2018

# Assess the perceptions of personal data privacy amongst users and developers of mobile applications in Kenya

Roselyn M. Njuguna,
*Strathmore Business School (SBS)*
*Strathmore University*

# Assess the Perceptions of Personal Data Privacy amongst Users and Developers of Mobile Applications in Kenya

**Roselyn Muthoni Njuguna**

**Masters in Public Policy and Management**

**2018**

# Assess the Perceptions of Personal Data Privacy amongst Users of Mobile Applications in Kenya

**Roselyn Muthoni Njuguna**

**Submitted in partial fulfillment of the requirements for the Degree of Masters of Public Policy and Management at Strathmore University**

**Institute of Public Policy and Governance**

**Strathmore University**

**Nairobi, Kenya**

**June, 2018**

## DECLARATION

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.



.....

.....

.....

**Approval**

The thesis of Roselyn Muthoni Njuguna was reviewed and approved by the following:

Dr. Monica Kerretts
Strathmore Business School

Professor Robert Mudida
Head of School/Strathmore Institute for Public Policy and Governance (SIPPG)/Strathmore Business School

Professor Ruth Kiraka
Dean, School of Graduate Studies

## ABSTRACT

This paper aims to demonstrate the importance of understanding the right to privacy of personal data relating to someone's personal life. The objectives guiding this study were: to establish to what extent users of mobile applications understand that personal data collected through these applications was private. To understand the role of mobile application users in enhacing the knowledge of role of privacy when using mobile application. Finally, to establish to what extent mobile application users understood that they have a responsibility for their personal data. The paper utilized a descriptive research design.

A total of 259 respondents were interviewed in Nairobi County. The study found out that most users of mobile applications were aware of their right to privacy of personal data regarding their personal lives and families. The study found out that if mobile application users understood that they had rights with respect to personal data relating to their private and family life, they are most likely to protect any information they share when using mobile applications. Those who were aware of their rights to privacy were most likely to refuse to provide any information. However, majority of users were not aware they had a right to access and correct any personal data collected from their mobile applications.

From a mobile developers perspective, the study found out that creating knowledge on privacy amongst mobile application users such as purpose of collecting personal data, recipient of the data and how the data was to be processed increased users likelihood to know their rights to privacy. The study also found out that mobile application developers had an important role in educating users on how their information is being used. The study further found out that those agencies that had full access of your personal data, were most likely to transmit it to third parties. The study recommends that there is a need to fast track the Data Protection Bill in Kenya currently under discussion. Additionally, there is a need for greater collaboration amongst private and public sector organisations to enhance knowledge on the role of rights to privacy when collecting personal data.



**Key words**: Personal data, Privacy

## Table of Contents

## LIST OF TABLES

**ACKNOWLEDGEMENTS**

The knowledge I acquired through the help of the lecturers in Strathmore Institute for Public Policy and Governance (SIPPG) of Strathmore Business School at Strathmore University. First, I would like to appreciate the Director of SIPPG, Professor Robert Mudida, for his guidance and encouragement during my learning at the school.

Second my sincere thanks go to Dr. Monica Kerretts who was my research supervisor by supporting me during the period of my research project. The preparation and compilation of this report would have been impossible without her help.

Third, I also wish to appreciate Dr. Alfred Kitawi and Dr. Vitalis Onzianyi for their additional guidance and support.

Fourth, the SIPPG administrative department, Bildad Nyongesa and Cynthia Gathungu.

Finally, I wish to thank my close family and friends for their outstanding efforts they made through moral support, encouragement and understanding during the period I was carrying out this research project.

If I have failed to give recognition for help and materials received, it has been wholly unintentional and is deeply regretted. However, the ideas expressed in this research paper are those of the author and none of the above mentioned people should be held responsible.

May God bless you all, Amen.

## DEDICATION

To my husband, Philip and our daughters Imani and Yanira.

## LIST OF ABBREVIATIONS

| | |
|---|---|
| AG | Attorney General |
| BDSG | *Bundesdatenschutzgesetz* |
| CAK | Communication Authority Kenya |
| CCK | Commission of Kenya |
| COFEK | Consumer Federation of Kenya |
| DNPDP | *Dirección Nacional de Protección de Datos Personales* |
| ENISA | European Union Agency for Network and Information Security |
| EU | European Union |
| FTC | Federal Trade Commission |
| GoK | Government of Kenya |
| HRDs | Human Rights Defenders |
| ICO | Information Commissioner's Office |
| ICOPR | International Covenant on Civil and Political Rights |
| ICT | Information Communication & Technology |
| IFAI | *Instituto Federal de Acceso a la Informacióny Protección de Datos* |
| IoT | Internet of Things |
| MVNO | Mobile Virtual Network Operator |
| NSA | National Security Agency |
| NIS | National Intelligence Agency |
| OECD | Organization of Economic Co-operation and Development |
| PPI | Protection of Personal Information |
| PETs | Privacy-enhancing Technologies |
| PbD | Privacy by Design |
| UDHR | Universal Declaration of Human Rights |
| UK | United Kingdom |
| USA | United States of America |

## DEFINITION OF TERMS

| | |
|---|---|
| Personal data | Information about a person (Government of Kenya, 2013) |
| Privacy | The feeling that one has the right to own private information (Warren, 2003). |

# CHAPTER ONE: INTRODUCTION TO THE STUDY

This chapter begins by providing the definition of personal data and privacy. It continues by providing a detailed explanation on the privacy concerns raised against governments and private organisations globally and locally. Finally, this chapter will state the problem, provide an outline of the research objectives, define the scope of the study and finally justify the importance of the research findings.

## 1.1 Background of the Study

Imagine a world where we never thought private life was accessible with a click of a button. A world where your service provider whether financial, telecommunications, utilities, healthcare would have access to your private life. A world where your personal information could be easily exchanged with third parties without your knowledge. A world where you were not aware and there was not legal recourse for you. This is the world of the Internet of Things (IoT). It is a world where a person "quantified self," complete with the personal details of lifestyle, habits and activities all tracked and recorded (Cavoukian and Popa, 2016). There is no doubt that the innovation has brought about a new standard as to how business is carried out. In fact innovations in digitization health information have led to making information easy to access and share (Goldfarb & Tucker, 2012). As a new world order of disruption and innovation spanning from inappropriate online etiquette, cyber bullying and the over-sharing of personal information that constantly pushes privacy limits are just some of the issues the digital world has created, there is a need for an all-inclusive regulatory framework. Legislation and regulation will need to be up to speed with ever changing trends on toe with requisite policy, compliance and regulatory frameworks for the privacy of personal information are no more than one step behind (Ernst & Young, 2013).

## 1.2 Personal data

According to the Government of Kenya, personal data is referred to as information about a person. This means information such as race, gender, pregnancy, national, ethnic or social origin, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of an individual; information relating to information, medical, employment and financial transactions; identifying number, symbol assigned to an individual; fingerprinted and blood type; contact details (telephone number; correspondence sent to someone privately; persons opinions and information related to prize award (GoK, 2013).

### 1.3 Privacy

There has been varying scholarly debate on the most viable definition of privacy and they have being discussed for a long period of time. Solove (2006) notes that privacy is a concept in disarray that cannot be clearly articulated by anybody. In fact privacy is inherently difficult to reduce to a single definition that is rich enough to explain perceptions and behaviors across a range of contexts due to social and technical developments due to complexities between information, physicality and expression (Vasalou, Joinson & Houghton, 2014)

Privacy is defined as a "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Drinan, 1968). This definition was developed by Alan Westin based on the fact that intrusions on people's privacy took place through various unknown forms of scrutiny without prior knowledge by the person that their personal information was recorded and disseminated without his knowledge or consent (Drinan, 1968). Another author Arthur Miller defines privacy as the ability of a person to control the dissemination of information about himself (Stephenson, 1971).

According to Clarke (2006), privacy is the interest that individuals have in sustaining "personal space" free from interference by other people and organizations (Clarke, 2006). Clarke goes further to define different dimensions of privacy. These are privacy of a person, privacy of personal behavior, personal communications and personal data (Clarke, 2006). For the purposes of this dissertation, the privacy dimension to be focused on, is privacy of personal data. This is referred to variously as 'data privacy' and 'information privacy', and regulatory measures are referred to as 'data protection'. Individuals claim that data about themselves should not be automatically available to other individuals and organizations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. Many analysts focus on this dimension almost to the exclusion of the others. (Clarke, 2006).

### 1.4 Privacy Concerns through Surveillance by Government

#### 1.4.1 A Global Perspective

The appetite for personal data consumption is not a recent phenomenon. In fact the history of privacy concerns on personal information can be traced back to the early days of colonial America (Solove, 2006). In the book review *The Annals of the American Academy of Political and Social Sciences*, an overview of the history of privacy where both public and private sectors

are believed to intrude into people's beliefs, behaviors and attributes is provided (Manheim 1981). On the other hand Drinan (1968) posits that the intrusion by government and the private sector was enabled by listening and computer devices. In a book review of Arthur Miller, *Assault on Privacy,* it revealed that privacy was threatened by the growing use of computer technology and that safeguards are required if we are to limit the detrimental aspect of these omnipotent, omniscient tools (Stephenson 1971).

The intrusions to personal information manifested themselves in several ways. First during the revolutionary war in the United States of America (USA); citizens became increasingly worried with the intrusion of personal space by the government. During that time people were troubled with the government intruding people's houses and basements by searching, ransacking and quantifying everything people ate and drank. These government actions into people's personal space resulted to the development of the Bill of Rights into the Third, Fourth and Fifth amendments. These development ensured that the government was only compelled to only search people's houses by obtaining a judicial approval (Solove, 2006).

Second intrusion to privacy continued as government went further to review census and government Records in 1790. The census exercise was actually perceived to delve into people's personal lives rather than achieve the objective the census exercise was supposed to undertake. This necessitated parliament to formulate stricter laws to protect confidentiality of census records. The third intrusion of personal information privacy evolved itself through mail. Employees were suspected of reading citizens private letters. Upon complaints from the citizens, it compelled the passing of several laws by Congress in 1825. Fourth, threats emerged from the use of telegraph communication which was invented shortly after the civil war. At the time Congress seeking to gaining access and visibility on the telegraphs. This resulted in development of a bill to protect telegrams in 1880 by Congress (Solove, 2006).

### 1.5 The Kenyan Perspective

In Kenya, The State of Surveillance in Kenya Report by Privacy International and National Coalition of Human Rights Defenders-Kenya, documents several ways government surveillance has taken place in Kenya that could be classsifed as intrusion of privacy. In July 2015, the Kenyan intelligence services enlisted the services of intrusion malware company Hacking Team with the aim of shutting down a critical blog 'Kahawa Tungu' as a 'proof of concept' for their surveillance tools. This unprecedented move by the Kenyan government was seen as an

attempt to procure the Remote Control System tool that allows for remote hacking and control of target devices amongst its citizens.

In May 2014, the Kenyan government contracted Safaricom to set up a new surveillance system for the Kenyan Police, known as the Integrated Public Safety Communication and Surveillance System. The system was to (i) link all security agencies in order to facilitate information sharing and public safety activities and (ii) establish a surveillance camera system consisting of 1,800 CCTV cameras nationwide. The information collected included facial and movement.

In April 2014, the Kenyan government announced that it was registering all Kenyans in a new national digital database that would include biometric details as well as information on land ownership, establishments and assets. The aim of the programme was to facilitate the identification of people holding forged or false identification documents. Under the initiative dubbed Umoja Kenya Initiative, the government would collect all data pertaining to an individual including name, age, identities of relatives, property owned and residence.

