RIGHT TO PRIVACY IN THE WAKE OF MOBILE MONEY TRANSFERS IN KENYA: IS THE DATA PROTECTION BILL A STEP IN THE RIGHT DIRECTION?

Submitted in partial fulfillment of the requirements of the Bachelor of Laws Degree,
Strathmore University Law School

By

Gichaga, Eric Wagura

084035

Prepared under the supervision of

Dr. Isaac Michael Rutenberg PhD, JD

March, 2018

Word count: 11,192

TABLE OF CONTENTS

TABLE OF CONTENTS.....ii
ACKNOWLEDGEMENT.....iii
DECLARATION.....iv
ABSTRACT.....v
LIST OF ABBREVIATIONS.....vi
LIST OF CASES.....vii
CHAPTER 1 – INTRODUCTION.....1
1.1 Background.....1
1.2 Statement of Problem.....3
1.3 Justification of Problem.....5
1.4 Statement of Objectives.....6
1.5 Research Questions.....6
1.6 Hypothesis.....7
1.7 Research Design and Methodology.....7
1.8 Limitations.....7
1.9 Chapter Breakdown.....8
CHAPTER 2 - CONCEPTUAL FRAMEWORK.....9
CHAPTER 3 - DATA PROTECTION IN KENYA IN VIEW OF MOBILE MONEY TRANSFERS.....14
3.1 Information Privacy in a digital space.....14
3.2 Privacy concerns.....16
a. Transparent use without privacy protection.....16
b. Limited privacy protections.....17
c. Potential for abuse.....18
3.3 The need for data protection in Kenya.....19
3.4 Current data protection framework in Kenya & legislation that threatens information privacy.....22
CHAPTER 4 – COMPARATIVE STUDY OF LEGISLATION IN GHANA AND KENYA'S DATA PROTECTION BIL.....25
4.1 Ghana.....26
4.2 Kenya.....27
CHAPTER 5 – CONCLUSION AND RECOMMENDATIONS.....32
BIBLIOGRAPHY.....36

ACKNOWLEDGEMENT

Thus far, I am grateful to God for his abundant grace and enduring love.

I am sincerely grateful to my mother for her prayers, counsel, encouragement and support all throughout my undergraduate study.

Equally, I would like to express my unreserved gratitude to my supervisor, Dr Isaac Michael Rutenberg, for offering his insight on this particular topic of study, his guidance, and patience throughout this process.

Finally, I would like to extend my appreciation to my family and friends who have helped and encouraged me in one way or another in the course of this dissertation project.

DECLARATION

I, **GICHAGA, ERIC WAGURA**, do hereby declare that this research is my original work and that to the best of my knowledge and belief; it has not been previously, in its entirety or in part, been submitted to any other university for a degree or diploma. Other works cited or referred to are accordingly acknowledged.

Signed: .....

Date: 30/5/2018

This dissertation has been submitted for examination with my approval as University Supervisor.

Signed: 30/5/18

DR. ISAAC M. RUTENBERG, PhD, JD.

SENIOR LECTURER & DIRECTOR, THE CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION TECHNOLOGY LAW (CIPIT)

ABSTRACT

Mobile Money Transfer has, in just a little over ten years, transformed the lives of millions of Kenyans in addition to greatly improving the economy of the country. Mobile money penetration in Kenya currently stands at 68% of the adult economy. This has not only made Kenyans the most banked people in Africa but has also greatly contributed to improving the lifestyles of many Kenyans who don't live within urban areas.

The success of mobile money in Kenya is greatly backed by the rise in mobile phone penetration and advancement in technology. This success is however greatly threatened owing to the fact that the telecommunication companies operating mobile money services do so in an environment where there is no clear law or regulation on data protection.

A mobile money environment is synonymous with generation of big data. Big data here includes large and complex sets of data that are usually collected by the telecommunication companies offering mobile money services. This data includes, but is not limited to, information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. If left unprotected, such information is vulnerable to potential abuses and misuse.

A data protection framework is thus not only vital to guarantee right to information privacy of individuals but also to necessary to ensure the continued success of mobile money as such a framework would give individuals increased confidence in using mobile money services.

This paper thus outlines the need to have in place a clear data protection regulatory framework in Kenya that clearly outlines the processes of data collection, retrieval, processing, storage, use and disclosure of personal data associated with mobile money transfers. The paper does this by discussing the need for privacy protection with regards to mobile money transfers, critically examining the Data Protection Bill 2013, and lastly looking at best practice from Ghana.

