privacy related decisions and security were influenced by their perceptions, understanding different security risks and their attitude. Quantitative data was collected for the study. From the analysis of the literature, there was a relationship between privacy and security related acts. The study also revealed that making the right security decisions might not be related to people's consciousness of the results of security warnings. The study suggested an implementation of additional persuasive approaches that focused on attending to technological and social aspects of the problem.

A study conducted by Nyokabi (2016) on the management of security and privacy concerns by smart phone and social media users in Nairobi. The purpose of the   study was to investigate the challenges of security and privacy of smart phone users on social media experience and if the users actually protect themselves. The study adopted survey questionnaires and focus group discussions as the methods of data collection. A sample population of 160 respondents aged between 18-35 years who were active social media users and had access to smart phones and was taken. The findings revealed that people were aware of some threats to privacy on social media and smart phones. It was recommended that there was a need for more awareness and education on the impact of digital footprint on personal, financial and professional lives of users.

A study was undertaken by Waithaka (2013) on internet use among university students in Kenya. The study was aimed at finding out internet usage among the students at the

University of Nairobi. The study adopted quantitative technique. A survey using questionnaires was carried out among 381 students and interviews conducted with the library staff of the university. The findings of the study established that the level of awareness that was offered in school on internet services was remarkable. The study further revealed that students used the internet to do research, study and also messaging their peers which could be public or private, depending on their privacy settings. The study recommended a formal internet training and free internet access to all the students.

A study was done by Osho, Yisa, Ogunleke and Muhammad (2016) on mobile spamming in Nigeria. The purpose of the study was to investigate the incidences of spam messages. Questionnaires were used to collect primary data. From a population of 270 mobile users, a sample of 191 users was used for the study. The study found out that all the mobile subscribers received spam SMS. It was also revealed that only a few mobile-users report cases of fraudulent spam messages to network providers or security agencies. The study recommended that guidelines and regulations needed to be reviewed so as to manage spam SMS.

2.7 Theoretical Framework

Theories of privacy are reviewed and discussed in the context of mobile applications security strategies, and privacy invasion. The theories reviewed include technological acceptance model, restricted access or limited control theory of privacy, control theory of privacy, and seclusion theory of privacy.

2.7.1 Technology Acceptance Model

The technology acceptance model (TAM) was developed by Davis (1986). It is an information system model which theorizes how people accept and use technology. When users are presented with new technology, there are a number of factors that influence their decisions on when and how they will use it. These factors include; perceived usefulness which refers to the degree in which a person believes that using a particular system will improve his/her action and perceived ease of use which refers to the belief that using a particular system would not require any effort (Davis, 1989).

According to the model the belief of an individual towards a system can be influenced by other factors which are known as external variables. The external factors include; social factors, political and cultural factors. The social factors are skills, language and the facilitating conditions. The political factors include; the impact of using technology in politics and political crisis. The attitude to use technology is concerned with the user's evaluation of the desirability and application of a given information system (Surendran, 2012). model was extended by Venkatesh and Davis (2000) to provide more detailed explanations for the reasons users found a given system useful at three points in time that is at the pre-implementation point, one month post implementation and three months post implementation. The model postulates that users conduct mental assessment of the match between significant goals at work and the consequences of performing work tasks using technology. The mental assessment forms the basis of perceptions on the usefulness of the technology.

According to Parasuraman and Colby (2001) technology consumers can be categorized in to five technology readiness segments. The segments include; pioneers, paranoids, explorers and laggards. The model is based on the assumption that when a person forms an intention to act they will be free to act without limitation (Davis, Bagozzi and Warshaw, 1989). The model also assumes that when users perceive that a given type of technology is easier to use they will be willing to use it to make their work easier (Davis, 1989).

The limitations of the model include; the behavior of users is evaluated using the subjective means. The model is also grounded on behavior which cannot be reliably quantified in an empirical investigation due to societal factors, personal attributes and personality traits (Venkatesh & Brown, 2018 The TAM). The technology acceptance model does not consider factors such as education and age as some of the external factors that can affect the willingness of an individual to use technology. The theory also has limited predictive and explanatory power. Behavior expectations could be measured in relation to the levels of compliance and not solely on the perceptions of the consumers as postulated by the model. The theory can only be applied in cases of personal use of technology and cannot be conceptualized in a work environment (Shan & King, 2015).

The theory is relevant to the current study in that it helps to explain the development of advanced software testing techniques on privacy invasion. The mobile app developers should align the various features of the applications to the target consumers' characteristics. The application developed should provide opportunities for businesses to improve their service offering, that is, it should be applicable to the business environment and processes. The application developed should also be easily available, convenient for its consumers, be easy to learn and use, and should offer security to the consumer in regard to all the information the user shares on the application. The application should also serve a specified need for it to be easily accepted by the consumer.

2.7.2 Restricted Access and Limited Control Theory of Privacy

The restricted access and limited control theory **(**RALC) theory stems from the early works of Warren and Brandeis in 1890s on the concept of privacy and control. The concept has been refined to arrive at RALC theory. The theory states that one has privacy when access to information about oneself is restricted or limited in certain contexts (Gavison, 1984). The theory further differentiates the concept of privacy from both the justification and management of privacy. According to the theory, one has normative privacy in a situation where one is protected by explicit norms, policies or laws established to protect privacy (Tavani, 2007).

Privacy is established if one is able to limit and restrict others from accessing personal information and personal affairs. It is averred that restricted access theories see privacy as a moral structure aimed at protecting human beings (Mill, 1965). The theory is objective in that it perceives privacy as a moral structure that exists as right and ethical and relatively independent of single human actions (Tavani, 2008).

The theory recognizes the essence of drawing up boundaries or zones of privacy. It is noted that RALC distinguishes between the concepts of privacy and management of privacy which is achieved through limited controls for individuals. The restricted access and individual control are mutually constitutive under the theory. Privacy may be regulated in certain ways by individuals or the society. A sphere of privacy of individuals protected from access to others is set up and it enables individuals in the society to act (Nissenbaum, 2010).

The theory poses questions with regard to advancing technology, that is, to keep technology in check. In order to protect privacy, various kinds of restrictions should be put in place. It is suggested that rather than asking questions about personal control of information, it is important to have specific situations having restricted access (Moor, 1990). RALC theory is based on the assumption of the differentiation of the concept of privacy from both the justification and the management of privacy. It is noted that the theory has three components which include; an account on the concept of privacy, an account of the justification of privacy, and an account of the management of privacy (Tavani, 2007)

According to Tavani and Moor (2001), in tandem with the aforementioned three components, RALC distinguishes the condition of privacy and right to privacy. An individual has privacy, according to the theory, in a situation with regard to others if in that situation privacy is protected from intrusion, interference and information access by others (Moor, 1997). An individual has natural privacy or descriptive privacy if such an individual is in a situation where they are naturally protected. The theory further distinguishes between naturally private situations and normatively private situation where the former involves physical boundaries or situations where individuals are blocked from observation, interference and intrusion by natural means. Normatively private situations involve locations such as persons' house, relationships such as medical records and religious confessions. In this situation, ones' privacy can be violated, invaded or lost (Tavani & Moor, 2001).

The theory further posits that control is essential for management of privacy. Therefore, in order to manage one's privacy, one needs not to have absolute control over information about oneself. For instance, in ones' medical records, doctors, nurses and practitioners may have access to such information. According to the theory, a person needs a degree of control, that is, choice, consent and correction in respect of control of information. The latter implies choosing what to offer to others, waiving the right to restrict other from accessing certain information and to access information and amend it if necessary (Tavani, 2007).

The theory is applicable in privacy concerns under mobile applications. There are norms that are explicit, privacy laws and informal privacy policies that protect against breach or invasion of private, sensitive and intimate information, for instance, medical information or financial information. The providers of financial and medical services can use the insights from the RALC theory to develop privacy policies and laws in respect of use of mobile apps. According to this theory, mobile applications developers should put into consideration privacy concerns of users. This could be achieved, for instance, through encryption of user information and limiting its access by third parties. Though, this could be violated by hackers who are capable of accessing such information using modern high computing machines (Dixit, Trivedi, Gupta & Yadav, 2018)

2.7.3 Control Theory of Privacy

The control theory of privacy states that one has privacy if and only if one has control over information about oneself (Westin, 1967). According to Miller (1971) the theory is about the ability to control the circulation of information about oneself. It separates the concepts of liberty and solitude. The theory, however, is unclear on the kind of information one can exercise control over and the control that one can have over one’s personal information. Tavani (2008) observes that the theory conceives privacy as control and self-determination over personal information and over access to that information. The theory has been criticized over its impracticability. An individual is never able to have absolute control of information about personal affairs. It is further flawed in that one can reveal every bit of information but still retain the privacy of that information. Under the theory, one has a choice to grant or deny access or right to access all or none of the information in question.

In respect of mobile application security, control theory of privacy is applicable in that users of mobile applications or companies that develop such apps can control, to a certain extent, the information accessible to the public. Mobile devices’ users can make use of passwords or other encryption measures to limit the access to specified applications that have sensitive information. However, on successful hacking users can lose control and consequently privacy of sensitive information stored in mobile devices. In this case the user has no absolute control of their personal information.

2.7.4 Seclusion Theory of Privacy

The seclusion theory of privacy was proposed by Westin (1967). The theory defines privacy as ‘being alone’. A variation of the seclusion theory identifies privacy as voluntary and temporary withdrawal of a person from the society through physical ways in a state of solitude (Westin, 1967). It provides an account of privacy that is descriptive, which means an individual enjoys natural privacy because they are naturally protected. The theory suggests that the more alone a person is, the more that person enjoys or has privacy. This theory, therefore, fails to distinguish privacy from solitude (Tavani, 2008).

The theory is criticized on the basis that it is possible to one to enjoy privacy without necessarily being in solitude. The theory addresses privacy concerns in the form of unwarranted intrusion into one’s personal space by someone physically accessing one’s home, personal papers or locality. There are other aspects of non-intrusion theory that concern with the ability of an individual to make certain kinds of decisions. These concerns have led to the emergence of control and limitation of informational privacy issues (Tavani, 2007).

The physical seclusion of an individual to some extent can guard privacy particularly, natural privacy. In line with this theory, private information stored on hard drives or hard copies at home may be safe due to natural or descriptive privacy. Nevertheless, the privacy may be lost when such information is stored on platforms supported by mobile applications, despite an individual enjoying natural privacy (Dixit *et al*., 2018).

2.8 Conceptual Framework

A conceptual framework is a diagrammatic structure which that explains the natural progression of the phenomena to be studied (Camp, 2001). It describes the perceived interaction between the key variables of a study (Grant & Osanloo, 2014). With regard to the present study, Figure 2.1 illustrates the conceptual framework. The main study constructs fall under three distinct categories, that is, independent, dependent, and moderating variables. The first category of variables (independent) encompasses the various concepts characterizing mobile applications strategies. These include data encryption, advanced software testing techniques, risk analysis, and privacy settings. Privacy invasion constitutes the dependent variable while the moderating variables are education level and age of users of mobile devices. Both the independent and dependent constructs have been operationalized using pertinent indicators as shown in Figure 2.1. It is hypothesized that there exist relationships between each of the aforementioned explanatory variables and privacy invasion. However, this relationship is presumed to be influenced or moderated by the education level and age of mobile devices' users. This general hypothesis will guide the study.