In March 2013, shortly after the elections, the Kenyan government requested that mobile phone providers block text messages that were deemed to incite violence by using a firewall that would detect messages containing key words, identified beforehand, to be further analysed. At the time, it was reported that to the National Steering Committee on Media Monitoring of the Ministry of ICT had reportedly intercepted 300,000 texts messages during that time.

The Kenyan government through CCK entreated that all telecommunication service providers collaborate in the setting up of internet traffic monitoring equipment; known as the Network Early Warning System (NEWS). The CCK cited a rise in cyber security threats as a justification for this move.

In January 2013, The Citizen Lab of the University of Toronto reported that Blue Coat PacketShaper installations in countries including Kenya. Through these installalations, surveillance and monitoring of interactions mobile applications such as Facebook, Gmail, Skype and Twitter was being done.

In the year 2012, the Peace Brigades International stated in relation to human rights defenders (HRDs) in Kenya that “incidences of surveillance by state and non-state actors have been

reported. Some of the cases included offices raided or burgled, computers hacked while several organisations suspected that their phones were being tapped.

In December 2012, the Kenyan government set up the Integrated Population Registration System (IPRS). The aim of IPRS was to collect data from databases held by various government agencies. It combined data from birth and death registers, the citizenship register, ID card register, aliens register, passport register and the marriage and divorce register as well as elections register, tax register, drivers register, National Social Security Fund (NSSF) register, National Hospital Insurance Fund (NHIF) register and the Kenya National Bureau of Statistics (KNBS) register. At the time of deployment, Kenya had not adopted any data protection legislation to regulate the collection, centralisation and sharing of this type of data.

Not only was the Kenyan government conducting surveillance on its citizens, the US government was accused of secretly monitoring Kenyan citizens. In May 2014, The Intercept reported that a programme of the US National Security Agency (NSA) called MYSTIC secretly monitored the telecommunications systems of several countries including Kenya, through a system known as DUSKPALLET. The programme was described in internal documents as a program for embedded collection systems overtly installed on target networks, predominantly for the collection and processing of wireless/mobile communications networks. Evidence provided to The Intercept showed that the programme dated back to 2013, and that data gathered through it had been used to generate intelligence reports.

### 1.6 Privacy Concerns through Surveillance by Private Sector

#### 1.6.1 A Global Perspective

It is not only governments that intrude into people's personal information. Private organizations also intrude into personal information. In fact organizations view personal information as a corporate asset based on the heavy investment put in collecting customer personal information (Schwartz, 2004). Through data mining, organizations are using personal information to understand customer behavior. Organizations are using several methods to collect customer information from loyalty programs to mobile applications (apps). The success of this data collection is largely driven by innovation. There is no doubt the innovation has brought about a new standard as to how organizations are run (Ernst & Young, 2013). Mobile applications have become emerging technology through which personal data is collected. In fact, by 2015, there were over ninety three billion applications that had been transferred (Statista, 2015). Nakra

(2001), notes that privacy violations occur when a business entities use customers' information ranging from phone numbers to credit card histories to online behavior patterns in ways the customer did not unequivocally allow when first divulging the information. Database technology has long been in use without much concern over privacy issues.

According to Forbes magazine 2016, uknowkids.com a mobile application that tracks the online activity of your children had leaked 6.8 million texts and 1.8 million photos from children's phones. All the data that had been leaked came from mobile application platforms as Instagram, Facebook and Twitter because uknowkids.com had failed to lock down a database containing the information (Thomas, 2016). This information was leaked because its cyber-security provider Mackeepers failed to use any username and password making the information available and accessible for a staggering 48 days before it was locked down (Thomas, 2016). Also, a 300GB voter database of 191 million US voters that included names, home address, phone numbers, dates of birth, party affiliations and logs of whether or not they voted in the primary and general elections was left unprotected by the very same cyber-security provider of Uknowkids.com (Thomas, 2016).

In the U.S.A, mobile application developers such as Apple and Google argue that they have privacy policies which require their mobile applications to obtain permission before revealing certain kinds of user information (Thurm & Cane, 2010). However, on the other hand, complaints have been made of mobile applications collecting more information from users and distributing to third parties with user consent, knowledge or approval. The lack of standard practices (Thurm & Cane, 2010) that regulate how information is collected, how personal data is stored, coded and encoded results in different mobile application developers interpreting privacy based on their own interests.

In Singapore, the Straight Times, reported that almost ninety percent of mobile applications breached the Singapore privacy law. It was noted that users freely gave permission upon installation without any information how their personal information will be used. The core issue in the article was that mobile applications were collecting excessive information than they should be collecting. For example HSBC's mobile banking applications asked for user call logs and device identification, which was far more from the location service purposes. Another example included a calendar mobile application that asked for access to users' location and photos. It

also raised a pertinent issue that perhaps the developers of the mobile applications did not actually know that they were indeed contravening the law (Tham, 2015).

With the increased adoption of mobile money in Africa, mobile money services have become a necessity to operate in a data rich environment. For example, the mobile money ecosystem consists of mobile network operator, financial institution, service manager, marketer, retailer and the customer (Harris, Gooman & Traynor, 2013). With too many interested parties, there are high risks of personal data leakage with little customer privacy protection, hence resulting in great exposure of customer personal data (Harris, Gooman & Traynor, 2013).

### 1.6.2 A Kenyan Perspective

According to media monitoring company Reelforge between the period of 1st August, 2014 to 29th September 2015, fifty nine incidents were reported in the media relating to consumers expressing concerns about their privacy (ReelForge, 2015). The incidences reported on privacy intrusion such as mobile virtual network operator (MVNO) using thin-sim technology which was a new technology by Equity Bank. The risks associated with this was gaining access to customer information. Additionally, the use of Biometric Identity Cards for registration of persons capable of phishing through citizens' short messages and phone calls. On the other hand, consumers were worried about invasion of private health related information such as collection of information about individual HIV status (ReelForge, 2015).

Additionally, in 2014, reports of sharing of customer information without consent made news headlines in Kenya. While making reference to a text sent out by Safaricom to its customers that read in part "Following the impressive results the board has recommended a dividend payout of Kshs.0.47 per share". This message caused a huge uproar amongst customers complaints were raised specifically by a Safaricom customer as well as the Consumer Federation of Kenya (COFEK). Safaricom in their defense said they did not share their details with a third party so did the Communications Commission of Kenya (CCK) (CIO, 2014).

## 1.7 Problem Statement

Kenya does not currently have specific data protection legislation. However, a Data Protection Bill 2013 has been forwarded to the Attorney General for publication. The Bill was last discussed in February 2016 and has not yet been approved. The proposed Data Protection Act will immediately operationalize the implementation of Article 31(c) of the Constitution. It will also

regulate the collection, retrieval, processing, storing, use and disclosure of personal data (Privacy International, 2017).

From an organization' and consumer perspective, data mining of secondary information (personal information) has been the best disruptive innovation of the new age and has benefits attached to it. Data is the new natural resource. Time Business (2013) reports that information is the new currency. Most organizations infringe on their customers databases and share the information with third parties without their (customer's) consent. Complaints have been raised against telecommunication service providers for sharing of customers databases with third parties for the purposes of advertising.

Hence this research seeks to understand the role of privacy in safeguarding information deemed personal in nature.

### 1.8 Research Objectives

a) To determine to what extent mobile application users understand that personal data collected from mobile applications is private
b) To understand the role mobile application developers can play in enhancing knowledge on privacy
c) To establish to what extent users of mobile applications are taking responsibility for their personal data

### 1.9 Research Questions

a) Do mobile application users know that personal data collected from mobile applications is private?
b) Do mobile application developers understand they can play a role in enhancing knowledge on privacy?
c) Do users of mobile applications understand that they have a role in taking responsibility for their personal data?

### 1.10 Scope of the Study

This study will concentrate on the role of creating awareness of privacy with the aim of enhancing protection of user information against use without their knowledge.

### 1.11 Significance of the Study

As previously stated, misuse of personal information with user knowledge can be harmful. First, it can result to the isolation and seclusion of a customer humiliating facts are highlighted (Goldfarb & Tucker, 2012). For example, when a patient calls a medical facility to collect their results and the receptionist inadvertently discloses the patient's results in public, the patient may suffer psychological uneasiness especially if the information was unpleasant (Petronio, 2002).

Second, it can result to a security gap, especially if personal information is accessed by unauthorized persons (Culnan, 1993). For consumers that use mobile applications for financial transactions for example, mishandling of information may result to security breach as well as identity theft.

Third, it can result to an ethical issue as well as organizations strategy issues (Culnan, 1993). Finally, the lack of fair information practices has allowed marketers to phish information from consumers from the internet without their knowledge. Though there exists terms and conditions, most people will easily opt in for the sake of convenience (Tene & Polonetsky, 2012).

The purpose of this research therefore is to understand mobile applications users perceptions on privacy of mobile applications.

## CHAPTER 2: LITERATURE REVIEW

This chapter examines the type of personal data collected through mobile applications, theories and principles of privacy laws and a review of privacy laws in selected countries.

### 2.1 Personal Data Collection through Mobile Applications

Mobile applications are defined as software applications that are built to run on smartphones, tablet computers and other mobile devices. Mobile applications are used to provide mobility and reachability for users. Liang and Wei (2004) define six categories of mobile applications. First, time critical series that exploits the reachability property of mobile users for providing emergency and time-critical services. These include short message services, or alerts. Second, location-aware and location-sensitive services have the ability to identify the location of a mobile user or a moving target at a particular moment, for instance car tracing; also it creates significant value form mobile services. Third is Identity-Enacted Services are used to identify users. These include those used by mobile banking. Fourth is omnipresent communications and content distribution services whose role is mobile communications that facilitate personal contact anytime, anywhere such as 3G networks. Fifth business process rationalization that enhances the efficiency of business processes that include location-sensitive or time-critical activities to reduce transaction costs or improve service quality. Finally, mobile offices used for the office (Liang & Wei, 2004).

Mobile applications are available through intrinsic distribution platforms, so-called mobile application stores which are activated by the owners of the mobile operating system (Statista, 2015) as shown in Table 2.1-1.

**Table 2.1-1: Mobile Applications Usage Overview**

| Mobile App Usage Overview | Values |
|---|---|
| Number of mobile apps downloads worldwide | 102,062m |
| Projected number of apps downloads 2017 | 268,692m |
| Number of free mobile apps downloads | 92.88bn |
| Number of paid mobile app downloads | 9.19bn |
| Worldwide mobile app revenue | $34.99bn |

**Source**: Statista 2015

The perceived benefits of mobile application include: instrumental, experiential, identity, and social benefits. Instrumental benefits, refer to better task performance or enhanced productivity when using a mobile app (Yoo, 2010). Experiential is the fun experienced in using the mobile application. Identity is about mobile app is expressive of one's social or personal identity. Social benefits is the ability to connect with others through the mobile apps.

However, as mobile applications support services in healthcare, retail, financial services, marketing, gaming, entertainment, education (Statista, 2015), they also collect data that defined as personal data. McFarland (2014), notes that mobile applications collect both personal information such as names, addresses, phone numbers, email addresses and net IDs, transaction history, amount of assets, type of car owned, family situation, age, gender, geo location and so on, to target and adapt their advertising. This information that is generated from users without their knowledge is transmitted to third parties to support advertising and marketing. With marketers having an immense appetite for personal information, concerns continue to be raised whether customers willingly share their information freely (McFarland, 2014).