LIST OF ABBREVIATIONS

CBK	Central Bank of Kenya
CAK	Communications Authority of Kenya
EAC	East African Community
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
EU	European Union
FATF	Financial Action Task Force
FII	Financial Inclusion Insights
GDPR	General Data Protection Regulation
IP	Internet Protocol
KBA	Kenya Bankers Association
NIS	National Intelligence Service
NPS	National Payment Systems
OECD	Organisation for Economic Co-operation and Development
P2P	Peer-to-peer
PIN	Personal Identification Number
PwC	PricewaterhouseCoopers
SIM	Subscriber Identification Module
STK	SIM Application Tool Kit
T&Cs	Terms and Conditions
UK	United Kingdom

UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNGA	United Nations General Assembly
UDHR	Universal Declaration of Human Rights
US	United States
USSD	Unstructured Supplementary Services Data

LIST OF CASES

Benard Murage v Fineserve Africa Limited and others, [2014] eKLR High Court of Kenya

Olmsted v United States 277 US 438 (1928)

Riley v California 573 US 783 (2014)

CHAPTER 1 - INTRODUCTION

1.1 BACKGROUND

Right to privacy is one of the most fundamental rights a human being should be able to enjoy as it is intrinsic to the right to life.[1] In its earliest formulations, the right to privacy is seen in the 1789 American Bill of Rights proposed by James Madison. The Ninth Amendment describes the right as; *"an unspecified right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."*[2]

In as much as the original purpose of this amendment was to limit the powers of the Federal government, not to expand them, the overarching conception of privacy is strikingly manifest. The same right is then later seen in the Universal Declaration of Human Rights (UDHR) which guarantees that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. It further states that everyone has the right to the protection of the law against such interference or attacks.[3]

The Constitution of Kenya (2010) also provides for the right to privacy.[4] In addition to guaranteeing the right to privacy, the Kenyan Constitution further provides for the right to information privacy under article 31(c) and (d). This article states that;

> *"Every person has the right to privacy which includes not to have; information relating to their family or private affairs unnecessarily required or revealed; or the privacy of their communications infringed."*

This then begs the question what constitutes as the right to privacy or specifically information privacy and eventually what aspects about your information privacy should be protected by a law on data protection.

Information privacy can be defined as, legal safeguards that have been put in place in information storing systems to prevent the collection, retrieval, processing, storage, use and

---

[1] Right to Privacy is a fundamental right, it is intrinsic to the right to life: Supreme Court, https://timesofindia.indiatimes.com/india/right-to-privacy-is-a-fundamental-right-supreme-court/articleshow/60203394.cms on 9 December 2017.

[2] 1791: US Bill of Rights (1st 10 Amendments) - with commentary http://oll.libertyfund.org/pages/1791-us-bill-of-rights-1st-10-amendments-with-commentary on 9 December 2017.

[3] UNGA, Universal Declaration of Human Rights, UN GA res 217A (III), UN Doc A/810 at 71 10 December 1948.

[4] Article 31 (c) and (d), *Constitution of Kenya* (2010).

disclosure of personal information by unauthorised parties.[5] On the other hand, personal information/data means any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.[6] Such information may include, but is not limited to, financial records, data shared over the internet, or even medical health records.

In this study, Data Controller means, any natural or legal person, public or private, any other organization or association which alone or jointly with others, decides to collect and process personal data and determines the purposes.[7] Whereas, Data Subject means, any natural person that is the subject of personal data processing.[8]

In this study, information privacy will narrow down to focus majorly on personal information that is stored over mobile money transfer databases. Such information is usually stored by the agents that facilitate mobile money transfers or by the databases of the relevant telecommunications companies involved or both. The data shared will usually include information that is of a personal nature, that is, information that is specific to a certain identifiable individual.[9] Most of the time, such information encompasses: age, gender, personal identification numbers (PINs), current location, debit and credit transactions and at times even personal communications between other mobile money transfers users.[10]

Mobile money transfer, on the other hand, can be defined as a movement of value that is made from a mobile wallet, accrues to a mobile wallet, and/or is initiated using a mobile phone.[11] A mobile wallet is an account that is primarily accessed using a mobile phone.[12] A