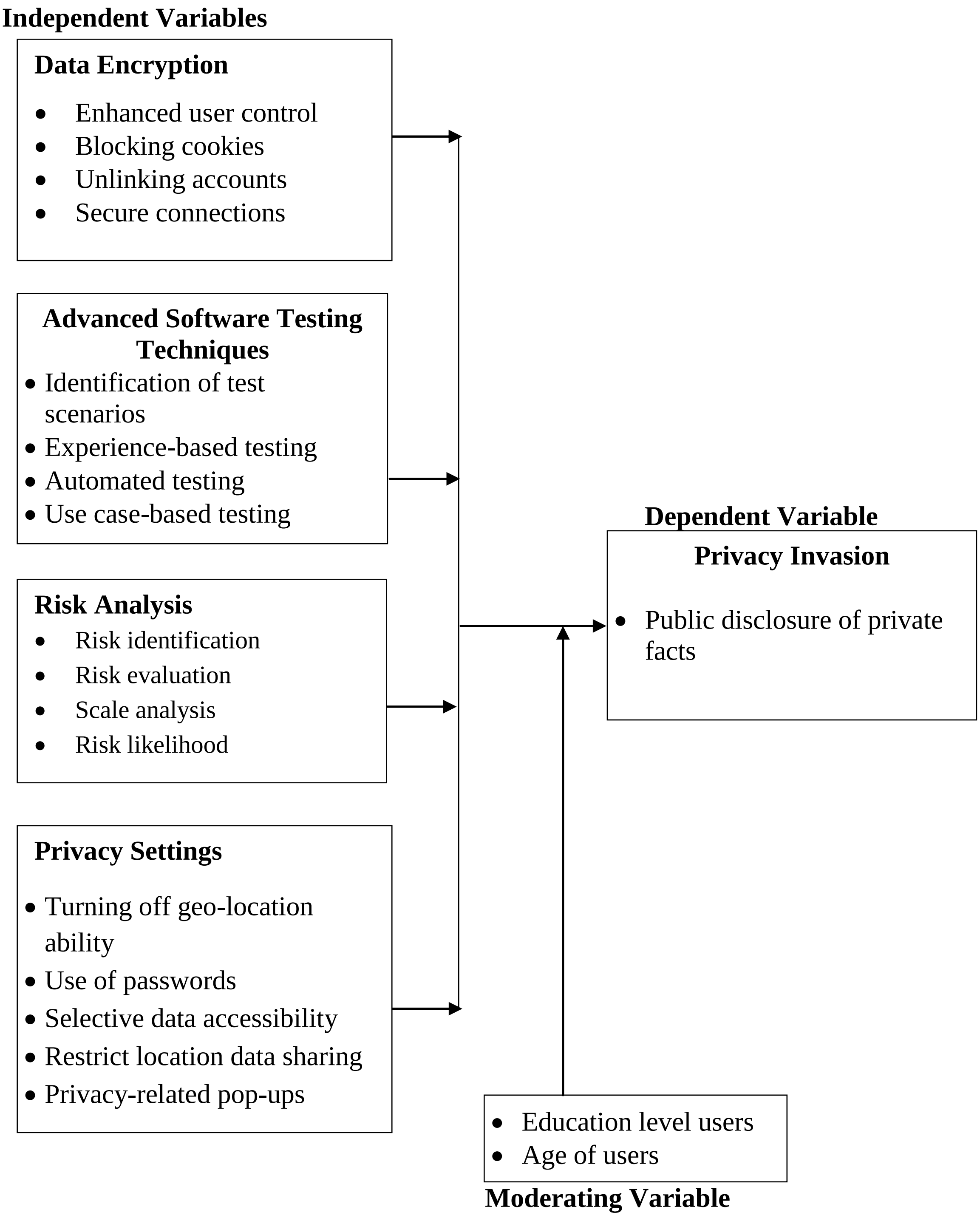


Figure 1: Conceptual Framework

Source: Researcher (2019)

2.9 Research Gaps

A critique of the reviewed local empirical studies acknowledges what has hitherto been done and pinpoints what has not been done with regard to effect of mobile application security strategies and privacy invasion in Kenya. A study by Mutua (2013) examined implementation of advanced encryption standards in mobile communication. The results of the study indicated that the system was able to encrypt, decrypt, send and receive text messages without adding or changing the size of the packets. This notwithstanding, the study did not focus on privacy invasion. Another empirical study conducted by Kazungu (2015) revealed that the organization engages in encryption and protects passwords. However, the study fell short of linking data encryption to privacy invasion.

In reference to advanced software testing techniques, a study by Chepchieng (2006) examined software testing processes employed by software developers. It was noted that software testing was hampered by the inadequacy of software testing skills by consultants. However, the aforementioned techniques were not linked to privacy invasion. In relation to risk analysis a study conducted by Wambua (2012) established that users of mobile applications can employ a number of tools to address mobile application insecurity. Nonetheless, the mobile applications were not examined in the context of privacy invasion.

With regard to privacy settings in mobile applications, a study done by Waithaka and Mnkandla (2017) mobile applications for e-commerce were facing critical risks which include potential loss of data. Yet, the study did not examine the risk involved with the use of mobile apps with regard to privacy invasion of users of mobile applications. A related study by Karanja (2017) noted that there was a risk if unauthorized access to mobile banking systems. Nevertheless, this issue was not discussed in relation to privacy invasion of mobile application users. The crucial research gaps identified in the reviewed empirical studies will be purposed to be addressed by this study going forward.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

In this chapter, the research design that guided the study was explained. In addition, the population, sampling procedure, research instrument and pilot testing of the said instrument are discussed. The chapter also outlined data collection procedure and methods of data analysis. Lastly, the chapter states how the results of the analysis were presented.

3.2 Research Design

According to Kothari (2004) a research design is a blueprint of conducting a study. It is stated that the function of a research design is to ensure that the evidence obtained by a study facilitates effective addressing of the research problem as logically and unambiguously as possible (De Vaus, 2001). This study adopted a cross-sectional research design. The rationale of adopting this design is premised on the assertion that cross-sectional studies provide a clear snapshot of the outcome and the characteristics associated with it, at a specific point in time (Hall, 2008). The present study in line with the selected research design was conducted over a specific period of time and involved randomly picked respondents from residents of Nakuru town.

3.3Location of the Study

The study was carried out in Nakuru Central Business District which is at the heart of Nakuru town. The town is not only the headquarters of Nakuru County but it is also the capital of the greater Rift Valley Region under the National Government’s jurisdiction. The town is the fourth largest town in Kenya after Nairobi, Mombasa and Kisumu city. In the recent years it has previously been reported that residents of Nakuru have been a target of cyber criminals. This makes the residents of the town including within Nakuru East Sub-County to be possibly vulnerable to privacy invasion.

3.4 Population of the Study

Target population describes all the members of a population that have common characteristics (Kothari, 2004). Narrowing down from the target population is the study population which refers to the population that a researcher has the capacity to access. The unit of observation were mobile shops within Nakuru East Sub-County; while the unit of analysis were operators of mobile shops. According to Nakuru East Sub-County Business Register (2019), there are 221 mobile shops within Nakuru town. The researcher purposively selected one respondent (Operators) from each of the 221 mobile shops therefore the study population was 221 respondents. The operators were selected since they are involved in the day to day operations of the mobile shops.

3.5 Sample Procedure and Sample Size

A sample is a subset of the study population. It is necessitated when the study population is relatively large (Kothari, 2008). When the population is relatively large, a sample should be calculated and procedure of drawing respondents from the study population determined.

3.5.1 Sampling Procedure

The distribution of operators of mobile shops in Nakuru East Sub-County is densely populated and there is variation from one shop to the other. Therefore, in order to ensure fair and equitable distribution of respondents, the researcher used purposive sampling method to select respondents (Operators) from each of the 221 mobile shops.

3.5.2 Sample Size

The study population comprising of operators of mobile shops in Nakuru East Sub-County is large (221). Therefore, sampling is necessitated. Nassiuma's (2000) formula was used to determine the sample size of 70 operators of mobile shops as illustrated below.

$$n = \frac{NC^2}{C^2 + (N - 1)\,e^2}$$

Where: 'n' = Sample size

'N' = Study population (221)

'C' = Coefficient of variation (21% ≤ C ≤ 30%)

'*e*' = Precision level (2% ≤ *e* ≤ 5%)

The equation is substituted as follows;

$$n = \frac{221\times 0.3^2}{0.3^2 + (221 - 1)\,0.03^2}$$

$$n = 69.06$$

$$n = 70\text{respondents}$$

Therefore, the size of the sample was equivalent to 70operators of mobile shops in Nakuru East Sub-County.

3.6Instrumentation

A research instrument is a tool that is used to enable collection of data from the sampled respondents. The choice of a research instrument is determined by the kind of data that is purposed to be collected and also the number and distribution of respondents. Just like in survey studies, questionnaires were the most appropriate tools for collecting data from respondents in cross-sectional studies (Mugenda & Mugenda, 2009).Given that the study is a survey and the sample size is relatively large, it is imperative to use a questionnaire in data collection. Aself-designed, structured questionnaire was used to facilitate collection of requisite data. The questionnaire contained questions on a 5-point Likert scale that addressed all the study objectives.

3.6.1 Pilot Study

A pilot study is defined as a mini-version of the main study which is conducted to not only determine the feasibility of the full-scale study, but also pre-test the research instruments (Van Teijlingen & Hundley, 2001). It is used to test the consistency of internal data, reliability of the measurement scales and validity of the variables used in the questionnaire. With reference to the present study, the research questionnaires were pilot tested in order to determine both its validity and reliability.

The pilot study was conducted amongst randomly selected residents of Eldoret town. In agreement with Kothari's (2004) assertion, the participants of the pilot study were approximately 10% of the sample size, that is, 7 operators of mobile shops operating in Eldoret town. It is deemed important to ensure that participants of the pilot study are excluded from the main study, hence the choice of a town which is similar but not the same as the area of the main study, that is, Nakuru town.

3.6.2 Validity of the Instrument

Validity testing is done in order to ensure that the data collection tool is able to facilitate collection of the intended data (Kimberlin & Winterstein, 2008). This study sought to determine the content and construct validity of the research questionnaire by consulting the assigned university supervisor. The supervisor's opinion was deemed sufficient in determining the instrument's content validity. On the other hand, Principle Axis Factoring (PAF) method was used to test the construct validity of the data collection instrument. The Statistical Package for Social Sciences (SPSS) tool facilitated analyzing of the collected data in order to test the construct validity of the research questionnaire. The validity threshold, in this case, was Eigen values greater than 1. This means that only those factors under each construct which had met the foregoing criterion were considered in the final questionnaire.

3.6.3 Reliability of the Instrument

Reliability is a measure of consistency of the research instrument. A reliable instrument is as such one that facilitates collection of similar data when administered on respondents across similar study populations. Given that the data collection instrument was structured on a 5-point Likert scale, the Cronbach’s alpha coefficient was used to test the reliability of the research instrument.

The process of reliability testing involved coding and entering of the data collected during the pilot study with the aid of the SPSS. The entered data was then analyzed to establish the results of the Cronbach’s alpha coefficient. The study variables were considered upon returning coefficients equal to 0.7 or greater than 0.7.According to Nunnally and Bernstein (1994), it is recommended to strive to achieve reliability values of 0.7 or higher. To enhance the reliability of the instrument, the researcher sought to increase the test length or number of test items (Bolarinwa, 2018).From the findings the Cronbach Alpha was between the recommended 0.7-0.9 implying that the instruments were reliable.

Table 1: Reliability Analysis

Variable	No. of items	Cronbach alpha	Decision
Privacy Invasion	7	0.706	Reliable
Data Encryption	5	0.838	Reliable
Advanced Software Testing Techniques	5	0.742	Reliable
Risk Analysis	5	0.822	Reliable
Data Settings	7	0.7461	Reliable

Source: (Researcher, 2019)

From the findings of all the 5 variables gave Cronbach's Alpha threshold values greater than 0.7. As shown in Table 3.1. From the pilot study the Cronbach Alpha values was 0.706, 0.838, 0.742, 0.822 and 0.7461 respectively. Therefore, privacy invasion, data encryption, advanced software testing techniques, risk analysis and data settings all had Cronbach values which were greater than 0.7. According to George and Mallery (2003), Cronbach correlation coefficients greater or equal to 0.7 are acceptable

3.7 Data Collection Procedure

The structured questionnaires were used to facilitate data collection from the sampled respondents. The researcher obtained the requisite consent from the relevant authorities. First and foremost, a letter of introduction was duly obtained from the Institute of Postgraduate Studies of Kabarak University in order to be allowed to embarkon data collection. This was followed by applying and obtaining a research permit and authorization letter from the National Commission of Science, Technology and Innovation (NACOSTI).

The research questionnaires were issued to the respondents by the researcher in person, and also with the assistance of trained research assistant. The researcher used trained research assistant to make the necessary clarifications on some of the technical issues that were not clear to the respondents. The questionnaires were filled on the spot by the respondents on their own and, in case of difficulties, the researcher and/or research assistants filled them on their behalf.

3.8 Data Analysis

The filled questionnaires were critically analyzed to ensure that only those filled according to instructions and expectations were considered. Incomplete and wrongly filled questionnaires were discarded in order to minimize the number of outliers. The Statistical Package for Social Sciences (SPSS) tool was employed to facilitate processing and analysis of the collected data.

Descriptive statistics such as frequencies, percentages, means, standard deviations, and chi-square were used in the analysis. Moreover, inferential statistics in form of correlation and multiple regression analyses were also used. The results of the analyses were presented in tabular form. The following regression model was adopted.