### 2.2 The Evolution of Privacy Laws

As technology evolved into computers, the development of privacy laws became very important thus making the evolution of privacy laws being deemed very significant. As the evolution continued, the formulation was of the regulation was not that strict. For example, the Freedom of Information Act of 1996 (USA) warranted any person could request personal records without necessarily stating the reason for requesting the information. However, some restrictions to access records were applied and specifically to medical ones. As the formulation and amendments in privacy laws continued, stricter laws were formulated. The Fair Information Practices (USA) on the other hand recommended that all personal data was to be kept in secret records and an individual must be notified that their personal information was to be used. The law further made it clear that individuals information could not be used for the purpose it was not intended for and one should be allowed to amend and correct records. Organizations, on the other hand were to take precautions to ensure that the personal information they had was reliable (Solove 2006).

In addition, the Fourth and Fifth Amendments of USA constitution, are the first laws to recognize the protection of an individual's personal information. For example, the Privacy of the Body Law

(USA) was actually established to protect against the physical body intrusions. Also the Fair and Accurate Credit Transactions Act of 2003 obligated all credit scoring agencies disclosing individual's credit scores should alert all agencies when doing so. The National Do-No-Call Registry allowed people to register phone numbers with the do-no-call registry and telemarketers could not access it. The CANSPAM Act 2003 restricted against sending commercial messages to deceive recipients. Remsburg v. Docusearch (2003) adopted a theory that mobile application developers could be liable to sharing information with third parties (Solove 2006).

William Prosser back in 1960 attempted to make sense of the landscape of privacy law by identifying four different interests. These included (i) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs, (ii) public disclosure of embarrassing private facts about the plaintiff, (iii) publicity which places the plaintiff in a false light in the public eye and (iv) appropriation for the defendant's advantage, of the plaintiff's name or like-ness. However, new technologies have given rise to a panoply of new privacy harms (Solove, 2006).

It is important to note that the role of privacy laws is protection of users' privacy by ensuring information that is not supposed to be disclosed stays that way. Solove (2006) argues that disclosure and breach of confidentiality causes different kinds of injuries to individuals. Privacy breaches not only reveal secrets about a person, but also violates the confidentiality placed in the trust in a specific relationship (Solove 2006).



### 2.3 Theory, Principles and Practice: A Review of a Selection of Privacy Protection Laws

Privacy law formulation should premise from the tenets of prevent, detect and respond. According to Hoepman (2013), the author notes that in the European Union, the legal right to privacy is founded on Article 8 of the European Convention of Human Rights of 1950.

#### 2.3.1 International Conventions on Privacy

Kenya is a signatory to the Universal Declaration of Human Rights (UDHR) and has ratified the International Covenant on Civil and Political Rights (ICCPR). Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation".

### 2.3.2 The OECD guidelines

In the perspective of data protection, this right was made categorical in the 1995 data protection directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, which is based on the privacy guidelines of the Organization of Economic Co-operation and Development (OECD) from 1980. The OECD privacy guidelines are based on notice, choice, access and security of which eight principles on privacy are based on (Hoepman, 2013). First, the collection limitation principle states that there should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Second, data quality principle states that personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. Third, purpose specification principle states that the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. Fourth, use limitation principle states that personal data should not be disclosed, made available or otherwise used for purposes other than those.

Fifth, security safeguards principle, states, personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. Sixth, openness principle states that, there should be a general policy of openness about developments, practices and policies with respect to personal data. That is, means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller. Seventh, individual participation principle states that an individual should have the right to obtain the right data, communicated to the user with reasons and has the ability to challenge the data. Finally, the accountability principle states that a data controller should be accountable for complying with measures which give effect to the principles stated above (OECD, 1980).

### 2.3.3 Data protection in Europe

European data protection laws note that personal data must be processed fairly and lawfully, must be collected for a specified purpose, and must not be further processed in a way

incompatible with those purposes. Furthermore the data must be adequate, relevant, and not excessive. It must be accurate and up to date, and kept no longer than necessary. These provisions express a need for purpose limitation, data minimisation, and data quality (Hoepman, 2013).

### 2.3.4 The ISO 29100 Privacy Framework perspective

The ISO 29100 Privacy Framework is based on eleven privacy principles as a response to the growing concerns on data privacy. First, consent and choice requires that an entity must inform data subjects, present the available choices and obtain consent. Second, purpose legitimacy and specification ensures compliance with data protection legislation and inform data subjects. Third, collection limitation limits data collection to what is needed for the purpose. Fourth, data minimisation decreases the amount of personal data collected, the number of actors that have access, offer a default non-privacy invasive options, and deletes data once it has become irrelevant. Fifth, the use, retention and disclosure limitation, limits the use, retention and disclosure of personal data to what it is needed for. Sixth, accuracy and quality, ensures that the data is accurate, upto- date, adequate and relevant, verify this, and periodically check this.

Seventh, openness, transparency and notice, informs data subjects about the data controller policies, give proper notices that personal data is being processed, and provide information on how to access and review personal data. Eighth, individual participation and access, gives data subjects a real possibility to access and review their personal data. Ninth, accountability, documents, policies, procedures and practices, assign the duty to implement privacy policies to specified individuals in the organisation, provide suitable training, inform about privacy breaches, give access to effective sanctions and procedures for compensations in case of privacy breaches. Tenth, information security provides a proper level of security, and implement the right controls, based on an appropriate risk assessment. Finally, privacy compliance verifies and demonstrates that the IT systems meets legal requirements, and have appropriate internal controls and supervision mechanisms (Hoepman, 2013)

### 2.3.5 A Review of Privacy Laws in Selected Countries

A total of ten countries have been reviewed across five continents. The following parameters were used in the review. They include: Country, Definition of personal data, Data protection authority, Registration of databases, Collection and processing, Transfer, Security, Breach Notification and Online Privacy (DLA Piper, 2012).

Argentina defines personal data as any type of information related to identified or identifiable individuals or legal entities. Registration of databases is governed by *Dirección Nacional de Protección de Datos Personales* (DNPDP). There are no restrictions for collection and processing of personal data and the user is not always required for approval in sharing personal information to third parties, however the transfer of data is governed by European Commission guidelines. While security of personal data is a key requirement, there is no specific requirement to report notifications neither does the legislation to govern online privacy exists.

In Brazil, there is no legal definition for personal data or data protection authority. However, the collection and processing of personal data as well as online privacy is established under the Brazilian Internet Act. The transfer, security and breach of personal data have no specific requirements with the exception of transfer of health and government records.

China defines personal data as any data or information in connection with a specific individual or can be used, separately/combined with other data. The registration, transfer and breach of privacy of online personal data have no requirements with the exception of security that is regulated under Article 29 of the Consumer Rights Law that only applies to business operators collecting customer personal information.

In Germany, personal data is defined as information concerning the personal or material circumstances of an identified or identifiable natural person ('data subject'). Whilst there does not exist a requirement to register databases, the collection, processing and breach of the personal data is regulated under explicit consent from Federal Data Protection Act (*Bundesdatenschutzgesetz* in German) (BDSG). There does not exist any requirements for transfer of personal data, however with regards to online privacy, users must always be informed on the use of cookies in a privacy notice

India defines personal data as any information that relates to a natural person, which either directly or indirectly, combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person. There is no requirement for registering databases as a data protection authority does not exist as well as online privacy. The collection and transfer of data requires consent from the user. Whilst the security of the database

requires approval from General Government, in case of a breach on the personal data, this is regulated by Computer Emergency Response Team (Cert-In).

Mexico defines personal data as information concerning an identified or identifiable individual. The collection, processing, security, breach and online privacy are regulated under the Federal Institute for Access to Information and Data Protection (*Instituto Federal de Acceso a la Informacióny Protección de Datos*) (IFAI) and the Ministry of Economy (*Secretaría de Economía)*. There is no requirement for registration of databases though, regulations for transfer exist, there is no requirement of data subject to be informed nor consent sought when the transfer of data is done.

In South Africa personal data is defined as identifiable, living, natural person, and where applicable, an identifiable juristic person/legal entity. The transfer, security and breach of data is regulated under Protection of Personal Information (PPI) Act, Information Protection Regulator. There are no regulations on registration of databases and online privacy.

The United Kingdom (UK) defines personal data as any information relating to a data subject where the data subject means a natural person. The registration, collection, processing, and transfer are regulated by the Information Commissioner's Office (ICO). However, on data transfers in Europe, the European Commission (EU) rules apply. Additionally, on online privacy, implied consent is allowed.

In the United States of America (USA), personal data is defined as information that can reasonably be used to contact or distinguish a person, including IP addresses and device identifiers. The regulating agency is Federal Trade Commission (FTC) and there is no requirement of registration of databases and transfer. However, with transfer, government records are regulated. Collection, processing, security and breach is regulated. There is no specific federal law on online privacy, but the development of codes of conduct for mobile applications privacy is well underway.

From the summary above, it is clear that there is a deliberate effort by governments across the world to protect and manage collection, usage and storage of personal information. Countries, specifically in the European Commission block, intentionally implemented privacy laws. It can also be noted that countries are not well equipped to develop privacy laws in the existing

dynamic technological environment. The gap is in the knowledge with which these countries are well equipped in understanding dynamic environments and developing privacy laws to match the fast pace environment.

### 2.4 Privacy Laws in Kenya

The Constitution of Kenya, Article 31 part (c) states that every person has the right to privacy to (a) their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed (Government of Kenya, 2013).

Second, Kenya does not have a law on cybercrime however, the 2014 draft Cybercrime and Computer Related Crimes Bill 10 seeks to equip law enforcement agencies with the legal and forensic tools to tackle cybercrime. Third, data retention is governed by the 2009 Kenya Information and Communications Act regulates the retention of electronic records and of "information in original form". Upon further scrutiny of the Kenya Information and Communications Act Section 15(1) of the Kenya Information and Communications (Consumer Protection) Regulations 2010, states that a licensee "shall not monitor, disclose or allow any person to monitor or disclose, the content of any information of any subscriber transmitted through the licensed systems by listening, tapping, storage, or other kinds of interception or surveillance of communications and related data" (Privacy International, 2017).

The recently adopted 2009, Kenya Information and Communications has the following provisions: Article 31 "A licensed telecommunication operator who otherwise than in the course of his business - (a) intercepts a message sent through a licensed telecommunication system; or (b) discloses to any person the contents of a message intercepted under paragraph; or, (c) discloses to any person the contents of any statement or account specifying the telecommunication services provided by means of that statement or account, commits an offence and shall be liable on conviction to a fine not exceeding three hundred thousand shillings or, to imprisonment for a term not exceeding three years, or to both." Article 83W states that (1) Subject to subsection (3), any person who by any means knowingly: (a) secures access to any computer system for the purpose of obtaining, directly or indirectly, any computer service; (b) intercepts or causes to be intercepted, directly or indirectly, any function of, or any data within a computer system, shall commit an offence. Article 93 (1) states that no information with respect to any particular business which - (a) has been obtained under or by virtue of the provisions of

this Act; and b) relates to the private affairs of any individual or to any particular business, shall, during the lifetime of that individual or so long as that business continues to be carried on be disclosed by the Commission or by any other person without the consent of that individual or the person for the time being carrying on that business (Privacy International, 2017).

The proposed Data Protection Bill 2013 Part II (7) 1 on Duty to Notify, states that "Before an agency collects personal information directly from a data subject, the agency must take steps are in the circumstances to ensure that the data subject is aware (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipient of the information; (d) the name and the address of the agency that is collecting the information, the agency that will hold the information and whether or not any other agency will receive the information; (e) where the information is collected pursuant to any laws; (f) the consequences if any, where the data subject fails to provide all or any part of the requested information; and (g) the rights to access to, and correction of, personal information provided under section 12 an 13 of this Bill". The Bill does not in anyway specify the need to acquire user consent before the collection of personal information. In addition to this, there is no clear directive what happens when if users would like to opt out to use of their personal information but still continue using the services.

### 2.5 Government Actors in Regulating Data Privacy in Kenya

There are several government actors in law enforcement. First, there is the CA that was established in 1999 and is responsible for facilitating the development of the ICT sector, including broadcasting, multimedia, telecommunications, electronic commerce, postal and courier services. Second, National Intelligence Agency (NIS). The primary function of the NIS is to gather, collect, analyse and transmit or share with the relevant state agencies, security intelligence and counterintelligence with an aim of detecting and identifying threats or potential threats to national security. It also advises the President and government of these threats, and transmits intelligence information to other agencies. Third is the National Security Council (NSC) that oversees intelligence operations. The council is comprised of the President, Cabinet Secretaries, including the Secretaries responsible for defence, foreign affairs, and internal security; the Attorney-General (AG); the Chief of Kenya Defence Forces; the Director-General of the National Intelligence Service; and the Inspector-General of the National Police Service. Finally, is the National Police that collects and provide criminal intelligence; undertake investigations on serious crimes such as cybercrime. National Police has surveillance powers,

established in the National Police Service Act 201127 and the National Police Service Commission Act 2011.

### 2.6 Conclusion

With increased technological advances, customers will be subjected to new methods e-marketing as organizations seek competitive advantage. With customers seeking convenience, invasions of privacy occur when there is loss of control resulting from marketing exchanges (O'Malley and Prothero, 2004). That not-withstanding, a forward looking approaching policy keeping in mind the changes must be fully developed to protect customers. If this does not change customers will be subjected to sharing of information through the Internet and risking their personal information in a virtual environment where they have no control.

However, the purpose of this research is to review if users of mobile applications understand their role in maintaining the privacy laws. The information from this research thesis be used to better inform mobile application users and developers on the role of data protection.

# CHAPTER 3: RESEARCH METHODOLOGY

This chapter presents an outline of the research design, unit of analysis, population and sampling, data collection methods, data analysis, research quality and ethical considerations is considered.

## 3.1 Research Design

The proposed research design was descriptive research design. Descriptive research design is used to investigate what if type of questions (Knupfer, 2001). The purpose of selecting this research design was to investigate what attributes were important to create more awareness on the right to privacy, enhance knowledge on the role of privacy and what responsibility individuals must take to protect their personal data.

## 3.2 Unit of Analysis

The primary unit of analysis was users and developers of mobile applications. The justification for including this cohort was to gain an understanding of users and developers perceptions on privacy.

## 3.3 Population and Sampling

### 3.3.1 Population

Population is referred to the entire group of individuals, events or objects having a common observable characteristic (Mugenda & Mugenda, 1999). The target population for this study will be individuals that use and develop mobile applications.

### 3.3.2 Sampling

Sampling is the process of selecting a number of individuals for a study in such a way that the individuals selected represent the large group which they were selected (Mugenda & Mugenda, 1999). The sample for this study was selected through purposive sampling. Purposive sampling involves the selection of specific cases for a specific purpose (Teddlie & Yu, 2007). For the purpose of sampling, Nairobi region was selected. Nairobi was selected due to its economic strength by having the largest county-level GDP. (World Bank, 2016).

**Mobile application users**

In order to determine the sample size, the formula used has been adapted from (Mugenda & Mugenda, 1999) for populations that could be higher than ten thousand (10,000) users. According to the 2009 Kenya Population and Housing Census, Nairobi County has a population of 3,138,369 million people living in the county (KNBS, 2015).

$$n = \frac{Z^2pq}{d^2}$$

Where N (population size) of 3.1 million people in Nairobi smart phone users, z (confidence level of 1.96, E is the error at 0.05, P and Q values are 0.5 respectively. The total target sample n is 385.

**Mobile application developers**

For this, mobile application developers will be sourced randomly from developers of mobile applications. A total of twenty five (25) mobile application developers will be targeted.

### 3.4 Data Collection Methods

A quantitative data collection approach was used. According to Creswell (2009), a quantitative approach typically uses survey instruments, so that numbered data can be analyzed using statistical procedures.

#### 3.4.1 Research Instruments

A research instrument was used to collect primary information. The data collection involved the gathering numeric information so that the final database represented quantitative information (Creswell 2003). Questionnaires were the main method of collecting data. The questionnaires comprised of structured questions.

#### 3.4.2 Data Collection Procedures

The questionnaires were administered through face to face interviews with participants.

#### 3.4.3 Reliability and Validity

Reliability refers to whether scores to items on an instrument are internally consistent, stable over time (test-retest correlations) and whether there was consistency in test administration and scoring (Creswell, 2009). Validity and reliability are two fundamental elements in the evaluation of a measurement instrument. Validity is entails the extent to which an instrument measures

what it is intended to measure. Reliability is concerned with the ability of an instrument to measure consistently. The reliability of an instrument is closely associated with its validity. An instrument cannot be valid unless it is reliable. Cronbach's alpha is the most widely used objective measure of reliability. Alpha was developed by Lee Cronbach in 1951 to provide a measure of the internal consistency of a test or scale expressed as a number between 0 and 1 (Tavakol & Dennick, 2011). For this study, Cronbach's Alpha was adopted.

### 3.5 Data Analysis

The analysis technques used were frenquencies and descriptive stastistics to provide a overview of the attributes. In addition, correlation statistical analysis was used to identify the which attributes were strongly correlated to privacy, knowledge and responsibility.

### 3.6 Research Quality

To ensure research quality, the following steps were undertaken. Firstly, to include sufficient raw data in the report and secondly, choose the most informed respondent.

### 3.7 Ethical Considerations

#### 3.7.1 Confidentiality and privacy

The study ensures that all information provided by respondents has remained confidential (Mugenda & Mugenda, 1999).

#### 3.7.2 Anonymity

The identity of respondents shall not be revealed to third parties without their knowledge (Mugenda & Mugenda, 1999).

# CHAPTER 4: PRESENTATION OF RESEARCH FINDINGS

This chapter presents the findings of the study. The study targeted 385 mobile application users and 25 mobile application developers. Of the 385 mobile application users targeted, a sample of 259 respondents was achieved representing a response rate of 67%. On the other hand all 25 questionnaires targeting the mobile application developers were achieved representing a 100% response rate.

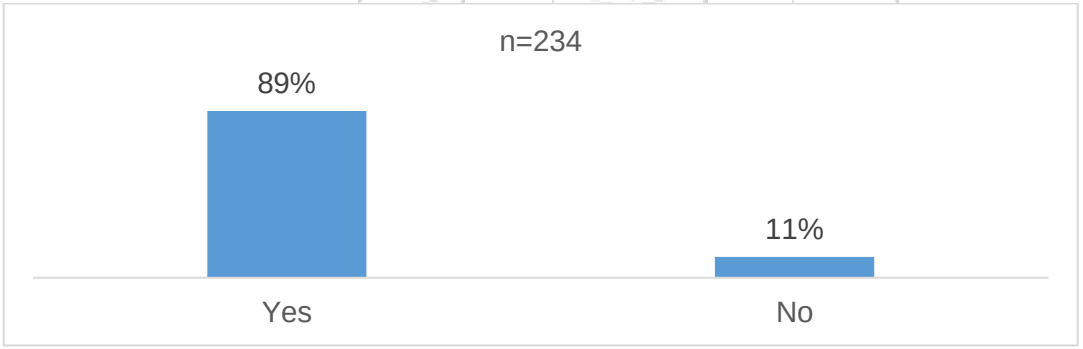
The presentation of the findings is based on the objectives. These are: to determine to what extent mobile application users understand that personal data collected from mobile applications is private; to understand the role of mobile application developers can play in enhancing knowledge on privacy and to establish to what extent users of mobile applications are taking responsibility for their personal data

## 4.1 Privacy of personal data

### 4.1.1 Awareness of the right to privacy

The study required to find out if mobile applications users were aware that every person had a right to privacy with respect to their personal data. 89% of the respondents agreed they were aware of that right as shown in Table 4.1.1-1.

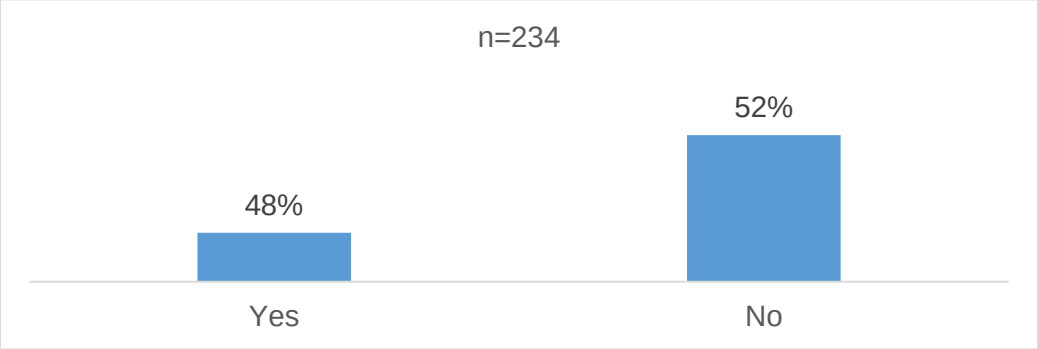
**Table 4.1.1-1: Awareness of the right to privacy**




### 4.1.2 Right to access and correct personal data collected through mobile applications

The study sought to find out if users were informed that they had the right to correct any informaiton collected by mobile applications. 52% of the people interviewed indicated they had not been provided with that information as shown in Table 4.1.2-1.

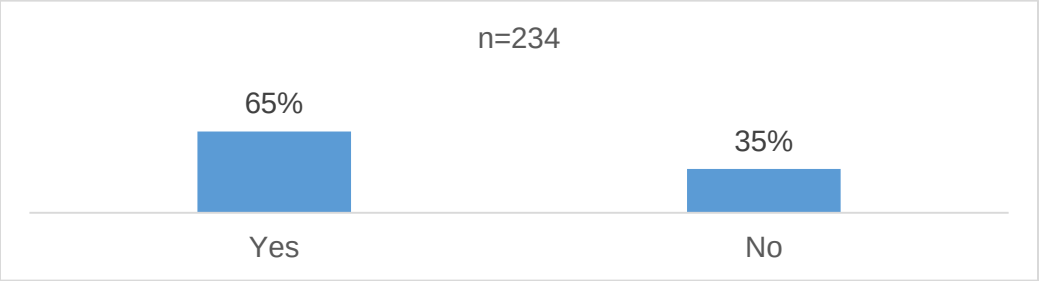
**Table 4.1.2-1: Right to access and correct personal data**




### 4.1.3 Right to refuse to provide personal data

The study further sought to find out is users were aware they had the right to refuse to provide personal data on mobile applications. 65% of the people interviewed said they were aware of the right to refuse to provide such informaiton as shown Table 4.1.3-1.