$Y= \beta_0 + \beta_1X_1 + \beta_2X_2 + \beta_3X_3 + \beta_4X_4 + \varepsilon$

Where:

Y	represents	Privacy Invasion
β_0	represents	Constant
X_1	represents	Data Encryption
X_2	represents	Advanced Software Testing Techniques
X_3	represents	Risk Analysis
X_4	represents	Data Settings
ε	represents	Error term
$\beta_1, \beta_2, \beta_3, \beta_4$	represents	Régression Coefficients for Independent Variables

3.9 Ethical Considerations

A number of ethical considerations were factored by the study especially prior, during, and after data collection. Given that primary data was collected, the researcher obtained a research permit and authorization letter from NACOSTI. Moreover, the researcher ensured and assured respondents of the confidentiality of the data collected from them. This means that the identity of the respondents was not sought. The study also was delimited to academic purposes andas such, not be used for any other objectives.

CHAPTER FOUR

DATA ANALYSIS, PRESENTATION AND DISCUSSION

4.1 Introduction

The chapter focuses on data analysis, results presentation and discussion of the findings. The general objective of the study was to evaluate the effect of mobile application security strategies on privacy invasion with special focus on mobile users residing in Nakuru Central Business District, Kenya.

4.2 Response Rate

Response rate equals the number of people with whom semi-structured questionnaires were properly completed divided by the total number of people in the entire sample (Fowler, 2014). The study administered 70 questionnaires for data collection. However, 62 questionnaires were properly filled and returned. This represented 89% overall successful response rates. Respondents were also assured of confidentiality of the information provided. Trex (2012) suggested that a response rate of 50% is adequate 60% is good and 70% and above very good for analysis. This implies that 89 percent response rate was very appropriate for data analysis.

Table 2 : Response Rate

Question Issued	Question Correctly Filled	Response Rate (%)
70	**62**	**89**

4.3Demographic Information

The demographic information presented is on the, age of the respondents, education level of the respondents and duration the respondents had owned mobile shops.

4.3.1 Age of the Respondents

The respondents were asked to indicate the age of the respondents. The findings were as shown in Figure .

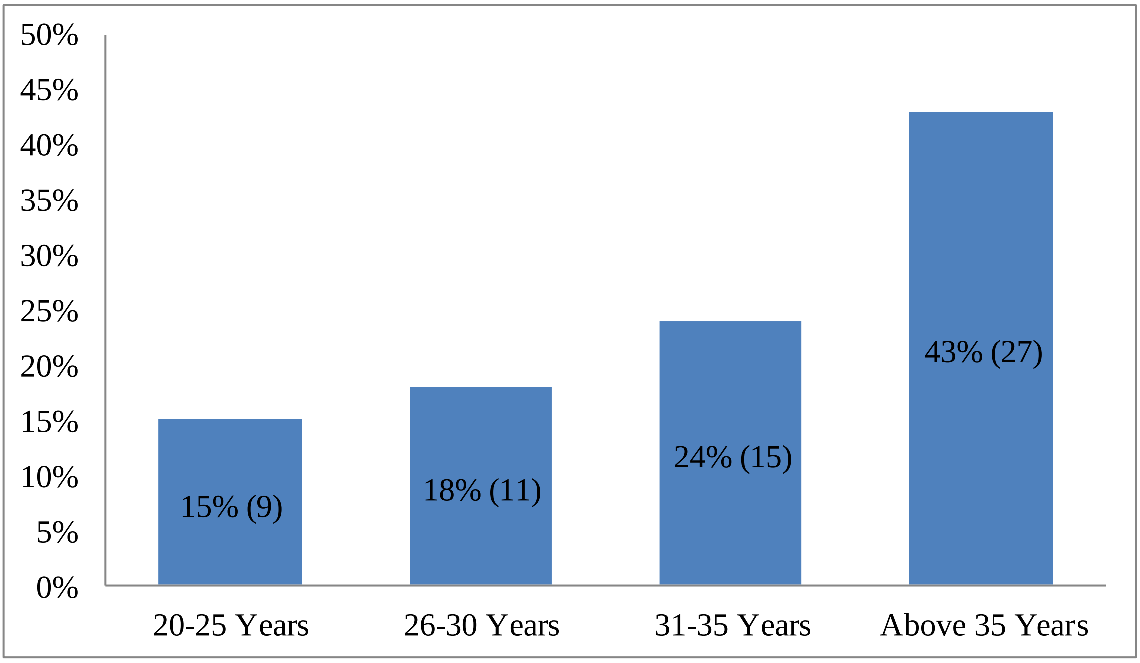


Figure 2: Age of the Respondents

From the findings, 9 (15%) of the respondents indicated that they were in the age bracket of 20-25years, 11 (18%) indicated that they were in the age bracket of 26-30years, 15 (24%) indicated that they wer in the age bracket of 31-35years while (27) 43% indicated that they were above 35years. Age determines the efficiency of the human resource managers in the mobile industry. Human resource above 35 years have been in the market for a while and thus, they understand the marketing strategies better than the youngsters. This implies that most of the respondents were above 30 years.

4.3.2 Respondents' Highest Level of Education

The respondents were asked to indicate their highest level of education. The findings were as shown in Figure 3.

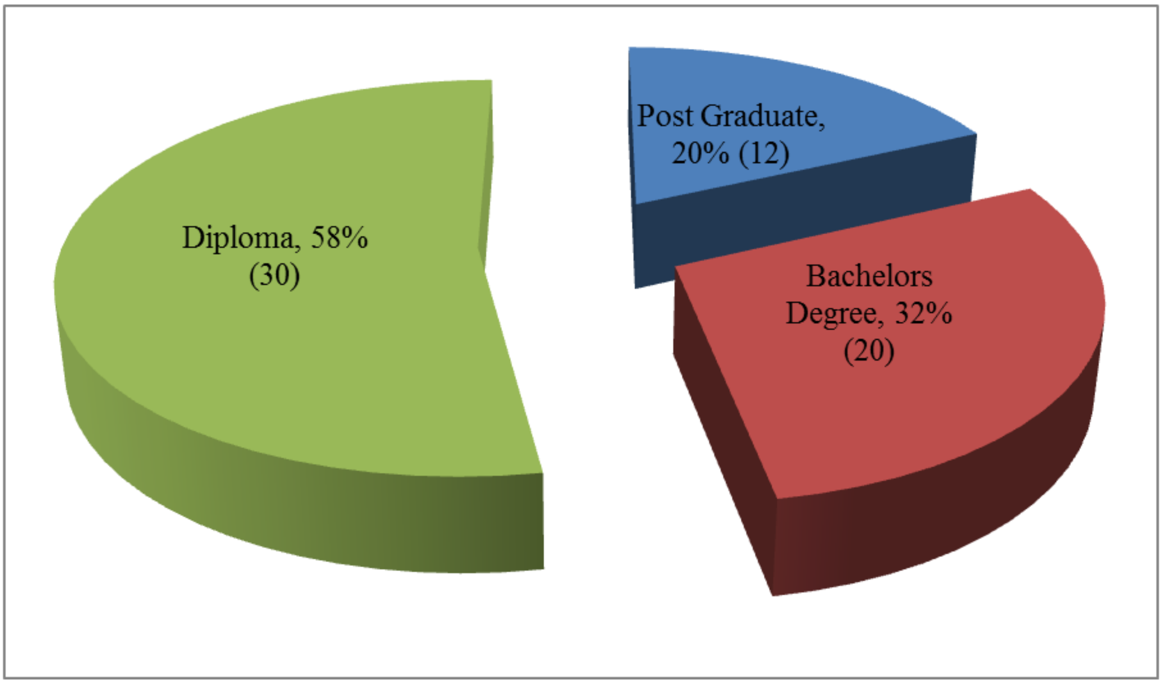


Figure 3: Respondents' Highest Level of Education

From the findings, 12 (20%) of the respondents indicated that they had attained post graduate education, 20 (32%) indicated that they had attained bachelors degree education while 30 (58%) indicated that they had attained diploma education. The education level determines the efficiency of an employee. This implies that majority of the respondents had attained diploma education.

4.3.3 Duration in the mobilephone business

The respondents were also asked to indicate the duration the respondents had been selling mobile devices. The findings were presented in Table 3.

Table 3: Duration in the Mobile Phone Business

Duration	Frequency	Percentage
Less than 1 Years	20	33
1-5 Years	22	35
6-10 Years	12	19
More than 10 years	8	13
Total	**62**	**100**

According to the findings, 20 (33%) of the respondents indicated that they have been selling mobile phone for less than 1 years, 22(35%) of the respondents indicated that they had been selling mobile phone for 1-5 years, 12(19%) of the respondents indicated that they had been selling mobile phone for 6-10 years while 8(13%) of the respondents indicated that they have been operating a mobile shops for more than 10 years. The duration of service an individual has worked determines his/her capacity. Employees who have longer working experience tend to have better skills. This shows that majority of the respondents had been operating mobile shops for less than 1 years.

4.4.4 Association Between Duration in the Mobile Phone Business and Age

The researcher sought to determine the association between duration in the mobile phone business and age using Pearson Chi-Square Test. The findings are as shown in Table 4.

Table 4: Pearson Chi-Square Test on the association between duration in the mobile phone business and age

Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	92.179[a]	9	.000
Likelihood Ratio	84.048	9	.000
Linear-by-Linear Association	41.401	1	.000
N of Valid Cases	62		

From the findings the P=0.000 which was less than the 0.05 significant level implying that there is statistically significant association between duration in the mobile phone business and age

4.4 Descriptive Statistics

The study requested respondents to give opinions in regard effect of data encryption, advanced software testing, effect of risk analysis, and effect of privacy settings on privacy invasion in Nakuru East Sub-County, Kenya. The interpretation of the findings was made based on the mean and standard deviation. The value of the mean indicated the level of agreement. The value of the mean ranged between 1-5, with 1 being the least mean and 5 being the highest mean. Standard deviation is a measure of the dispersion of a set of data from its mean

4.4.1 Data Encryption on Privacy Invasion

The respondents were asked to indicate their level of agreement on the effect of Data Encryption on privacy Invasion in Nakuru East Sub-County, Kenya. The findings are presented in Table 5.

Table 5: Data Encryption on privacy Invasion

Statement	SA %	A %	U %	D %	SD %	Mean	Std
My mobile device has strong data/file encryption capability, where only people with certain key can access the said data.	26	47	17	10	0	3.887	0.907
My device is installed with software that enables effective blocking of cookies.	37	45	13	5	0	4.113	0.870
I always use specific keys on all the data that I save on my phone.	55	42	0	0	8	4.516	0.565
My device has enhanced user control, meaning that I have a large room of controlling who can and who cannot access data stored on my phone	57	37	6	0	0	4.500	0.621
Most of the time, I block cookies that pop up on my device	39	44	11	6	0	4.145	0.866
Privacy Invasion overall mean						**4.232**	**0.766**

According to the findings, majority of the respondents (73%) agreed that their mobile device has strong data/file encryption capability, where only people with certain key can access the said data with a mean of 3.887 and the standard deviation of 0.907. The findings concurs with, Asikoyo (2016) who observed that encryption scrambles text to make it unreadable by anyone other than those with the keys to decode it, and it’s becoming less of an added option and more of a must-have element in any security strategy for its ability to slow down and even deter hackers from stealing sensitive information. The findings further indicated that majority of the respondents (82%) agreed that their device are installed with software that enables effective blocking of cookies. with a mean of 4.113 and the standard deviation of 0.870. In addition majority of the respondents (97%) agreed that they always use specific keys on all the data that they save on their phone with a mean of 4.516 and the standard deviation 0.565. The findings further indicated that majority of the respondents (94%) agreed that the their device has enhanced user control, meaning that the respondents have a large room of controlling who can and who cannot access data stored on their phone with a mean 4.500 and the standard deviation of 0.621.

In addition majority of the respondents (83%) agreed that the most of the time, they block cookies that pop up on their device with a mean of 4.145 and the standard deviation of 0.866. The standard deviation ranged from 0.565 to 0.907 indicating that the dispersion of the respondents from the mean was minimal. This implies that data encryption affects privacy Invasion. The findings are in line with Mutua (2015) study who noted that most mobile users in Kenya often block cookies that pop up on their device while using the online platforms. Most modern websites use cookies in some way, and it is unlikely that the majority of internet users even notice cookies working away in the background as they browse from site to site. Until now it has been up to individual users to either block or allow cookies using settings in their internet browser.

4.4.2 Advanced Software Testing Techniques on Privacy Invasion

The respondents were asked to indicate their level of agreement on the effect of Advanced Software Testing Techniques on privacy invasion Nakuru East Sub-County, Kenya. The findings are presented in Table 6.