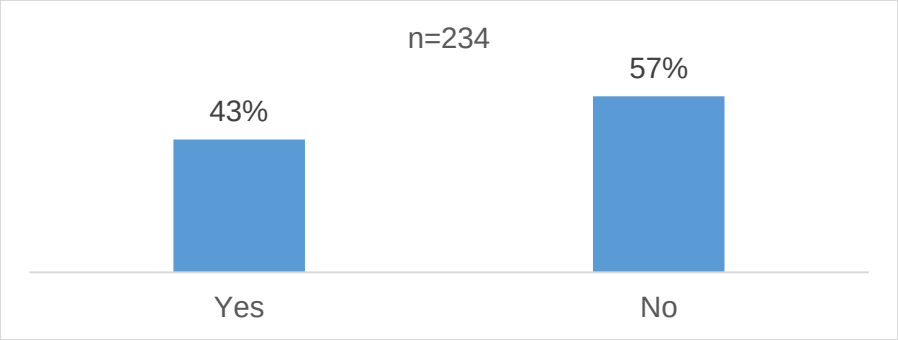
**Table 4.1.3-1: Right to refuse to provide personal data**




### 4.1.4 Type of personal data being processed from your mobile application

The study required to find out if users were informed of the type of personal data processed from mobile applications. 57% of the people interviewed said they were not informed of the type of information processed as shown in Table 4.1.4-1.

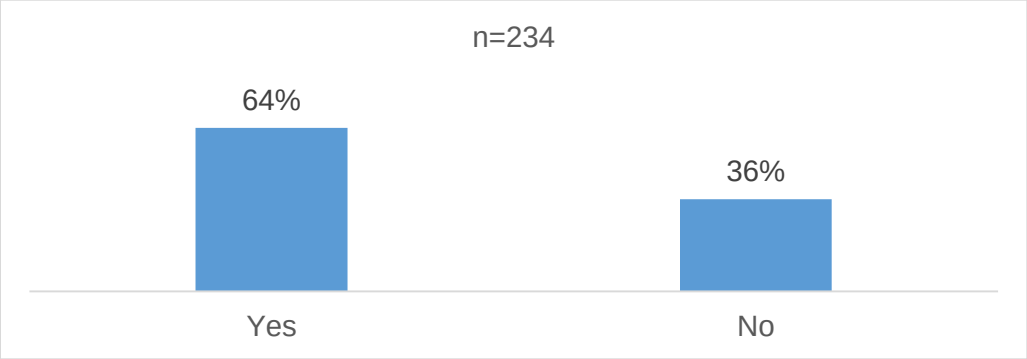
**Table 4.1.4-1: Type of personal data being processed from your mobile application**




### 4.1.5 Correction of information collected through mobile applications

The study required to find out if users were able to correct information provided to mobile applications. 64% of the people interviewed said they were able to rectify personal data as shown in Table 4.1.5-1.

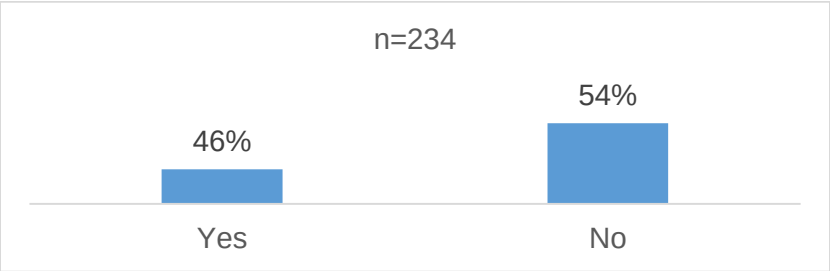
**Table 4.1.5-1: Correction of informaiton collected through mobile applications**




### 4.1.6 Consent for use of personal data

The study sought to find out if users provided consent for their personal data to be provided for commercial purposes. 54% of those interviewed indicated their consent had not been sought as shown in Table 4.1.6-1.

**Table 4.1.6-1: Consent for use of personal data**



### 4.1.7 Correlation analysis on right to privacy of personal data

The study sought to investigate the relationship between attributes related to privacy of personal data. The study found out that there is strong correlation between knowledge of privacy rights and ability to access and correct any information about themselves (p=0.02). In addition, there is a strong correlation between right to refuse to provide personal data with rights to privacy (p=0.00) and right to access and correct personal data (p=0.00). The study also found out that there was a strong correlation between information on how data will be processed with rights to privacy (p=0.010), right to access, correct personal data (p=0.00) and the right to refuse to provide that personal data (p=0.039). Further the study found that there was a strong correlation between ability to correct information with rights to privacy (p=0.014) and right to access, correct personal data (p=0.00) and the right to refuse to provide that personal data (p=0.019) as shown in Table 4.1.7-1.

**Table 4.1.7-1: Correlation analysis on right to privacy of personal data**

| | | Awareness of the right to privacy | Informed of your rights to access data | Informed of the right to refuse to provide personal data | Informed of processing of personal data | Ability to correct personal data | Consent for use of personal data |
|---|---|---|---|---|---|---|---|
| Awareness of the right to privacy | Pearson Correlation | 1 | | | | | |
| | Sig. (2-tailed) | | | | | | |
| | N | 234 | | | | | |
| Informed of your rights to access data | Pearson Correlation | .203** | 1 | | | | |
| | Sig. (2-tailed) | .002 | | | | | |
| | N | 234 | 234 | | | | |
| Informed of the right to refuse to provide personal data | Pearson Correlation | .278** | .371** | 1 | | | |
| | Sig. (2-tailed) | .000 | .000s | | | | |
| | N | 234 | 234 | 234 | | | |
| Informed of processing of personal data | Pearson Correlation | .168* | .262** | .135* | 1 | | |
| | Sig. (2-tailed) | .010 | .000 | .039 | | | |
| | N | 234 | 234 | 234 | 234 | | |
| Ability to correct personal data | Pearson Correlation | .161* | .289** | .153* | .052 | 1 | |
| | Sig. (2-tailed) | .014 | .000 | .019 | .427 | | |
| | N | 234 | 234 | 234 | 234 | 234 | |
| Consent for use of personal data | Pearson Correlation | -.055 | -.029 | .006 | -.003 | .067 | 1 |
| | Sig. (2-tailed) | .406 | .659 | .933 | .968 | .305 | |
| | N | 234 | 234 | 234 | 234 | 234 | 234 |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | | | | | |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | | | | | |

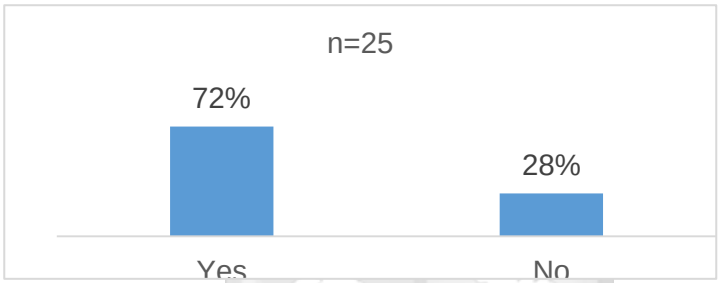
### 4.2 Enhancing the knowledge on privacy

The aim of this objective was to understand if developers understood their role in providing knowledge to customers in order to enhance their knowledge on privacy.

#### 4.2.1 Purpose of collecting the personal information

The study required to find out if mobile application developers provided information on the purpose of collecting personal data. 72% indicated they provided they informed users the purpose of collecting personal data as shown in Table 4.2.1-1.

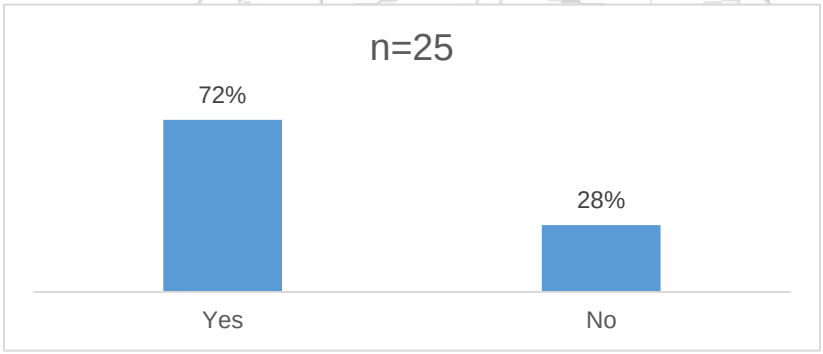
**Table 4.2.1-1: Purpose of collecting the personal information**




#### 4.2.2 Intended recipient of collected information

The study sought to find out if mobile application developers informed users of the intended recipient of personal data. 72% of the mobile developers interviewed that they had informed users of the recipients of their data as shown in Table 4.2.2-1.

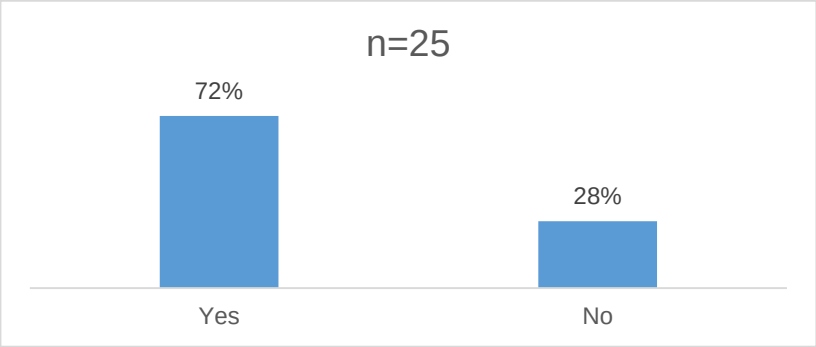
**Table 4.2.2-1: Intended receipient of collected information**




#### 4.2.3 Name of agency collecting the information

The study sought to find out if mobile application developers informed users of the agency collecting their personal data. 72% of the mobile developers interviewed that they had informed users of the name of the agency collecting the data as shown in Table 4.2.3-1.

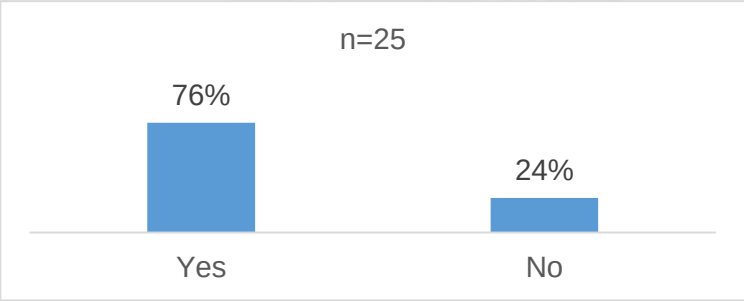
**Table 4.2.3-1: Name of agency collecting the information**




### 4.2.4 Right to access and correct personal data collected

The study sought to find out if developers informed users of the right to access and correct personal data collected. 76% indicated they provided that information to users and indicated in Table 4.2.4-1.

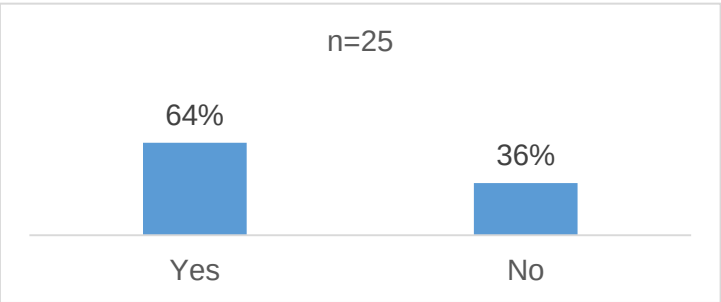
**Table 4.2.4-1: Right to access and correct personal data collected**




### 4.2.5 Inform users prior to collecting personal data

The study further sought to find out if developers informed users that their personal data was been collected. 64% of those interviewed indicated they had provided that information as shown Table 4.2.5-1.

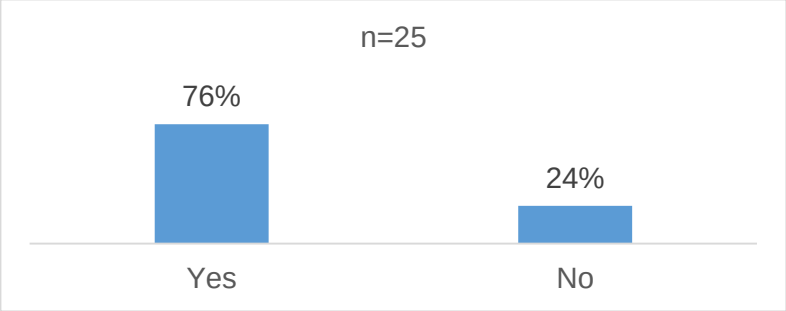
**Table 4.2.5-1: Inform users prior to collecting personal data**



### 4.2.6 Inform users rights to refuse to collection of personal data

The study required to find out if they informed users that they had the right to refuse to have their personal information collected. 76% indicated that they informed their users on their rights to refuse to have their data collected as shown in Table 4.2.6-1.

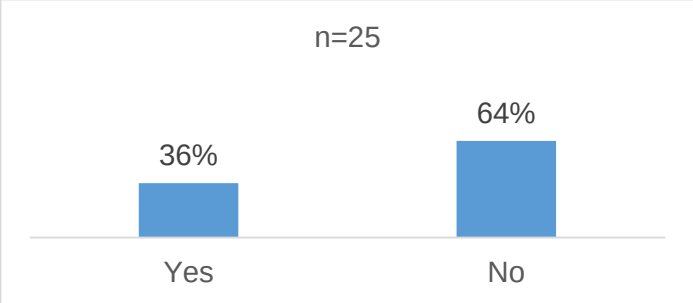
**Table 4.2.6-1: Inform users rights to refuse to collection of personal data**




### 4.2.7 Inform users of type of personal data processed

The study further sought to find out if developers informed users the type of personal data is to be processed. 64% of the developers indicated they did not provide such information as shown in Table 4.2.7-1.

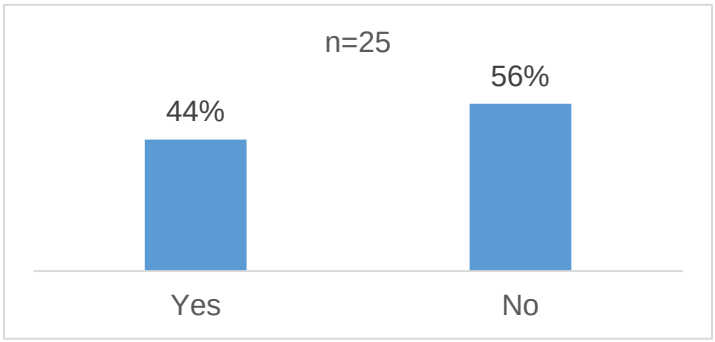
**Table 4.2.7-1: Inform users of type of personal data processed**




### 4.2.8 Inform users during transmission of personal data

The study sought to find out if mobile application developers informed users when transmission their personal data to third parties. 56% of those interviewed indicated that they did not provide such information as shown in Table 4.2.8-1.

**Table 4.2.8-1: Inform users during transmission of personal data**




### 4.2.9 Correlation to understand the role of knowledge in enhancing privacy

The study found out that there was a strong correlation between advising users the name of agency collecting the information and intended recipient (p=0.045). The study also found out that there was a strong correlation users the right to access and correct personal data with providing information of the intended recipient (p=0.000) and name of the agency collecting the information (0.014). The study further found out that there was a strong correlation between informing users prior to their information being collected with intended recipient (p=0.000), name of the agency collecting the information (p=0.021) and right to access and correct information 0.004). In addition, the study found out that there was a strong correlation between informing users of the purpose of collecting personal data with name of the agency collecting the information (p=0.27), right to access and correct personal data (p=0.006) and providing prior information on collection of personal data (0.022). Further, the study found out that there is a strong correlation between informing using of the type of information collected with name of the agency collecting the information (p=0.09) and right to access and correct personal data (p=0.021). Finally, the study found out that there is a strong correlation between providing information on type of personal data being collected and the type of data being processed (p=0.043) as shown in Table 4.2.9-1.

## Table 4.2.9-1: Correlation to understand the role of knowledge in enhancing privacy

| | | Inform users the purpose of collecting personal data | Inform users the intended recipient of personal data | Inform users of name and agency collecting persona data | Inform users right to access and correct personal data | Inform users prior to personal data collection | Inform users their right to refuse | Inform users the purpose of collecting personal data | Inform users of personal data being processed | Inform users personal data is being transmitted to 3rd parties |
|---|---|---|---|---|---|---|---|---|---|---|
| Inform users the purpose of collecting personal data | Pearson Correlation | 1 | | | | | | | | |
| | Sig. (2-tailed) | | | | | | | | | |
| | N | 25 | | | | | | | | |
| Inform users the intended recipient of personal data | Pearson Correlation | 0 | 1 | | | | | | | |
| | Sig. (2-tailed) | 0.322 | | | | | | | | |
| | N | 25 | 25 | 25 | | | | | | |
| Inform users of name and agency collecting persona data | Pearson Correlation | 0.008 | .405* | 1 | | | | | | |
| | Sig. (2-tailed) | 0.970 | 0.045 | | | | | | | |
| | N | 25 | 25 | 25 | 25 | | | | | |
| Inform users right to access and correct personal data | Pearson Correlation | 0 | .693** | .484* | 1 | | | | | |
| | Sig. (2-tailed) | 0.751 | 0.000 | 0.014 | | | | | | |
| | N | 25 | 25 | 25 | 25 | 25 | | | | |
| Inform users prior to personal data collection | Pearson Correlation | 0.089 | .646** | .460* | .554** | 1 | | | | |
| | Sig. (2-tailed) | 0.672 | 0.000 | 0.021 | 0.004 | | | | | |
| | N | 25 | 25 | 25 | 25 | 25 | 25 | | | |
| Inform users their right to refuse | Pearson Correlation | -.142 | .275 | .275 | .123 | .359 | 1 | | | |
| | Sig. (2-tailed) | .499 | .183 | .183 | .559 | .078 | | | | |
| | N | 25 | 25 | 25 | 25 | 25 | 25 | | | |
| Inform users the purpose of collecting personal data | Pearson Correlation | .260 | .260 | .450* | .547** | .467* | .149 | 1 | | |
| | Sig. (2-tailed) | .219 | .219 | .027 | .006 | .022 | .487 | | | |
| | N | 24 | 24 | 24 | 24 | 24 | 24 | 24 | | |
| Inform users of personal data being processed | Pearson Correlation | .145 | .327 | .509** | .459* | .102 | .076 | .244 | 1 | |
| | Sig. (2-tailed) | .488 | .110 | .009 | .021 | .627 | .716 | .250 | | |
| | N | 25 | 25 | 25 | 25 | 25 | 25 | 24 | 25 | |
| Inform users personal data is being transmitted to 3rd parties | Pearson Correlation | .097 | .282 | .282 | .226 | .042 | .031 | -.111 | .408* | 1 |
| | Sig. (2-tailed) | .646 | .172 | .172 | .277 | .843 | .882 | .605 | .043 | |
| | N | 25 | 25 | 25 | 25 | 25 | 25 | 24 | 25 | 25 |

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

**. Correlation is significant at the 0.01 level (2-tailed).

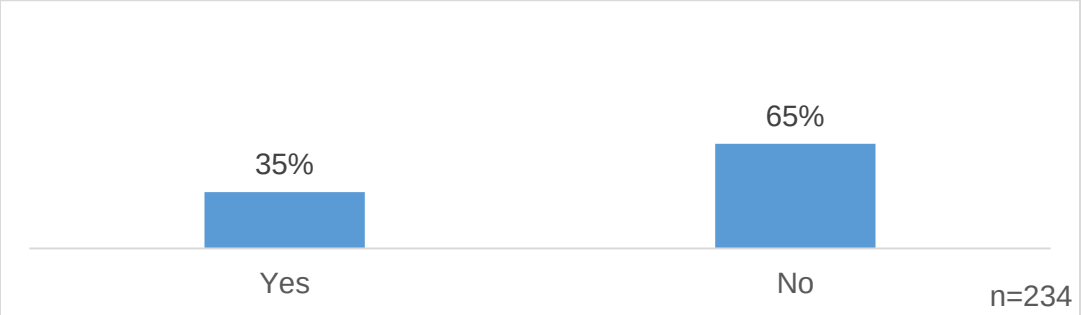
### 4.3 Mobile application user responsibility of personal data

The purpose of this objective is to establish to what extent mobile users are taking personal responsibility of their personal data.

#### 4.3.1 Information of transmission of data to third parties

The study further sought to find out if users were informed that their personal data was transmitted to third parties. 65% of the people interviewed said that such information was not provided as shown in Table 4.3.1-1.

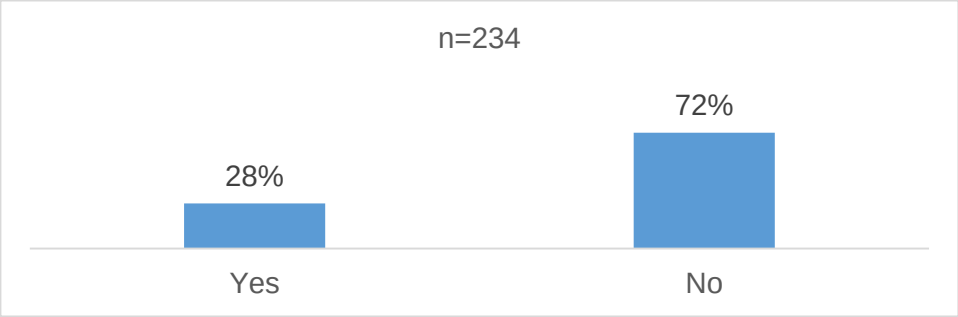
**Table 4.3.1-1: Information of transmission of data to third parties**




#### 4.3.2 Confirmation from agency that personal data is been used

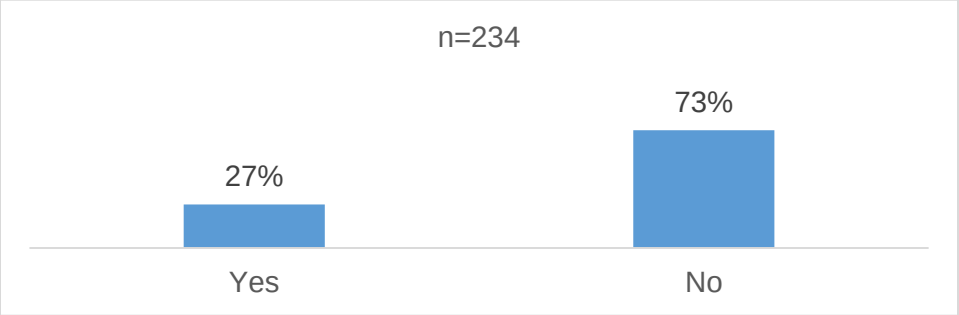
The study further required to find out if they had received any confirmation from the agency they have previously interacted on use of personal data. 72% of the people interviewed said no such confirmations had been made as shown in Table 4.3.2-1.