Table 6: Advanced Software Testing Techniques on privacy invasion

Statement	S A %	A %	U %	D %	SD %	Mean	Std
My mobile phone was installed with applications bearing in mind how I would effectively use those applications.	52	39	9	0	0	4.419	0.667
The features of my phone indicate that past and current experience was used in developing apps installed in my phone.	37	31	19	13	0	3.887	1.073
It is highly probable that efficient testing techniques were used in developing apps installed in my phone.	44	40	6	10	0	4.177	0.932
Various actors and their interactions with mobile apps were involved in developing apps installed in my phone	37	39	10	14	0	3.984	1.032
Mobile apps installed in my mobile devise are relatively difficult to hack.	42	39	11	8	0	4.145	0.921
Privacy Invasion overall mean						**4.123**	**0.925**

According to the findings majority of the respondents agreed (91%) that their mobile phone are installed with applications bearing in mind how they would effectively use those applications with a mean of 4.419 and the standard deviation of 0.667. According to Pogue (2016) most mobile devices are sold with several apps bundled as pre-installed software, such as a web browser, email client, calendar, mapping program, and an app for buying music, other media, or more apps. Some pre-installed apps can be removed by an ordinary uninstall process, thus leaving more storage space for desired ones. Where the software does not allow this, some devices can be rooted to eliminate the undesired apps. The users of the mobile phones install the apps bearing in mind how to uninstall them. They can also root the phone to get more other apps.

The findings further indicated that majority of the respondents (68%) agreed that the features of their phone indicate that past and current experience that is used in developing apps installed in their phone with a mean of 3.887 and the standard deviation of 1.073. The study is in agreement with Musiu (2015) study which found that the features of their mobile phones indicate that past and current experience was used in developing apps installed in my phone.

Also, the findings indicated that majority of the respondents (84%) agreed that it is highly probable that efficient testing techniques are used in developing apps installed in their phone with a mean of 4.177 and a standard deviation of 0.932. According to Digitaltimes, (2016) before developing mobile apps, mobile software quality assurance is done. This is a process-oriented activity that requires the application of a whole set of approaches, methods, and standards to the creation of software, directed at obtaining a quality product that is maximally adapted for potential user requests, as a result. Further memory leakage testing is conducted when a computer program or application is unable to manage the memory it is allocated resulting in poor performance of the application and the overall slowdown of the system. As mobile devices have significant constraints of available memory, memory leakage testing is crucial for the proper functioning of an application.

Further majority of the respondents (76%) agreed that various actors and their interactions with mobile apps was involved in developing apps installed in their phonewith a mean of 3.984 and a standard deviation of 1.032. Majority of the respondents (81%) also indicated that mobile apps installed in their mobile devise are relatively difficult to hack a mean of 4.145 and a standard deviation of 0.921. The standard deviation ranged from 0.667 to 1.073 indicating that majority of the respondents agreed with the issues raised. From the findings it is clear that advanced software testing techniques affects privacy invasion among the mobile shop operators in Nakuru East Sub-CountyAccording to Himalaya (2017) it is relatively difficult to hack the mobile phone depend on the operating system used. If you are using Apple's IOS then it is completely mission impossible to use for hacking because IOS kind of very closed operating system and does not give full permissions to even normal users and for hacking you need minimum 4 GB of R.A.M and in the case of apple you can't get even in next 3-4 years. If you are using Windows phone again it is not possible because Windows operating is not appropriate for hacking. Hardware specs are also not enough for this work.

4.4.3 Risk Analysis on Privacy Invasion

The respondents were asked to indicate their level of agreement on the effect of risk analysis on privacy invasion in Nakuru East Sub-County, Kenya. The findings are presented in Table 7.

Table 7: Risk Analysis on Privacy Invasion

	S A	A	U	D	SD	Mean	Std
Statement	**%**	**%**	**%**	**%**	**%**		
I identify risks which could potentially affect personal and confidential data stored on my device.	47	34	13	6	0	4.210	0.908
I always evaluate the risks of an application before installing it in my mobile phone	50	31	15	5	0	4.258	0.886
I analyze the predisposing risk factor of an application before installing it in my mobile phone	44	53	3	0	0	4.403	0.557
The likelihood of a given risk occurring is determined using measurable parameters.	37	44	16	3	0	4.145	0.807
I am able to analyze all forms of risks that my mobile device is exposed to.	35	45	5	0	0	4.452	0.592
Privacy Invasion overall mean						**4.294**	**0.750**

According to the findings majority of the respondents (81%) agreed that they identify risks which could potentially affect personal and confidential data stored on the device with a mean of 4.210 and a standard deviation of 0.908. Majority of the respondents (81%) also agreed that they always evaluate the risks of an application before installing it in the mobile phonewith a mean of 4.258 and a standard deviation of 0.886. The findings agree with Metayer, (2018) who observed that most of the mobile operators are very keen on privacy of their portable devises. They identify potential risk associated with portability of the devices like theft, which could potentially affect the confidentiality of their data stored in the devices. Further the mobile users also avoid public Wi-Fi network which are especially risky and a frequent target of attackers looking for data to pilfer. Attackers often linger nearby and use tools such as Kismet and Wire shark to intercept unencrypted data.

Majority of the respondents also (97%) agreed that they analyze the predisposing risk factor of an application before installing it in their mobile phone with a mean of 4.403 and a standard deviation of 0.557. According to Juniper Research, (2018)people gladly install mobile apps and provide personal information, but rarely stop to think about the security implications positive technologies experts regularly perform security analysis of mobile applications. The research further noted that comprehensive security checks of a mobile application include a search for vulnerabilities in the client and server, as well as data transmission between them

In addition majority of the respondents (81%) agreed that the likelihood of a given risk occurring is determined using measurable parameters with a mean of 4.145 and a standard deviation of 0.807. Further majority of the respondents (80%) agreed that they are able to analyze all forms of risks that my mobile device is exposed to, with a mean of 4.452 and a standard deviation of 0.592. The findings imply that risk analysis affects privacy invasion among the mobile shop operators in Nakuru East Sub-County. The study agree with a study with Nafula (2017) study which noted that the in data security risk occurrences is determined using measurable parameters like the absorption rate (SAR) given in units of Watts of power absorbed per kilogram of tissue (W/kg), and the loud-based testing technique.

4.4.4 Privacy Settings on Privacy Invasion

The respondents were asked to indicate their level of agreement on the effect of Privacy Settings on Privacy Invasion in Nakuru East Sub-County. The findings are presented in Table 8.

Table 8: Privacy Settings on Privacy Invasion

	S A	**A**	**U**	**D**	**SD**	**Mean**	**Std**
Statement	**%**	**%**	**%**	**%**	**%**		
My mobile phone has the option of turning off accessibility of the phone's location	37	34	10	16	3	3.855	1.185
I frequently use passwords to safeguard the data stored on my phone.	55	34	8	3	0	4.403	0.778
I sometimes select the type and amount of data which can be accessed by outsiders.	44	46	7	3	0	4.307	0.738
I often restrict sharing of data on my location.	37	44	16	3	0	4.145	0.807
I sometimes accept privacy related pop-ups that regularly feature on the screen of my device.	55	33	7	5	0	4.387	0.869
Privacy Invasion overall mean						**4.219**	**0.875**

According to the findings majority of the respondents (71%) agreed that their mobile phone has the option of turning off accessibility of the phone's location with a mean of 3.855 and a standard deviation of 1.185. According to Xiaoman, (2017) in mobile accessibility, screen contents are displayed in Braille in a way that will give you an idea of visual information such as format, hierarchy, control type, and phone location. In this mode, mobile speak sends information to the display that is relevant to the current cursor position. The information sent includes things such as control type, dialog name, or number of items in a list (where the list index is not really displayed visually) and the options for turning off the mobile location.

Majority of the respondents (89%) also agreed that they frequently use passwords to safeguard the data stored on their phone with a mean of 4.403 and a standard deviation of 0.778. They further agreed (90%) that they sometimes select the type and amount of data which can be accessed by outsiders. with a mean of 4.307 and a standard deviation of 0.738. According to Konglin (2017) most of the mobile users frequently use password to secure their data such as copies of their driver's license, employer data, insurance details, social security card, and bank account information on their mobile device

In addition majority of the respondents (81%) agreed that they often restrict sharing of data on my location with a mean of 4.145 and a standard deviation of 0.807. Majority of the respondents (88%) also agreed that they sometimes accept privacy related pop-ups that regularly feature on the screen of my device with a mean 4.387 and a standard deviation of 0.869. The finding agrees with Arif (2016) study which found that only a few mobile-users report cases of fraudulent spam messages to network providers or security agencies and some of the mobile subscribers received spam SMS and accept the privacy related to the pop-ups that regularly feature on the screen of my device.

4.4.5 Privacy Invasion

The study sought to determine the trend of privacy invasion in Nakuru East Sub-County. The finding are indicated in Table 9.

Table 9: Privacy Invasion

Privacy Invasion	**SA (%)**	**A (%)**	**N (%)**	**D (%)**	**SD (%)**	**Mean**	**Std.**
I have in several occasions experienced privacy breach when using my mobile device.	58	24	8	4	6	4.177	0.912
I have never experienced my private data or information stored in my mobile device being disclosed to the public.	40	48	4	8	0	3.984	1.032
I have experienced impersonation of my identity.	50	34	8	4	4	4.145	0.921
Third parties occasionally intrude into the content of my mobile device.	54	36	2	5	3	4.563	.608
I have experienced presentation of false information regarding me on mobile device.	48	40	3	5	4	4.181	.513
I am greatly concerned by invasion of my privacy by unsolicited persons/entities.	58	24	8	4	6	4.177	0.912
Invasion of my privacy through mobile device has greatly affected my day-to-day life.	40	48	4	8	0	3.984	1.032
Privacy Invasion overall mean						**4.173**	**0.8471**

From the findings 58% of the respondents strongly agreed that they have in several occasions experienced privacy breach when using my mobile device, 24% agreed 8% of the respondent were neutral 4% disagreed while 6% strongly disagreed (mean=4.177, SD=0.912). From the finding 40% of the respondents strongly agreed that they have never experienced private data or information stored in their mobile device being disclosed to the public, 48% agreed, 4% were neutral while 8% disagreed (mean=3.984, SD=1.032). On the same note, 50% of the respondents strongly agreed that they have experienced impersonation of their identity, 34% agreed 8% were neutral 4% disagreed while 4% strongly disagreed (mean=4.145, SD=0.921).

The study sought to find out whether third parties occasionally intrude into the content of their mobile device. From the findings 54% of the respondents strongly agreed, 36% agreed, 2% were neutral, 5% did not agree while 3% strongly disagreed (mean=4.563, SD=0.608). Moreover, 48% of the respondents agreed that they have experienced presentation of false information regarding on their mobile device, 40% agreed, 3% were neutral 5% did not agree while 4% strongly agree (mean=4.181, SD=0.513). Further, the study findings revealed that 58% of the respondents strongly agreed that they are greatly concerned by invasion of their privacy by unsolicited persons/entities, 24% agreed 8% of the respondent were neutral 4% disagreed while 6% strongly disagreed (mean=4.177, SD=0.912). From the finding 40% of the respondents strongly agreed that invasion of their privacy through mobile device has greatly affected my day-to-day life 48% agreed, 4% were neutral while 8% disagreed (mean=3.984, SD=1.032). The findings are congruent to those of Ratemo (2015) study which found out that most of the respondents reported that have in several occasions experienced privacy breach when using my mobile device.

4.5 Inferential Statistics

Inferential statistics makes inferences and predictions about a population based on a sample of data taken from the population in question. The study used Pearson correlation analysis and regression analysis.

4.5.1 Correlation Analysis

Correlation is a technique for investigating the relationship between two quantitative, continuous variables. The study will adopted Pearson correlation analysis. Pearson's correlation coefficient (r) a measures the strength of the association between the two variables

4.5.1.1 Data Encryption on Privacy Invasion

The study sought to establish the correlation between data encryption on privacy invasion of the mobile users in Nakuru East Sub-County. The findings are presented in Table 10.

Table 10: Data Encryption on Privacy Invasion

		Privacy Invasion
Data Encryption	Pearson Correlation	-.323*
	Sig. (2-tailed)	.000
	N	62

*. Correlation is significant at the 0.05 level (2-tailed).

As indicated in Table 10, the study indicates that there was a negative and statistically significant correlation between data encryption and privacy invasion of the mobile users in Nakuru East Sub-County. ($r = -.323$; $p < 0.05$). This implies that an increase in data encryption will result to reduction in privacy invasion. The findings of the study concurs with to Zappala, (2018) study which noted that, encryption of health electronic records resulted to reduction in privacy and protection from issues such as theft, data breaches, loss, inaccuracies, exposure of personal data and medical identity.

4.5.1.2 Advanced Software Testing Techniques on Privacy Invasion

In addition the study sought to establish the correlation between advanced software testing techniques on privacy invasion of the mobile users in Nakuru East Sub-County. The findings are presented in Table 11.