**Table 4.3.2-1: Confirmation from agency that personal data is been used**



### 4.3.3 Full access to personal data

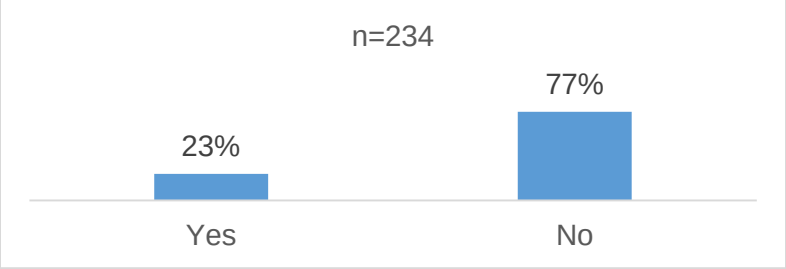
The study sought to find out if users were aware that agencies that collected information had full access to their personal data. 73% of the users interviewed indicated they had not received such information as shown in Table 4.3.3-1.




### 4.3.4 Rectify misleading information

The study further sought to find out if users had requested agencies to erase any misleading data. 77% of the people interviewed said they had not asked organizations to correct any false while 23% of the users said they had contacted agencies to change their information as shown in Table 4.3.4-1.

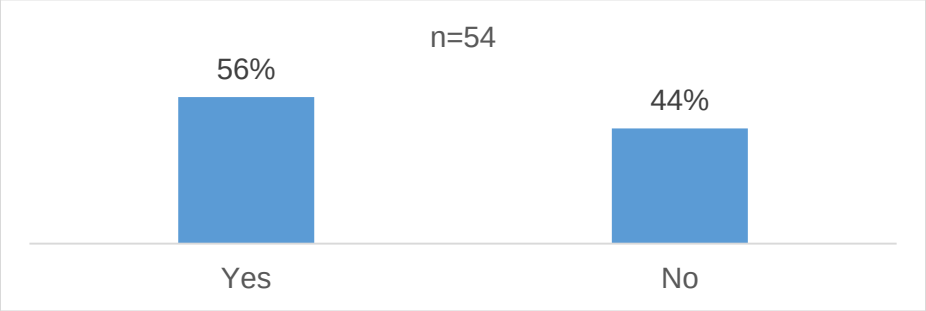
**Table 4.3.4-1: Rectify misleading information**




### 4.3.5 Approval of request by agency

The study required to find out, of those users who had made a request to have misleading information deleted, if their requests had been approved. 56% of the people interviewed said their requests were approved while 44% said their requests were not approved as shown in Table 4.3.5-1.

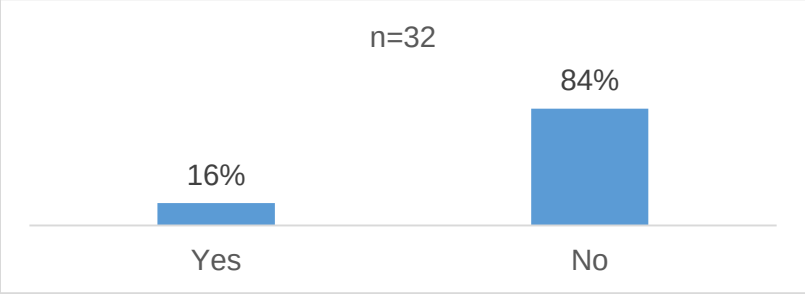
**Table 4.3.5-1: Approval of request by agency**




### 4.3.6 Reasons for rejecting request to change details

The study further out from those respondents whose requests were rejected if reasons had been provided for the rejection. 84% of those interviewed said no reasons were provided for rejection of their requests as shown in Table 4.3.6-1.

**Table 4.3.6-1: Reasons for rejecting request to change details**




### 4.3.7 Correlation of attributes to understand users responsibility of their personal data

The study found out that there is a strong correlation with the agency collecting the personal data having full access to personal data with transmission of personal data to third parties (p=0.011) and confirmation that agency collecting information is using collected personal data (p=0.000). The study also found a strong correlation between contacting the agency to delete any misleading personal information and an agency having full access of personal information (p=0.003). In addition, the study also found out that there was a strong correlation between an agency declining a request to correct personal data with transmission of personal data to third parties (p=0.004) and agency having full access to personal information (p=0.033) as shown in Table 4.3.7-1.

**Table 4.3.7-1: Correlation of attributes to understand users responsibility of their personal data**

| | | Informed of transmission of personal data | Informed that your personal data is being used | Informed that organization has full access of your personal data | Contacted an agency to delete misleading information | Approval of request | Reasons for rejection |
|---|---|---|---|---|---|---|---|
| Informed of transmission of personal data | Pearson Correlation | 1 | | | | | |
| | Sig. (2-tailed) | | | | | | |
| | N | 234 | | | | | |
| Informed that your personal data is being used | Pearson Correlation | .090 | 1 | | | | |
| | Sig. (2-tailed) | .169 | | | | | |
| | N | 234 | 234 | | | | |
| Informed that organization has full access of your personal data | Pearson Correlation | .166* | .333** | 1 | | | |
| | Sig. (2-tailed) | .011 | .000 | | | | |
| | N | 234 | 234 | 234 | | | |
| Contacted an agency to delete misleading information | Pearson Correlation | .071 | .068 | .193** | 1 | | |
| | Sig. (2-tailed) | .283 | .301 | .003 | | | |
| | N | 234 | 234 | 234 | 234 | | |
| Approval of request | Pearson Correlation | .135 | .000 | .017 | .c | 1 | |
| | Sig. (2-tailed) | .331 | 1.000 | .904 | 0.000 | | |
| | N | 54 | 54 | 54 | 54 | 54 | |
| Reasons for rejection | Pearson Correlation | .497** | .114 | .378* | .c | .305 | 1 |
| | Sig. (2-tailed) | .004 | .536 | .033 | 0.000 | .090 | |
| | N | 32 | 32 | 32 | 32 | 32 | 32 |
| *. Correlation is significant at the 0.05 level (2-tailed). | | | | | | | |
| **. Correlation is significant at the 0.01 level (2-tailed). | | | | | | | |
| c. Cannot be computed because at least one of the variables is constant. | | | | | | | |

# CHAPTER 5: DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

This chapter presents the discussions, conclusions and recommendations from the study.

## 5.1 Summary of findings

The study found out that most users of mobile applications were aware of their right to privacy of personal data regarding their personal life and family. They were also aware they had a right to refuse to provide any information as well as correct any information collected. However, majority of users were not aware they had a right to access and correct any personal data collected from their mobile applications. From a mobile developers perspective, they study found out that developers informed users of the purpose, recipient, agency collection information and their rights to correct any information collected. However, they indicated they did not inform users the type of personal data that is processed.

### 5.1.1 Privacy of personal data

The study indicated that if mobile application users understood that they had rights with respect to personal data relating to their private and family life, they are most likely to protect any information they share when using mobile applications. The study also revealed that those mobile application users who understood their rights to privacy of personal data were most likely to refuse to provide any personal information about themselves. The study indicated that users who are understood how their personal data will be processed, demonstrated they understood their rights to privacy over their personal data. In fact, those users who understood they have rights to correct personal data collected, understood their rights to privacy, right to refuse to provide any information and understood they had a right to correct any information collected about them.

### 5.1.2 Using knowledge to enhance personal data privacy

The study found out that mobile application developers had an important role in educating users on how their information is being used. Informing users of the recipients of the personal data was important. In fact, the study revealed it was important for developers to inform users the intended recipients of their personal data and more so that they could access the personal data any time and make corrections to it where necessary. Further, the study indicated it was important to inform users of the type of information collected and the agency collecting this information. In addition to these, the study found out that the informing users of the type of information being collected and processed was important.

### 5.1.3 Mobile application users responsibility of personal data

The study found out that those agencies that had full access of your personal data, were most likely to transmit it to third parties. Therefore users wanted to know the agency that was collecting this information. The study also indicated that those users who knew that an agency had full access of their personal data, were most likely to ask those agencies to remove or rectify any misleading information in their possession. In addition the study found out that those agencies that declined to approve requests to rectify misleading personal data were most likely to transmit such personal with third parties.

## 5.2 Conclusion

There is currently no legislation that protects personal data in Kenya. The proposed Data Protection Bill is expected to regulate the collection, retrieval, processing, storing, use and disclosure of personal data. The study therefore concludes that creating more awareness on the rights to privacy of personal data, there is a high likelihood people will protect any information they share through mobile applications. Further, the more people understood their rights to privacy, they are more likely not to reveal any information about themselves.

The literature review has revealed that organizations consider personal data as the new natural resource. In fact, most institutions infringe on their customers personal data without consent and share their personal data with third parties. The study therefore concludes that developers of mobile applications had a responsibility to inform users the purpose of collecting personal data, who is accessing the data, the name of the agency accessing the data as well how that information will be processed. In addition, they should also inform users that they had a right to correct and rectify any misleading information in their possession.

Users of mobile applications have more often than not taking any responsibility in reading terms and conditions with most of them easily opt in to mobile applications for the sake of convenience. The study therefore concludes that users must take responsibility in engaging agencies that collect personal data so that any information collect is a true reflection. In fact, the more information an agency has about an individual the more likely they are to transmit to third parties.

### 5.3 Recommendations

The study suggests that there is a dire need to get the current Data Protection Bill into law. In the absence of such legislation, there is a need of multi-sectoral body should be put in place to enable oversight that included private and public sector organizations. The body should incorporate private sector representation, Commission of Administration of Justice (CAJ), Communication Authority of Kenya, National Police Service and National Intelligence Service. This will ensure that mutual responsibility is accorded to all parties sharing, receiving and providing oversight of personal information.

There needs to be an alignment with the current various legislations, whilst on one hand some advocate for data protection, others seem to advocate for the need of prying into personal data as security mechanism against unlawful activities. This contradiction therefore leaves room for different agencies pursuing personal data for own advantage to take advantage of the gaps in the system.

There needs to a greater emphasis on capacity building that needs to be undertaken amongst both private and private sector organizations to ensure that privacy of personal data is recognized. There needs to be an understanding of the basic principles on privacy, mitigation measures of privacy concerns, need for qualified human resource on privacy and the adoption and integration of privacy enhancing technologies.

### 5.4 Limitations of the study

The questionnaire used in the study was closed ended. Therefore this has limited getting more opinions and explore deeper issues on privacy of personal data.

### 5.5 Suggestion further study

The technology that is evolving is not limited to mobile applications. The study focused in understanding privacy concerns in the usage of mobile applications. A similar study should be conducted to understand the perception on all forms of digital methods.

## LIST OF REFERENCES


Cavoukian, A. (1997). Privacy by Design: The 7 Foundational Principles. Available at: http://www.privacybydesign.ca/. Accessed 25 April 2016.

Cavoukian, A. (2011). Privacy by Design: The 7 Foundational Principles. Available at: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf . Accessed 5 May 2017

Cavoukin, A. & Popa, C. (2016). Embedding Privacy Into What's Next: Privacy by Design \ for the Internet of Things

Culnan, M. J. (1993). How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. *MIS, Quarterly*. 17(3): 341-363.

CIO, (2014). We did not share consumer data. Available at. http://www.cio.co.ke/news/main-stories/we-did-not-share-consumer-data,-safaricom-says. [Accessed on 12 October 2015].

Clarke, R. (2006). What is Privacy? Available at http://www.rogerclarke.com/DV/Privacy.html. Accessed on 12 October 2015.

Creswell, J. W. (2012). Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research.

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

Creswell, J. W. (2003). Research design: Qualitative, quantitative, and mixed methods.

Drinan, R.F. (1968). Review. *American Bar Association Journal*. 54 (6):593.