Table 11: Advanced Software Testing Techniques on Privacy Invasion

		Privacy Invasion
Advanced Software Testing Techniques	Pearson Correlation	-.311*
	Sig. (2-tailed)	.006
	N	62

*. Correlation is significant at the 0.05 level (2-tailed).

As indicated in Table 11, the study indicates that there was a negative and statistically significant correlation between advanced software testing techniques and privacy invasion. (r = -.311; p < 0.05). This implies that advanced software testing techniques results to reduction in privacy invasion of the mobile users. The findings concurs with Westin(2017) study which noted that advanced software testing techniques/application security is more of a sliding scale where providing additional security layers helps reduce the risk of privacy invasion to an acceptable level of risk for the organization. Thus, advanced software testing techniques reduces risk in of privacy invasion.

4.5.1.3 Risk Analysis on Privacy Invasion

The study further examined the correlation between risk analyses on privacy invasion of the mobile users in Nakuru East Sub-County. The findings are presented in Table 12.

Table 12: Risk Analysis on Privacy Invasion

		Privacy Invasion
Risk Analysis	Pearson Correlation	-.241*
	Sig. (2-tailed)	.000
	N	62

*. Correlation is significant at the 0.05 level (2-tailed).

The study as shown in Table 12 established that there was a moderate negative correlation existed between risk analysis and privacy invasion of mobile users in Nakuru East Sub-County(r = -.241; p < 0.05). The results of the correlation analysis indicated that better risk analysis reduction cases of privacy invasion of mobile users in Nakuru East Sub-County. The findings is in agreement with Ayandi (2015) some of the risk analysis techniques which can be employed to address risks of hacking mobile apps include Delphi method, probability analysis, and decision theory and all these have a positive relationship with the privacy invasion.

4.5.1.4 Privacy Settings on Privacy Invasion

The study further examined the correlation between privacy settings on privacy invasion of mobile users in Nakuru East Sub-County, Kenya. The findings are presented in Table 13.

Table 13: Privacy Settings on Privacy Invasion

		Privacy Invasion
Privacy Setting	Pearson Correlation	-.441*
	Sig. (2-tailed)	.000
	N	62

*. Correlation is significant at the 0.05 level (2-tailed).

The study as shown in Table 13 established that a strong negative correlation existed between Privacy setting and privacy invasion (r = -0.441; p < 0.05). The results of the correlation analysis indicated that better privacy setting improve the privacy invasion of the mobile users in Nakuru East Sub-County. The findings is in agreement with Venkat, Pichandy, Barcla, and Jayaseelan (2014) study on Facebook privacy management the study revealed that privacy setting had a positive relationship in protecting the data of the mobile users in Facebook accounts.

Table 14: Correlation Matrix

Correlations

		Data Encryption	Advanced Software Testing Techniques	Risk Analysis	Data Settings	Privacy Invasion
Data Encryption	Pearson Correlation	1	.068*	109*	.155*	-.323*
	Sig. (2-tailed)		.625	.062	.071	.000
	N	62	62	62	62	62
Advanced Software 5Testing Techniques	Pearson Correlation	.068*	1	.076*	.068*	-.311*
	Sig. (2-tailed)	.625		.028	.565	.006
	N	62	62	62	62	62
Risk Analysis	Pearson Correlation	109*	.076*	1	.068*	-.241*
	Sig. (2-tailed)	.062	.058		.865	.000
	N	62	62	62	62	62
Data Settings	Pearson Correlation	.155*	.035*	.232*	1	-.441*
	Sig. (2-tailed)	.071	.056	.063		.000
	N	62	62	62	62	62
Privacy Invasion	Pearson Correlation	-.323*	-.311*	-.241*	-.441*	1
	Sig. (2-tailed)	.000	.006	.000	.000	
	N	62	62	62	62	62

*. Correlation is significant at the 0.05 level (2-tailed).

4.6 Assumption of Regression Model

In order to justify the use of the regression model pre-estimation tests were conducted. The pre-estimation tests conducted in this case were multi-collinearity test. This was performed to avoid spurious regression results from being obtained.

4.6.1 Test for Multi-collinearity

A multi-collinearity test was carried out to ensure that the independent variables did not have co-linearity amongst themselves. The existence of a high degree of association between independent variables is said to be a problem of multi-collinearity which results into large standard errors of the coefficients of the affected. The variance inflation factors (VIF) and Tolerance were used to assess multi-collinearity. The VIF, which stands for variance inflation factor, is (1 / tolerance) and as a rule of thumb, a variable whose VIF value is greater than 10 may merit further investigation.

Table 15: Tolerance and VIF Test

		Tolerance	**VIF**
1	(Constant)		
	Data Encryption	.552	1.813
	Advanced Software Testing Techniques	.439	2.277
	Risk Analysis	.537	1.863
	Privacy Settings	.506	1.976

a. Dependent Variable: Privacy Invasion

From the findings, the variable data encryption had a tolerance of 0.552 and a VIF of 1.813, advanced software testing techniques had a tolerance of 0.439 and a VIF of 2.277, risk analysis had a tolerance of 0.537 and a VIF of 1.863 while privacy settings had a tolerance of 0.506 and a VIF of 1.317. Since the tolerance for all the variables was more than 0.1 and the VIF was not more than 10 therefore there was no need of further investigations.

4.6.2 Regression Analysis

The study carried out a regression analysis to evaluate the combined effect of data encryption, advanced software testing techniques, risk analysis, privacy settings on privacy invasion among the mobile users in Nakuru East Sub-County was established.

4.6.2.1 Model Summary

The researcher sought to determine the value of R^2. The R-Squared is the proportion of variance in the dependent variable which can be explained by the independent variables.

Table 16: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Sig. F Change
1	.878[a]	.770	.749	.3873	.000

The R-squared in this study was 0.770, which shows that the four independent variables (data encryption, advanced software testing techniques, risk analysis, privacy settings) can explain 77.0% on privacy invasion of the mobile users in Nakuru East Sub-County, Kenya while other factors explain 23.0%.

4.6.2.2 Analysis of Variance

The analysis of variance in this study was used to determine whether the model is a good fit for the data. The findings is indicated in Table 17.

Table 17: Analysis of Variance

Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	28.563	3	9.521	64.769	.000[b]
	Residual	8.532	58	.147		
	Total	37.095	61			

a. Dependent Variable: Privacy invasion of the Mobile users
b. Predictors: (Constant), data encryption, advanced software testing techniques, risk analysis, privacy settings on privacy invasion

From the findings, the p-value was 0.000 which is less than 0.05 and hence the model is good in predicting how the four independent variables (data encryption, advanced software testing techniques, risk analysis, privacy settings on privacy invasion) affect privacy invasion of mobile users. Further, the F-value was (64.769) which shows that the model was fit in predicting the effect of the independent variables on the dependent variable.

4.6.2.3 Overall Model

Table 18 shows the overall significant test results for the hypothesized research model

Table 18: Regression Coefficients

Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**Variance Inflation**
		B	Std. Error	Beta			
1	(Constant)	1.195	.130		9.165	.796	
	Data encryption	-.047	.023	-.082	-2.026	.023	1.813
	Advanced software testing techniques	-.210	.034	-.269	-6.177	.016	2.277
	Risk analysis	-.522	.183	.533	-2.853	.008	1.863
	Privacy settings	-.439	.230	.360	-1.909	.003	1.976

The interpretations of the findings indicated follow the following regression model.

$Y=1.195 - 0.047 X_1 - 0.210 X_2 - 0.522X_3 -0.439X_4$

According to the intercept (β_0), when the four independent variables are held constant, the value of privacy invasion among the mobile users in Nakuru East Sub-County will be 1.195. In addition, holding all the other independent variables constant, a unit increase in data encryption would lead to a -.047 reduction in privacy invasion among the mobile users in Nakuru East Sub-County, Kenya. Further, holding on the other independent variables constant, a unit increase in advanced software testing techniques would lead to a -.210 reduction in privacy invasion among the mobile users in Nakuru East Sub-County, Kenya.

In addition, holding all the other variables constant, a unit increase in risk analysis would lead to a -.522 reduction in privacy invasion among the mobile users in Nakuru East Sub-County, Kenya. Finally holding all the other variables constant, a unit increase in privacy setting would lead to a -0.439 reduction in privacy invasion among the mobile users in Nakuru East Sub-County, Kenya. From these findings we can infer that data encryption is affecting privacy invasion among the mobile users in Nakuru East Sub-Countymost, followed by pprivacy settings, risk analysis and advanced software testing techniques.

4.7 Hypothesis Testing

The study carried a hypothesis testing using p-values in Table 19.

The study sought to test the hypothesis that: **H_{01}:** There is no significant effect of data encryption on privacy invasion in Nakuru East Sub-County, Kenya. From the findings the p-value was 0.023 which was less the 0.05 significant level. Therefore, based on the rule of significance, the study rejects the null hypothesis **(**H_{01}**)** and concluded that data encryption has a significant effect on privacy invasion in Nakuru East Sub-County.

The study sought to test the hypothesis that: **H_{02}:** There is no significant effect of advanced software testing techniques, on privacy invasion in Nakuru East Sub-County, Kenya. From the findings the p-value was 0.016 which was less the 0.05 significant level. Therefore, based on the rule of significance, the study rejects the null hypothesis **(**H_{02}**)** and concluded that advanced software testing techniques has a significant effect on privacy invasion inNakuru East Sub-County, Kenya.

The study sought to test the hypothesis that: **H_{03}**: There is no significant risk analysis on privacy invasion in Nakuru East Sub-County, Kenya. From the findings the p-value was 0.022 which was less the 0.05 significant level. Therefore, based on the rule of significance, the study rejects the null hypothesis **(**H_{03}**)** and concluded that risk analysis has a significant effect on privacy invasion in Nakuru East Sub-County, Kenya.

The study sought to test the hypothesis that: **H_{04}:** There is no significant effect of privacy setting on privacy invasion in Nakuru East Sub-County, Kenya.From the findings the p-value was 0.003 which was less the 0.05 significant level. Therefore, based on the rule of significance, the study rejects the null hypothesis **(**H_{04}**)** and concluded that privacy setting has a significant effect on privacy invasion in Nakuru East Sub-County, Kenya.

Table 20: Summary Table

Hypothesis		**Findings** **(**p-values**)**	**Decision**
i.	Data encryption	.023	Reject
ii.	Advanced software testing techniques	.016	Reject
iii.	Risk analysis	.022	Reject
iv.	Privacy Setting	.003	Reject

CHAPTER FIVE
SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter focuses on the summary of major findings of the study; both descriptive and inferential. This is followed by a presentation of the conclusions inferred from the findings. The relevant recommendations are then suggested. Finally, the chapter outlines the areas suggested for further research.

5.2 Summary

The major study findings are summarized in this section. It outlines the summary of the findings in line with the objectives of the study.

5.2.1 Effect of Data Encryption on Privacy Invasion

The study revealed that mobile device has strong data/file encryption capability, where only people with certain key can access the said data. It was also agreed that majority of mobile device are installed with software that enables them to effectively blocking of cookies. In addition majority of the respondents agreed that they use specific keys on all the data that they save on their phone. The study sought to test the hypothesis that: $H0_1$: There is no significant effect of data encryption on privacy invasion in Nakuru East Sub-County, Kenya. From the findings the p-value was 0.023 which was less the 0.05 significant level. Therefore, based on the rule of significance, the study rejects the null hypothesis ($H0_1$) and concluded that data encryption has a significant effect on privacy invasion in Nakuru East Sub-County. The study agrees with Mutua (2015) study who noted that most mobile users in Kenya often block cookies that pop up on their device while using the online platforms.

5.2.2 Advanced Software Testing Techniques on Privacy Invasion

From the study, majority of the respondents admitted that mobile phone have installed applications bearing in mind how they would effectively use those applications. It was also clear that the feature of majority of phones indicates they were installed with apps. The findings of the study further indicated that it is also highly probable that efficient testing techniques were used in developing apps installed in majority of phone. The study sought to test the hypothesis that: $H0_2$: There is no significant effect of advanced software testing techniques, on privacy invasion in Nakuru East Sub-County, Kenya. From the findings the p-value was 0.016 which was less the 0.05 significant level. Therefore, based on the rule of significance, the study rejects the null hypothesis (H02) and concluded that advanced software testing techniques has a significant effect on privacy invasion in Nakuru East Sub-County, Kenya. The study is in line with Musiu (2015) study which found that the features of their mobile phones indicate that past and current experience was used in developing apps installed in my phone.

5.2.3 Risk Analysis on Privacy Invasion

It was concurred that majority of mobile shops identify risks which could potentially affect personal and confidential data stored in their device. It was also agreed that majority of mobile shops always evaluate the identified risks in order to determine the extent of their threat to mobile data. The findings also revealed that they rank the various risks posed by apps installed in their device. The study sought to test the hypothesis that: H04: There is no significant effect of privacy setting on privacy invasion in Nakuru East Sub-County, Kenya. From the findings the p-value was 0.003 which was less the 0.05 significant level. Therefore, based on the rule of significance, the study rejects the null hypothesis ($H0_4$) and concluded that privacy setting has a significant effect on privacy invasion in Nakuru East Sub-County, Kenya. The findings agree with Metayer, (2018) who observed that most of the mobile operators are very keen on privacy of their portable devises. They identify potential risk associated with portability of the devices like theft, which could potentially affect the confidentiality of their data stored in the devices.

5.2.4 Privacy Settings on Privacy Invasion

The findings further agreed that majority of mobile phone has the option of turning off accessibility of the phone's location. It was also agreed that majority of mobile shops frequently use passwords to safeguard the data stored on their phone. The findings also revealed that sometimes mobile phone shops select the type and amount of data which can be accessed by outsiders. The study sought to test the hypothesis that: $H0_3$: There is no significant risk analysis on privacy invasion in Nakuru East Sub-County, Kenya. From the findings the p-value was 0.022 which was less the 0.05 significant level. Therefore, based on the rule of significance, the study rejects the null hypothesis ($H0_3$) and concluded that risk analysis has a significant effect on privacy invasion in Nakuru East Sub-County, Kenya. The finding agrees with Arif (2016) study which found that only a few mobile-users report cases of fraudulent spam messages to network providers or security agencies and some of the mobile subscribers received spam SMS and accept the privacy related to the pop-ups that regularly feature on the screen of my device.

5.3 Conclusions

5.3.1 Data Encryption on privacy Invasion

From the findings, the researcher concluded that majority of mobile phone devices have enhanced user control, meaning that they have a large room of controlling who can and who cannot access data stored on their phones. It was also noted that most of the mobile phone shops block cookies that pop up on their devices. The results of the study revealed that there was a negative and statistically significant correlation between data encryption and privacy invasion of the mobile users in Nakuru East Sub-County. (r = -.323; p < 0.05). This implies that an increase in data encryption will result to reduction in privacy invasion. The findings of the study concurs with to Zappala, (2018) study which noted that, encryption of health electronic records resulted to reduction in privacy and protection from issues such as theft, data breaches, loss, inaccuracies, exposure of personal data and medical identity.

5.3.2 Advanced Software Testing Techniques on Privacy Invasion

Regarding the effect of advanced software testing techniques on privacy invasion the researcher concluded that various actors and their interactions with mobile apps were involved in developing apps installed in my phone. The study also concluded that majority of mobile apps installed in their phones are relatively difficult to hack. The results of the study revealed that there was a negative and statistically significant correlation between advanced software testing techniques and privacy invasion. (r = -.311; p < 0.05). This implies that advanced software testing techniques results to reduction in privacy invasion of the mobile users. The findings concurs with Westin(2017) study which noted that advanced software testing techniques/application security is more of a sliding scale where providing additional security layers helps reduce the risk of privacy invasion. The findings concurs with Westin(2017) study which noted that advanced software testing techniques/application security is more of a sliding scale where providing additional security layers helps reduce the risk of privacy invasion to an acceptable level of risk for the organization.

5.3.3 Risk Analysis on Privacy Invasion

The study concluded that the likelihood of a given risk occurring is determined using measurable parameters. Majority of mobile shops are able to analyze all forms of risks that their mobile devices are exposed to. The results of the study revealed that there was a moderate negative correlation existed between risk analysis and privacy invasion of mobile users in Nakuru East Sub-County(r = -.241; p < 0.05). The results of the correlation analysis indicated that better risk analysis reduces cases of privacy invasion of mobile users in Nakuru East Sub-County. The findings is in agreement with Ayandi (2015) some of the risk analysis techniques which can be employed to address risks of hacking mobile apps.

5.3.4 Privacy Settings on Privacy Invasion

Regarding privacy setting the study concluded that majority of mobile shops often restrict sharing of data on the location. Majority of mobile shops also sometimes accept privacy related pop-ups that regularly feature on the screen of my device. The results of the study revealed that a strong negative correlation existed between Privacy setting and privacy invasion (r = -0.441; p < 0.05). The results of the correlation analysis indicated that better privacy setting improve the privacy invasion of the mobile users in Nakuru East Sub-County. The findings is in agreement with Venkat, Pichandy, Barcla, and Jayaseelan (2014) study on Facebook privacy management the study revealed that privacy setting had a positive relationship in protecting the data of the mobile users in Facebook accounts.

5.5 Recommendations for Further Research

The study recommended that mobile shop operators within Nakuru East Sub-Countyshould adopt data encryption security because it allows protection of data that they do not want anyone else to have access to. As businesses people it will help them to protect corporate secrets and secure classified information, and many individuals use it to protect personal information to guard against things like identity theft. It is also important in protecting folder contents, which could contain emails, chat histories, tax information, credit card numbers, or any other sensitive information. This way, even if your computer is stolen that data is safe.

The study further recommended that mobile shop operators should adopt advanced software testing techniques because it provides stakeholders with information about the quality of the software product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation. Test techniques include the process of executing a program or application with the intent of finding software bugs (errors or other defects), and verifying that the software product is fit for use.

Further the researcher recommended that mobile users within Nakuru East Sub-County should adopt risk analysis as this will help the mobile users, to understand the different kinds of risks and threats associated with the mobile platform. It is possible for organizations to mitigate the potential risks and vulnerabilities during the development of mobile applications by establishing (or optimizing) formal security policies, procedures, and standards; education and training; and security engineering activities.

Finally the researcher recommended that mobile phone users ought to adopt privacy setting techniques because it will help them to detect when their devices are being hacked and take measures to protect themselves online from malicious cyber attackers.

5.5 Suggestion for Further Study

The researcher recommended that a study should be conducted on the management of security and privacy concerns by smart phone and social media users in Nakuru East Sub-County. Further studies should be conducted to determine if the research will deduce similar findings as those of the current study.

REFERENCES

Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Cell phone clients: Understanding how security systems are seen and new powerful strategies. Plos one, 12 (1), 1-35.

Alsaleh, M., Alomar, N., &Alarifi, A. (2017). Cell phone clients: Understanding how security instruments are seen and new influential strategies. PLoS One, 12(3), 134 – 154. doi.org/10.1371/journal.

Amen,M., Mahmood, M., & Lu, J. (2015). Versatile Application Testing Matrix and Challenges. Recovered first March 1, 2019 from https://airccj.org/ CSCP/vol5/csit53503.pdf

Asare, T., & Missah, M. (2016). An upgraded Tripple Data Encryption Standard (TDES) calculation to verify wellbeing level seven information move. *Universal Research Journal of Engineering and Technology*, 3(10), 16-27.

Award, C., & Osanloo, A. (2014). Understanding, choosing, and incorporating a hypothetical system in thesis inquire about: Creating the plan for your "home." *Administrative Issues Journal: Connecting to Education, Practice, and Research*, 4(2), 12–26

Azeez, A., & Abubakar, A. (2018). Near investigation of encryption calculations. *Journal of Informatics and Communication Technology*, 6(1), 16-30.

Basharat, I., Azam, F., & Muzaffa, A. (2012). Database Security and Encryption: A Survey Study. *Global Journal of Computer Applications*, 47(12), 28-34.

Bolarinwa, O. (2015). Standards and techniques for legitimacy and unwavering quality testing of polls utilized in social and wellbeing science looks into. *Niger Postgrad Med*, 22, 195-201.

Camp, W. (2001). Defining and assessing hypothetical systems for profession and specialized training. *Profession and specialized training research*, 26(1), 4-25.

Chellegati, T. (2009) Man-In-The-Middle-Attack Prevention Using HTTPS and SSL. *Global Journal of Computer Science and Mobile Computing*, 5(6), 569-579

Chemwa, D. (2012). Security Issues looked by Mobile money Transfer Applications in Kenya on GSM and #G Networks. Establishment of Computer Science and Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya.

Chepchieng, K.H. (2006). A Survey of Software Testing forms Used by Software engineers in Kenya. *Unpublished MBA Project, University of Nairobi, Nairobi, Kenya.*

Culnan, J., & Bies, R. (2003). Shopper Privacy: Balancing Economic and Justice Considerations. *Journal of Social*, 59, 33-38

Davis, D. (1986). An innovation acknowledgment model for observationally testing new end client data framework: Theory and results. Massachusetts Institute of Technology: Massachusetts, United States.

Davis, D. (1989). Seen helpfulness, saw convenience and client acknowledgment of data innovation. *MIS Quarterly*, 13(3), 319-340.

Davis, D., Bagozzi, P., & Warshaw, R. (1989). Client acknowledgment of PC innovation: A correlation of two hypothetical models. *The executives Sciences*, 35(8), 982-1003.

Delac, G., Silic, M., & Krolo, J. (2011). Rising Security Threats for Mobile Platforms. Gathering: *MIPRO*, 1468-1473.

Deshmukh, R., & Patil, B.M. (2016). Successful hazard examination and hazard discovery for android applications. *Universal Journal of Computer Applications*, 147(6), 29-32.

Dixit, P., Trivedi, C., Gupta, K., & Yadav, K. (2018). Conventional and Hybrid Techniques: A Survey. Singapore: *Springer Nature Singapore* Plc Ltd.

Enck, W., Octeau, D., Mcdaniel, P., & Chaudhuri, S. (2011). An investigation of android application security. A paper introduced at the Proceedings of the twentieth USENIX Security Symposium.

European Union Agency Network. (2017). Security and Data Protection in Mobile Applications. A Study on the App Development Ecosystem and the Technical Implementation of GDPR. Heraklion, Greece: *European Union Agency for Network and Information Security,*

Factory, S. (1965) in Mill, J.S. (Ed.). Standards of Political Economy (second Ed.). *London: University of Toronto Press.*

Felt, P., Greenwood, K., & Wagner, D. (2011). The Effectiveness of Application Permissions. Paper introduced at the proc. Second USENIX Conf. *Web Application Development* (WebApps '11).

Fouchier, R., Adechy, B., Pierquin, G., & Girolamo, P. (2016). Gemalto: Building Trust in Mobile Apps. The shopper viewpoint. Recovered 30th January 2019 from https:// www.gemalto.com/ leaflets website/download-webpage/Documents/ tel-buyer perspectives.pdf

Gavison, R. (1980). Security and the Limits of Law. *The Yale Law Journal*, 89(3), 421-471

Gefen, D., & Pavlou, P. (2012). The limits of trust and hazard: The quadratic directing job of institutional structures. *Data Systems Research*, 23(32), 940–959.

George, D., & Mallery, P. (2003). SPSS for Windows bit by bit: A straightforward guide and reference. 11.0 update (fourth ed.). Boston: Allyn and Bacon.

Jawline, Y., Zhi, W., & Xuxian, J. (2012). Deliberate Detection of Capability Leaks in Stock Android Smartphones. In Proceedings of the nineteenth Annual Network and Distributed System Security Symposium, NDSS '12, February 2012

Karanja, J. (2017). Examination concerning the Risks Facing Mobile Nanking: A Case of Commercial Banks in Kenya. *Unpublished MBA Project, United States International University – Africa, Nairobi, Kenya*.

Kazungu, A. (2015). Data security and execution at Kenya Power. Unpublished MBA Thesis, University of Nairobi, Nairobi.

Kenya Human Rights Commission, (2014). The Internet Legislative and Policy Environment in Kenya. Nairobi: Kenya Human Rights Commission. Gotten to on February 16, 2019

Kesler, R., Kummer, M., & Schulte, P. (2017). Versatile Applications and Access to Private Data. 1-38.

Kimberlin, L., & Winterstein, G. (2008). Research essentials. *Am J Health-SystPharm,* 65 (4), 46 – 76.

Kirsten, M. (2018) Privacy Protection Overseas as Perceived by USA-Based IT Professionals. *Journal of Global Information Management* 6(15), 68-8

Kirsten, M. (2018). The punishment for protection infringement: How security infringement sway trust on the web. *Journal of Business Research,* 8(2), 103-116.

Kothari, C. (2004). *Research Methodology: Methods and Techniques*. New Delhi: Wiley.

Kothari, C. (2008). *Research Methodology: Methods and Techniques*. New Delhi: Wiley.

Kulesovs, I. (2017). *Portable Applications Testing*. Unpublished PhD theory. College of Latvia. Latvia.

La Diega, G. (2019). Crushing protection in the web of bodies: An observational investigation on dating portable applications for men who engage in sexual relations with men. *Journal of Strategy Management.* 4(8), 1-52.