Ernst & Young (2013). Privacy trends 2013. Available at: http://www.ey.com/Publication/vwLUAssets/Privacy_trends_2013_-

_The_uphill_climb_continues/$FILE/Privacy%20trends%202013%20-%20The%20uphill%20climb%20continues.pdf. Accessed 12 October 2015.

LLP, DLA Piper. (2012). Data Protection Laws of the World Handbook. United States of America.

Goldfarb, A., & Tucker, C. (2012). Privacy and Innovation. Inn*ovation Policy and the Economy*. 12 (1):65-90.

GoK.(2013).Data Protection Bill. Available at: www.cickenya.org/.../legislation/.../299_b3de9506b20338b03674eacd4. Accessed 12 October 2015.

GoK. (2014). Draft GoK Cybersecurity Strategy. Available at: https://www.scribd.com/mobile/.../Draft-GoK-Cybersecurity-Strategy. Accessed 12 October 2015

Hoepman, J. (2013). Privacy Design Strategies

KNBS. (2015). Kenya Stastistical Abstract.

Knupfer, N.M. & McLellan, H. (2001). Descritpive research methodologies. Available at http://www.aect.org/edtech/ed1/pdf/41.pdf. Accessed 13 June 2017.

Manheim, J.B. (1981). The Annals of the American Academy of Political and Social Sciences. American Academy of Political and Social Science 454: 245-246

McFarland, M. (2014). Unauthorized Transmission and Use of Personal Data. Available at: http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/unauthorized-use.html \. Accessed 12 October 2015.

Mugenda, O. M. & Mugenda, A.G. (1999). Research Methods: Quantitative and Qualitative Approaches.

Nakra, P. (2001). Consumer privacy rights: CPR and the age of the Internet. Management Decision. 39 (4): 272 – 279.

OECD, (1980). Annex to the Recommendation of the Council of 23rd September 1980: Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data. Available at http://oecdprivacy.org/. Accessed 25 April 2016.

Petronio, S. (2002). Communication Privacy Management Theory. Available at highered.mheducation.com/sites/dl/free/0073534307/.../SampleCh13. Accessed 17 December 2015.

Privacy International (2017). The State of Surveillance in Kenya is the result of an ongoing collaboration by Privacy International and National Coalition of Human Rights Defenders - Kenya. Available at https://www.privacyinternational.org/node/980. Accessed on 18 April 2017

Reelforge. (2014). Unpublished media monitoring reports.

Statista. (2015). Statistics and facts about Mobile App Usage. Available at: http://www.statista.com/topics/1002/mobile-app-usage/. Accessed 12 October 2015.

tephenson, M.S. (1971). Reviewed Work: The Assault on Privacy by Arthur R. Miller. *Michigan Law Review.* 69 (7).1389-1397.

Solove, D. J (2006). Brief History Privacy Law.

Schwartz, P.M. (2004). Property, Privacy, and Personal Data. *Harvard Law Review*. 117(7): 2056-2128.

Time Business (2013). Big Data Knows What You're Doing Right Now. Available at: http://business.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/. Accessed 12 October 2015.

Tene, O. & Polonetsky, J. (2012). Privacy in the Age of Big Data.

Teddlie, C. & Yu, F. (2007). Mixed Methods Sampling: A Typology With Examples. *Journal of Mixed Methods Research*. (77) 1.

Tham, I. (2015). 90% of mobile apps could be in breach of Singapore privacy law. Available at: http://www.straitstimes.com/tech/90-of-mobile-apps-could-be-in-breach-of-singapore-privacy-law. Accessed 12 October 2015.

Thurm, S. & Kane, Y.I. (2010). Available at: http://www.wsj.com/articles/SB10001424052748704368004576027751867039730. [Accessed 17 December 2015].

Thomas, F.B. (2016). 191 million US voter Registration Records Leaked. Available at www.forbes.com/us-voter-database-leak. [Accessed in Dec 2015].

Thomas, F.B (2016). Child Tracker App leaks 6.8 million texts, 1.8 million photos from kid's phones. Available at www.forbes.com/kids-photos-leaked. [Accessed 22 February 2016]

Vasalou, A., Joinson, A. & Houghton, D. Privacy as a Fuzzy Concept: A New Conceptualization of Privacy for Practitioners. *Journal of The Association For Information Science And Technology*, 66(5):918–929, 2015

Warren, W. (2008), the right of privacy, Harvard law review 4 (5): 193-220.

World Bank. (2016). Kenya Urbanisation Review.

Yoo, Y. 2010. Computing in Everyday Life: A Call for Research on Experiential Computing. *MIS Quarterly*. 34(2). 213-231.

## APPENDIX 1: MOBILE APPLICATION DEVELOPERS QUESTIONNAIRE

**Dear Sir / Madam**

I invite you to participate in my research study "Assess the Perceptions of Personal Data Privacy amongst users and developers of Mobile Applications in Kenya". I am currently enrolled in the Masters in Public Policy and Management at Strathmore Business School. The purpose of the role of creating awareness of privacy with the aim of enhancing protection of user information against use without their knowledge.

Your participation in the study is voluntary. Your response will be confidential and anonymous. Please answer all the questions on the questionnaire the best way you can.

**Screener Questions**

1. Do you develop mobile applications for smart devices such as smart phones or tablets?
   Yes
   No (terminate)

**Awareness**

2. Are you aware of the Data Protection Act of 2013?
   Yes
   No
3. Are you aware of which government agency is in charge with the implementation of the Data Protection Act 2013?
   Yes
   No
4. Are you aware that every person has a right to privacy with respect to their personal data relating to their private and family life?
   Yes
   No

**Characterization of information**

5. Which of the following information do you routinely collect from your customers through mobile applications? (Tick all that apply)
   Name and surname
   Telephone number
   E-mail address

Age

Gender

Others specify..

**Information to users (notification)**

6. Do you advise users when collecting personal data from mobile applications?

   Yes (Go to 7)

   No (Go to 8)

7. If YES, please explain
8. If NO, please explain
9. Do you inform users of the purpose of which the personal data is collected through their mobile applications?

   Yes

   No

10. Do you inform users who is the intended recipient of the personal data collected through mobile applications?

    Yes

    No

11. Do you inform users the name and agency collecting your personal information from mobile applications?

    Yes

    NO

12. Do you inform users the law regulating the collection of personal data from mobile applications?

    Yes

    No

13. Do you inform users that they have the right to access and correct personal data collected from mobile applications?

    Yes

    No

14. Do you inform users prior to collection of data from mobile applications?

    Yes

    No

15. Do users that they have the right to refuse to personal data collected by mobile applications?

Yes

No

**Collection of personal data**

16. What is the purpose of collecting personal data from users through mobile applicaitons?

    Sending emails

17. Do you inform users of the purpose of collecting personal data from mobile applications?

    Yes (Go to 18)

    No

18. If YES, please explain

19. Do you inform users how the information collection will be used?

    Yes

    No

**Data processing either manual or automated**

20. Do you inform users the type personal data being processed from their mobile applications?

    Yes

    No

21. Do you inform users that when their personal data is being transmitted to other parties?

    Yes

    No

22. Are users able to correct or rectify any personal data you have collected mobile applications?

    Yes

    No

**Protection and Security of Personal Information**

23. Do you have security safeguards for the control of personal data collected from mobile applications?

    Yes

    No

24. Do you have in place mechanisms to protect personal data during transmission to third parties in connection to a service?

    Yes (Go to 25)

    NO

25. If YES, please list the mechanisms put in place?

**Access to data**

26. Do you send a confirmation to users informing them that you are using the personal data collected from mobile application?

    Yes

    No

27. Do you inform users that your company shall have full access to personal data collected from a mobile application?

    Yes

    No

**Correction of information**

28. Have users ever contacted you to delete any false or misleading information?

    Yes (Go to 29)

    No (Go to 30)

29. Did you approve the requests from the users?

    Yes (Go to 31)

    No (Go to 30)

30. Did you the reasons for rejection in writing?

    Yes

    No

**Storage of Information**

31. For how long do you keep user information?

    6 months – 1 year

    1 -3 years

    3-5 years

    5+ years

**Consent**

32. Do you get consent from users when using their data for commercial purposes?

    Yes (Go to 33)

    No

33. Which of the following methods do you seek consent:

    Clicking a link

    Filling and signing a form

    Click on a check box

## APPENDIX 2: MOBILE APPLICATION USER QUESTIONNAIRE

**Dear Sir / Madam**

I invite you to participate in my research study "Assess the Perceptions of Personal Data Privacy amongst users and developers of Mobile Applications in Kenya". I am currently enrolled in the Masters in Public Policy and Management at Strathmore Business School. The purpose of the role of creating awareness of privacy with the aim of enhancing protection of user information against use without their knowledge.

Your participation in the study is voluntary. Your response will be confidential and anonymous. Please answer all the questions on the questionnaire the best way you can.

**Screener Questions**

1. Do you use smart devices such as smart phones or tablets?

   Yes

   No (terminate)

2. Do you frequently download mobile applications?

   Yes

   No (terminate)

**Awareness**

3. Are you aware of the Data Protection Act of 2013?

   Yes

   No (Go to 6)

4. Are you aware which government agency is in charge of the implementation of the Data Protection Act 2013?

   Yes (Go to 5)

   No (Go to 6)

5. Please specific which government agency?
6. Are you aware that every person has a right to privacy with respect to their personal data relating to their private and family life?

   Yes

   No

**Characterization of information**

7. Which of the following personal data do you routinely provide to mobile applications? (Tick all that apply)

   Name and surname

   Telephone number

   E-mail address

   Age

   Gender

   Other specify

**Information to users (notification)**

8. Are you advised when your mobile application is collecting your personal data?

   Yes

   No

9. If yes, explain how?
10. Are you informed, for what purpose your personal data is collected by the mobile application?

    Yes

    No

11. If yes, please explain?
12. Are you informed the intended recipient of the personal data collected from the mobile application?

    Yes

    No

13. Are you informed the name and agency collecting your personal information from the mobile application?

    Yes

    NO

14. Are you informed about the law regulating the collection of personal data from your mobile application?

    Yes

    No

15. Are you informed of your rights to access and correct personal data that you have shared through your mobile application?

    Yes

    No

16. Are you informed that you have a right to refuse to provide personal data to your mobile application?
    Yes
    No

**Data processing either manual or automated**

17. Are you informed the type of personal data being processed from your mobile application?
    Yes
    No
18. Are you informed if your personal data will be transmitted to other parties?
    Yes
    No
19. Are you able to correct or rectify any personal data you have collected through your mobile application?
    Yes
    No

**Access to data**

20. Have you ever obtained a confirmation from any agency or organization that you have previously interacted that they are using your personal data?
    Yes
    No
21. Has any agency or organization you have previously interacted through a mobile application with informed you that they shall have full access of personal data collected through their mobile application?
    Yes
    No

**Correction of information**

22. Have you previously contacted your agency or organization that has collected data through your mobile application to delete any false or misleading information?
    Yes (Go to 23)
    No (Go to 25)
23. Was your request approved by the agency or organization?
    Yes (Go to 25)
    No (Go to 24)

24. In the event your agency or organization rejected the request, did they provide you with the reasons for rejection in writing?

    Yes

    No

**Storage of Information**

25. Do you know for how long your personal information has being kept?

    6 months – 1 year

    1 -3 years

    3-5 years

    5+ years

**Consent**

26. Do you provide consent to your organization or agency when using their data collected from mobile applications for commercial purposes?

    Yes Go to 27

    No

27. Which of the following methods do you provide consent?

    Clicking a link

    Filling and signing a form

    Click on a check box