Lazic, L., & Mastorakis, N. (2008). Financially savvy programming test measurements. WSEAS *Transactions on Computers*, 7(6), 599-619.

Li, J. (2017). Research on the utilization of information encryption innovation in organize security transmission. Revisita De La Facultad De Ingeeeriera, 32(5), 595-604.

Lin, J. (2013). Comprehension and Capturing People's Mobile App Privacy Preferences. *Unpublished PhD Thesis, Carnegie Mellon University,* Pittsburgh, USA.

Liu, C., & Yao, D. (2017). Endeavor information rupture: Causes, difficulties, and counteractive action and future bearings. *WIREs Data Mining Knowledge Discovery*, 7 (5).

Luvanda, A., Kimani, S., & Kimwele, M. (2014). Absence of mindfulness by end clients on security issues influencing portable banking: A contextual analysis of Kenyan cell phone end clients. *Journal of Information Engineering and Applications*, 4(5), 19-28.

Mahoney, R., & Pokorny, C. (2009). Do-It-Without anyone else's help Guide to Cell Phone Malware. *Global Journal of Computer Science and Network Security*, 9(1), 43-46.

Manoti, M., & Odongo, O. (2016). Upgrading Security of Mobile Banking and installments in Kenya. Unpublished MSc venture, University of Nairobi, Nairobi Kenya.

McCarthy, M. (2013). Specialists Warn on Data Security in Health and Fitness Apps.Br. Medications. J, 347, 1

Mendel, T., Puddephatt, A., Wagner, H., & Torres, N. (2012). Worldwide Survey on Internet Privacy and Freedom of Expression. Paris: The United Nations Educational, Scientific and Cultural Organization. Gotten to on February 16, 2019

Mill operator, A. (1971). The Assault on Privacy. Cambridge: Harvard University Press.

Miltgen, F. (2016). Purchaser Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues* 5(5), 23-29.

Mirzoev, F., Brannon, D., Lasker, S. & Miller, D. (2014). Purchasers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security. Emory University: Atlanta, GA

Mohankumar, M., Banuroopa, K., & Sreevidhya, K. (2018). Overview on portable digital wrongdoing. *Global Journal of Research in Electronics and Computer Engineering*, 6 (3), 1-3.

Moore, A. (2008). Characterizing protection. *Journal of Social Philosophy*, 39(3), 411-428.

Muccini, H., Di Francesco, An., & Esposito, P. (2012). Programming Testing of Mobile Applications: Challenges and Future Research Directions. Recovered February 26, 2019 from https://www.computer.org/csdl/ procedures/ast/ 2012/1821/00/ 06228987.pdf

Mulligan, K., Koopman, C., & Doty, N. (2016). Protection is a basically challenged idea: A multi-dimensional investigative for mapping security. Phil. Trans. R. Soc. A, 374. Gotten to on February 17, 2019

Mutua, V. (2013). An execution of cutting edge encryption guidelines in versatile correspondence: Secure informing application. *Unpublished Master of Science Thesis, University of Nairobi, Nairobi.*

Nassiuma, K. (2008). *Overview Sampling:* Theory and Methods. Nairobi: Nairobi University Press.

Nissenbaum, H. (2010). *Protection in Context.* Stanford, CA: Stanford University Press.

Nunnally, C., & Bernstein, H. (1994). *Psychometric Theory*. (third Ed.). New York: McGrawHill.

Nyokabi, G. (2016). *The Management of Security and Privacy Concerns by Smart Phones and Social Media Users in University of Nairobi*. Unpublished Master of Arts postulation, University of Nairobi, Nairobi.

Osho, O., Yisa, V., Ogunleke, Y., & Muhammad, S. (2016). Versatile spamming in Nigeria: An observational Survey. London: The Free Fress.

Osho, O., Yisa, V.L., Ogunleke, O.Y., & Abdulhamid, S.M. (2015). Portable spamming in Nigeria: An observational study. *Worldwide Conference on Cyberspace Governance*. Recovered March 1, 2019 from

Parasuraman, An., and Colby, L. C. (2001). Techno-prepared market. London: The Free Fress.

Park, M. (2012). Versatile application security: Who, how and why. Trustwave Retrieved 30th January, 2019 from https://www.owasp.org/ pictures/c/cf/ASDC12Mobile _Application_Security_Who_how_and_why.pdf

Patel, D., & Patel, A. (2017). Versatile applications testing difficulties and related arrangements. *Worldwide Journal of Advanced Research in Computer Science*, 8(3), 541-544.

Rostami, A. (2016). Devices and procedures in chance distinguishing proof: An examination inside SMEs in the UK development industry. *All inclusive Journal of Management*, 4(4), 203-210. DOI: 10.13189/ujm.2016.040406

Sampat, B., & Prabhakar, B. (2017). Protection Risks and Security Threats in wellbeing Apps. *Journal of International Technology and Information Management*, 26 (4), 126-152.

Sayari, D. (2014) Modeling Corporate Wireless Security and Privacy. *Journal of Strategic Information Systems*, 14(3), 54-59

Shan, Y., & King, K. (2015). The Effects of relational tie quality and emotional standards on purchasers' image related referral goals. *Journal of Interactive Advertising*, 15(1), 16-27.

Surendran, P. (2012). Innovation Acceptance Model. *Worldwide Journal of Business and Social Research*, 2(4), 175-178.

Tavani, H. (2007). Morals and innovation: Ethical issues during a time of data and correspondence innovation (second ed.). Hoboken, NJ: John Wiley and Sons Inc.

Tavani, H., & Moor, J. (2001). Security assurance, control of data, and privacy-enhancing innovations. *SIGCAS Computers and Society*, 31(1), 6–11.

Tavani, H.T. (2008). Instructive Privacy: Concepts, Theories, and Controversies. In Kenneth Einar Himma/Herman Tavani (Hrsg.), The Handbook of Information and Computer Ethics, S. 121-164. Hoboken, New Jersey: Wiley.

TechWatch, T. (2009). Portable Applications. Recovered 30th January, 2019 from https://www.itu.int/dms_pub/itut/oth/23/01/T230100000C0004PDFE.pdf

Temkar, R., Gadekar, S., & Shah, D. (2015). Cloud based portable application testing. *Universal Journal of Science, Engineering and Technology Research*, 4(6), 2097-2102.

Vankatesh, V., & Davis, F. (2000). A hypothetical expansion of the innovation acknowledgment model. *The executives science*, 46(2), 186-204.

Venkat, A., Pichandy, C., Barclay, P., & Jayaseelan, R. (2014). Facebook Privacy Management: An Empirical Study of Awareness, Perception and Fears. *Worldwide Media Journal*, 5 (1), 1-20.

Venkatesh, V., & Brown, S. A. (2008). The contending jobs of conduct goal, encouraging conditions and social desires. *MIS Quarterly*, 32(3), 483-502.

Waithaka, M. (2013). Web use among University understudies in Kenya: An investigation of the University of Nairobi. Unpublished Masters of Arts Thesis, Pretoria.

Waithaka, T., & Mnkanda, E. (2017). Difficulties' confronting the utilization of portable applications for internet business in Kenya's assembling industry. EJISDC, 83 (1), 1-25.

Wambua, A.M. (2012). *Improving Information System Security in Mobile Phone Banking Services in Kenya*. Unpublished Post Graduate Diploma venture, University of Nairobi, Nairobi Kenya

Warren, S., & Brandeis, L. (1890). The privilege to security. *Harvard Law Review*, 14(5), 193–220.

Westin, A.F. (1967). Protection and Freedom. New York: Atheneum Press.

.

APPENDICES

Appendix I: Letter of Introduction

Dear Sir/ Madam,

Re: Consent Statement to the Respondent

I am a postgraduate student pursuing a Master of Business Administration (Management Information Systems Option) at Kabarak University. In tandem with the University's requirements, I am presently conducting an empirical study on "***Effects of mobile application security strategies on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya***."

In the foregoing regard, I kindly request you to provide me with data that will facilitate the study by filling objectively the questionnaire attached herewith. All the data collected and the study at large will be treated with utmost confidentiality. The study is absolutely for academic purposes. The researcher will be ready to share the results of the study with any interested respondent.

With thanks,

Angela Wanjiku Kivindyo

GMB/NE/0208/01/12

Appendix II: Research Questionnaire

Instructions

This questionnaire is intended to facilitate collection of data with regard to a study on, "Effects of mobile application security strategies on privacy invasion among mobile shop operators in Nakuru East Sub-County, Kenya." The questionnaire is divided into six (6) categories. These are background information, privacy invasion prevention strategies, challenges in combating privacy invasion, risk analysis, advanced software testing techniques, and privacy invasion.

Part A: Background Information

Kindly put a tick (√) against the correct choice in the brackets.

1. What is your age? ________________ years
2. What is your highest education level? ______________________

3. How many years have you owned or used or sold a mobile device such as a mobile phone, tablet or ipad? _______________ years

Part B: Data Encryption

Using the following Likert scale, indicate your level of agreement or disagreement with regard to the stated propositions.

'SA' represents 'Strongly Agree'; 'A' represents 'Agree'; 'NAND' represents 'Neither Agree nor Disagree'; 'D' represents 'Disagree'; and 'SD' represents 'Strongly Disagree'.

	SA	A	NAND	D	SD
4. My mobile device has strong data/file encryption capability, where only people with certain key can access the said data.					
5. My device is installed with software that enables effective blocking of cookies.					
6. I always use specific keys on all the data that I save on my phone.					
7. My device has enhanced user control, meaning that I have a large room of controlling who can and who cannot access data stored on my phone.					
8. Most of the time, I block cookies that pop up on my device.					

Part C: Advanced Software Testing Techniques

Using the following Likert scale, indicate your level of agreement or disagreement with regard to the stated propositions.

'SA' represents 'Strongly Agree'; 'A' represents 'Agree'; 'NAND' represents 'Neither Agree nor Disagree'; 'D' represents 'Disagree'; and 'SD' represents 'Strongly Disagree'.

It is true to state that:	**SA**	**A**	**NAND**	**D**	**SD**
1. My mobile phone was installed with applications bearing in mind how I would effectively use those applications.					
2. The features of my phone indicate that past and current experience was used in developing apps installed in my phone.					
3. It is highly probable that efficient testing techniques were used in developing apps installed in my phone.					
4. Various actors and their interactions with mobile apps were involved in developing apps installed in my phone					
5. Mobile apps installed in my mobile devise are relatively difficult to hack.					

Part D: Risk Analysis

Using the following Likert scale, indicate your level of agreement or disagreement with regard to the stated propositions.

'SA' represents 'Strongly Agree'; 'A' represents 'Agree'; 'NAND' represents 'Neither Agree nor Disagree'; 'D' represents 'Disagree'; and 'SD' represents 'Strongly Disagree'.

	SA	**A**	**NAND**	**D**	**SD**
6. I identify risks which could potentially affect personal and confidential data stored on my device.					
7. I always evaluate the risks of an application before installing it in my mobile phone					
8. I analyze the predisposing risk factor of an application before installing it in my mobile phone					
9. The likelihood of a given risk occurring is determined using measurable parameters.					
10. I am able to analyze all forms of risks that my mobile device is exposed to.					

Part E: Privacy Settings

Using the following Likert scale, indicate your level of agreement or disagreement with regard to the stated propositions.

‘SA’ represents ‘Strongly Agree’; ‘A’ represents ‘Agree’; ‘NAND’ represents ‘Neither Agree nor Disagree’; ‘D’ represents ‘Disagree’; and ‘SD’ represents ‘Strongly Disagree’.

	SA	**A**	**NAND**	**D**	**SD**
1. My mobile phone has the option of turning off accessibility of the phone’s location					
2. I frequently use passwords to safeguard the data stored on my phone.					
3. I sometimes select the type and amount of data which can be accessed by outsiders.					
4. I often restrict sharing of data on my location.					
5. I sometimes accept privacy related pop-ups that regularly feature on the screen of my device.					

Part F: Privacy Invasion

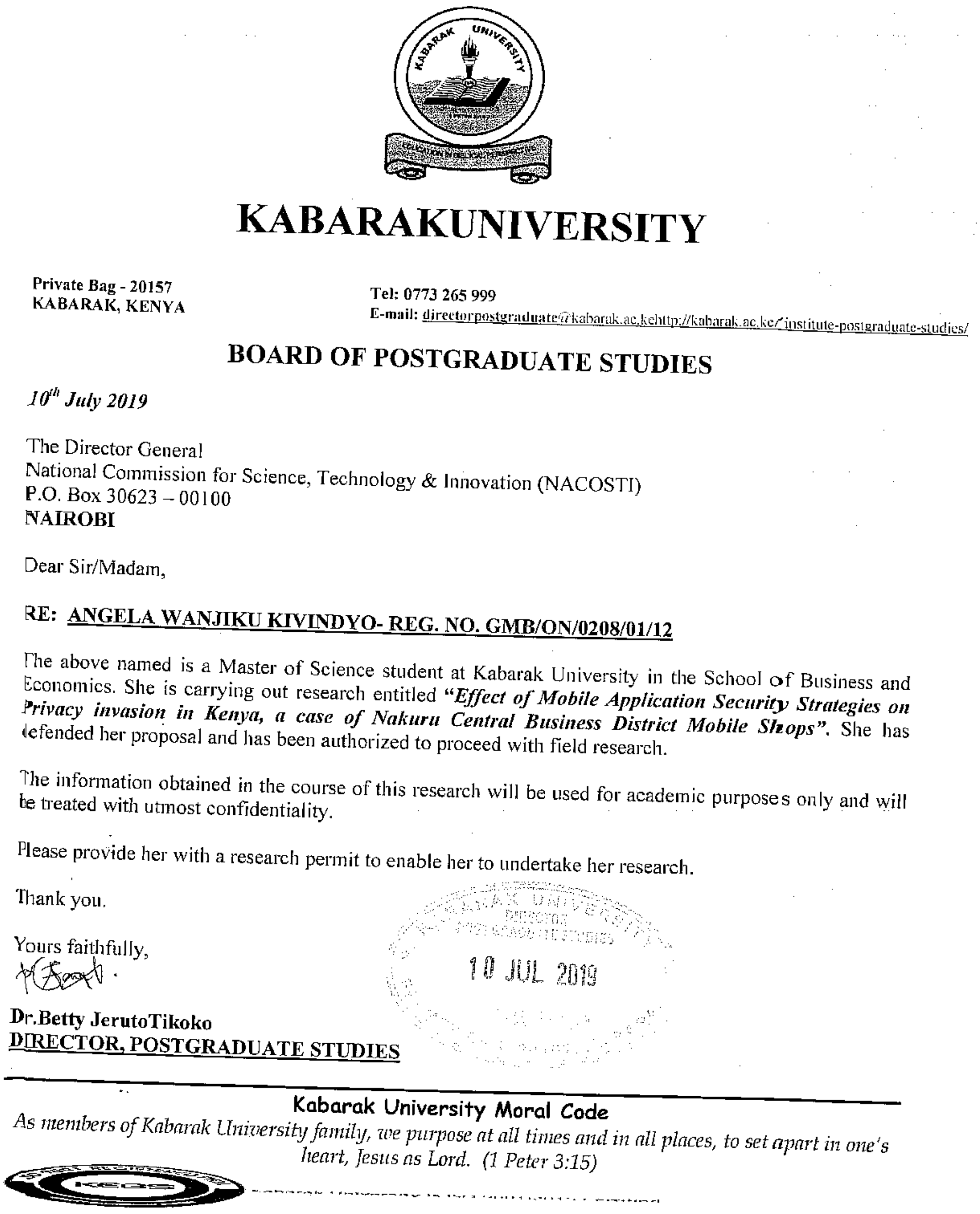
Using the following Likert scale, indicate your level of agreement or disagreement with regard to the stated propositions.

‘SA’ represents ‘Strongly Agree’; ‘A’ represents ‘Agree’; ‘NAND’ represents ‘Neither Agree nor Disagree’; ‘D’ represents ‘Disagree’; and ‘SD’ represents ‘Strongly Disagree’.

	SA	**A**	**NAND**	**D**	**SD**
6. I have in several occasions experienced privacy breach when using my mobile device.					
7. I have never experienced my private data or information stored in my mobile device being disclosed to the public.					
8. I have experienced impersonation of my identity.					
9. Third parties occasionally intrude into the content of my mobile device.					
10. I have experienced presentation of false information regarding me on mobile device.					
11. I am greatly concerned by invasion of my privacy by unsolicited persons/entities.					
12. Invasion of my privacy through mobile device has greatly affected my day-to-day life.					

Thank you for your time and cooperation.

Appendix III: Research Letter



KABARAKUNIVERSITY

Private Bag - 20157
KABARAK, KENYA

Tel: 0773 265 999
E-mail: directorpostgraduate@kabarak.ac.kehttp://kabarak.ac.ke/institute-postgraduate-studies/

BOARD OF POSTGRADUATE STUDIES

10th July 2019

The Director General
National Commission for Science, Technology & Innovation (NACOSTI)
P.O. Box 30623 – 00100
NAIROBI

Dear Sir/Madam,

RE: **ANGELA WANJIKU KIVINDYO- REG. NO. GMB/ON/0208/01/12**

The above named is a Master of Science student at Kabarak University in the School of Business and Economics. She is carrying out research entitled ***"Effect of Mobile Application Security Strategies on Privacy invasion in Kenya, a case of Nakuru Central Business District Mobile Shops"***. She has defended her proposal and has been authorized to proceed with field research.

The information obtained in the course of this research will be used for academic purposes only and will be treated with utmost confidentiality.

Please provide her with a research permit to enable her to undertake her research.

Thank you.

Yours faithfully,

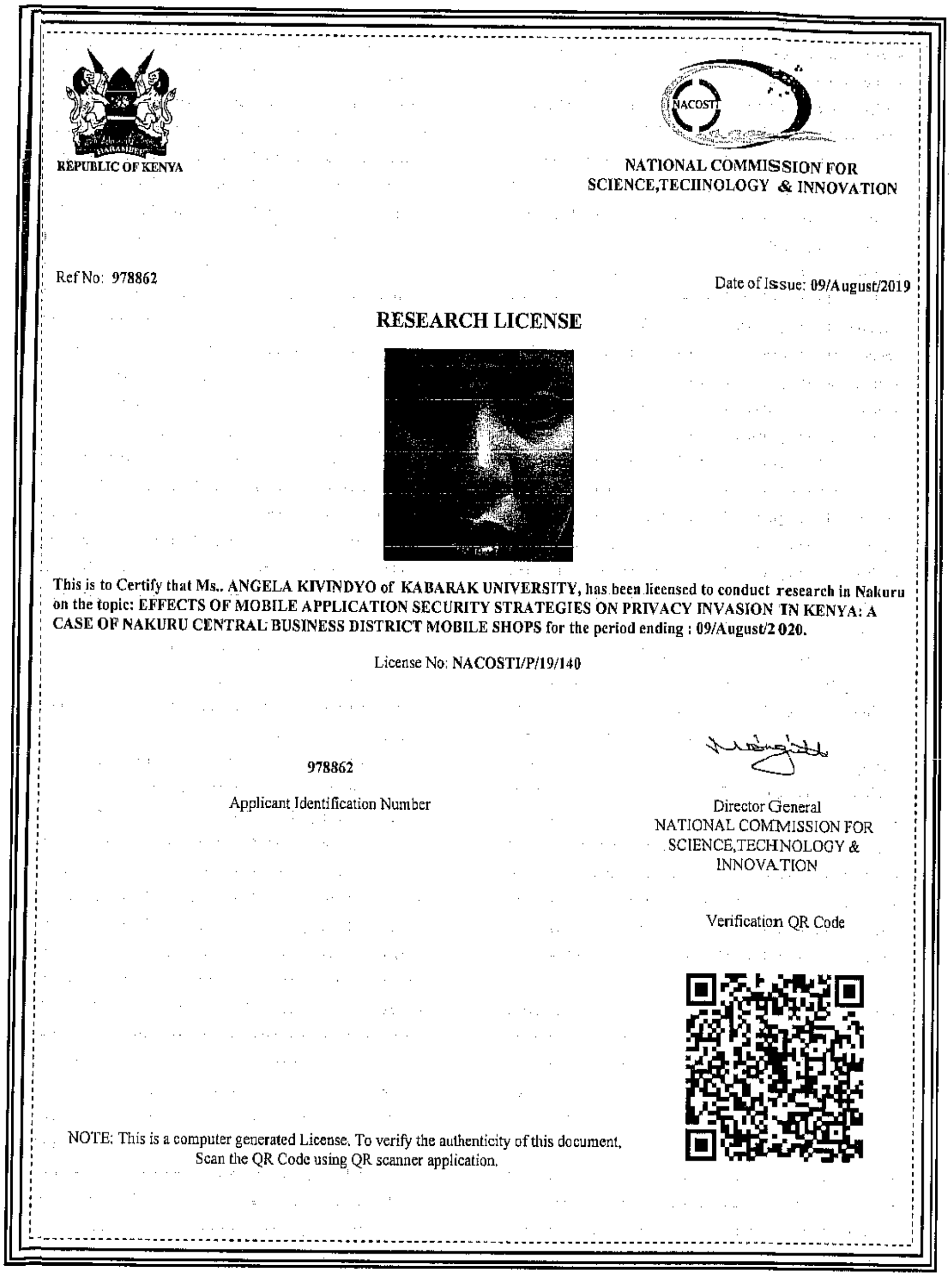
KABARAK UNIVERSITY
DIRECTOR
POSTGRADUATE STUDIES
10 JUL 2019

Dr.Betty JerutoTikoko
DIRECTOR, POSTGRADUATE STUDIES

Kabarak University Moral Code
As members of Kabarak University family, we purpose at all times and in all places, to set apart in one's heart, Jesus as Lord. (1 Peter 3:15)

KEBS

Appendix IV: NACOSTI letter



REPUBLIC OF KENYA

NATIONAL COMMISSION FOR
SCIENCE,TECHNOLOGY & INNOVATION

Ref No: 978862

Date of Issue: 09/August/2019

RESEARCH LICENSE

This is to Certify that Ms.. ANGELA KIVINDYO of KABARAK UNIVERSITY, has been licensed to conduct research in Nakuru on the topic: EFFECTS OF MOBILE APPLICATION SECURITY STRATEGIES ON PRIVACY INVASION IN KENYA: A CASE OF NAKURU CENTRAL BUSINESS DISTRICT MOBILE SHOPS for the period ending : 09/August/2020.

License No: NACOSTI/P/19/140

978862

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR
SCIENCE,TECHNOLOGY &
INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document,
Scan the QR Code using QR scanner application.

Appendix V: List of Sampled Mabile Shops in Nakuru Town

1. Blessed Communication
2. Bluen Tech Nakuru
3. Brendaa Mobile Technologies
4. Brother Dave Phone Accessories
5. Casjoy Smartphone
6. Centrium Communication
7. Computer World Nakuru
8. Dakom Communications
9. Giks Phone Repair
10. Glorious Communication
11. Hope shalom phones and accessories
12. iPhone Resellers
13. Jamia Online
14. Kasanga Mobiles
15. Kimcy Communications
16. Libla Connection Phones & Accessories
17. Lydia Arcarde (Jumia Shop)
18. Majesty solutions
19. Manchester solution mobile limited
20. Masto technologies
21. Max Tech Nakuru
22. Miharati Mobiles
23. Modern Mobiles
24. Modern Mobiles
25. M-Pesa Adtel Phone Company Ltd
26. M-Pesa Brasely Communications Ltd
27. M-Pesa Ushindi Communications Ltd
28. Muva technologies
29. N. M. Shah technologies
30. New Star Communication
31. Nimba technologies
32. Oppo Shop
33. Safaricom Shop
34. Splash Communication Mpesa
35. Superb General Suppliers
36. The mobile store
37. Urban technologies
38. Victory Phones Accessories Photocopy
39. Wintouch Nakuru
40. Shoppers Mobile Shops
41. Sage Telecommunication Limited

42. Amsa Communication Limited
43. Flash Dial Connections Ltd
44. Rumish Communication
45. Flamitechagencies
46. Vagutech Computers
47. Kwesmart Agencies
48. Soft Ventures East African Ltd
49. Heiz Electronics
50. Lustev Enterprises
51. Ushindi Communication Limited
52. Moneva Agencies
53. Lanstar Technologies Ltd
54. Comlink Investment Ltd
55. Adaresh Enterprise
56. Supreme Link Technologies
57. Centrtium Communication Limited
58. Al-Haqq Electronics
59. Telesonic Limited
60. Nakuru Stage Enterprises Limited
61. Pranshi Enterprises
62. Nakuru Computer Resources
63. Pace Connect Ltd
64. Geotab Telecommunications Ltd
65. Kims Collections
66. Lincret Enterprises
67. Savvoy Electricals
68. Ambok Technology Services
69. Mishku Communication Company Limited
70. Joalmo Mobile And Electronics
71. Ascom Ventures
72. Jazz Communication Limited
73. Digtronics System Two
74. Mishku Communication Co.Ltd
75. Techno Arch Concepts
76. Wise Power Technologies
77. Lydtec Enterprises