---

[5] Stanford Encyclopaedia of Philosophy: Privacy and Information Technology, https://plato.stanford.edu/entries/it-privacy/ on 8 February 2018.
[6] Article 1, *African Union Convention on Cyber Security and Personal Data Protection.*
[7] Article 1, *African Union Convention on Cyber Security and Personal Data Protection.*
[8] Article 1, *African Union Convention on Cyber Security and Personal Data Protection.*
[9] Scharwatt C, Katakam A, Jennifer F, Murphy A, and Naghavi N, 'Global System for Mobile Phone Communication Association: Mobile Money for the Unbanked, Mobile Money Definitions, *GSMA*, 2010, 4.
[10] Scharwatt C, Katakam A, Jennifer F, Murphy A, and Naghavi N, 'Global System for Mobile Phone Communication Association: Mobile Money for the Unbanked, Mobile Money Definitions, 4.
[11] Scharwatt C, Katakam A, Jennifer F, Murphy A, and Naghavi N, 'Global System for Mobile Phone Communication Association: Mobile Money for the Unbanked, Mobile Money Definitions, 4.
[12] Scharwatt C, Katakam A, Jennifer F, Murphy A, and Naghavi N, 'Global System for Mobile Phone Communication Association: Mobile Money for the Unbanked, Mobile Money Definitions, 4.

mobile money transfer can also occur in the form of a mobile payment which is a transfer to pay for goods or services, either at the point of sale (retail) or remotely (bill payments).[13]

1.2 STATEMENT OF PROBLEM

As it is currently world over, technology brings with it the risk of the violation of the right to information. In the Kenyan case of *Benard Murage v Fineserve Africa Limited and others,*[14] we see an instance where the right to information privacy was threatened. The petitioner was requesting the High Court at Nairobi to restrain the first and second respondents (Fineserve Africa Limited and Equity Bank respectively) from rolling out the thin SIM (Subscriber Identification Module) technology pending the enactment of the Data Protection Bill. The SIM was to be used by customers of the second respondent to interact with their banks directly from their phones. The petitioner claimed that the technology posed a risk to information privacy as the thin SIM technology, as proposed to be used by the respondent, is able to monitor communications taking place between the primary SIM and the mobile handset thus exposing it to man-in-the-middle attacks including personal data contamination and access by third parties.

It was also the Petitioner's case that the thin SIM technology, as manifested from its functionality, provides a real threat to the Petitioner's enjoyment of his rights under Article 31 (c) and (d) of the Constitution in so far as his personal data is concerned. His fears were grounded on the security vulnerabilities of the thin SIM which transcends the scope of the user by making it possible for third parties to access personal and sensitive data such as PINs (Personal Identification Number) and encryption keys.

Further, it was also the Petitioner's case that in countries where the thin SIM has been used, Data Protection laws have been enacted unlike in Kenya where there is no law on Data Protection.

The petition was however dismissed as the Petitioner had not satisfactorily proved breach of the right to privacy as guaranteed by the constitution or a threat to breach the right. In coming to his conclusion, the learned judge stated that the Communications Authority of Kenya

---

[13] Scharwatt C, Katakam A, Jennifer F, Murphy A, and Naghavi N, 'Global System for Mobile Phone Communication Association: Mobile Money for the Unbanked, Mobile Money Definitions, 4.
[14] [2014] eKLR, High Court of Kenya at Nairobi.

(CAK), as the communications regulator in the country, is better placed to assess on whether the thin SIM technology, as was intended to be used by the second respondent, would bring with it a threat of violation to the right to information privacy. With regards to the enactment of the Data Protection Bill, the learned judge stated that a court cannot order parliament to create law as it is a separate and distinct arm of government thus he chose to uphold the separation of powers doctrine.

Notwithstanding the failure to prove the Right to Privacy breach, the case clearly shows the imminent threat posed on privacy by technological advancements especially in the field of Mobile Money/Mobile Banking as companies continue to compete.

This however, is not an isolated case. Recently, the Financial Action Task Force (FATF), which is an organization that sets out internationally accepted standards and promote effective implementation of regulatory measures for combating money laundering and terrorism financing, recommended user transparency and collection of transaction data in mobile money transfers.[15] Kenya is a member country to Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG). This is the regional body tasked with combating money laundering by implementing the FATF Recommendations. The FAFT is the only global body that works to generate the necessary political will to bring about national legislative and regulatory reforms in the areas of money laundering, terrorist financing and other related threats to the integrity of the international financial system.[16] The FATF has developed a series of Recommendations that are recognised as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. First issued in 1990, the FATF Recommendations have been revised in 1996, 2001, and 2003. In 2012, these recommendations were again revised to ensure that they remain up to date and relevant, and they are intended to be of universal application. These recommendations have been integrated into national laws of its over 30 member states as well as member states of it regional affiliates such as ESAAMLG which in total include over 70 countries.[17] The Kenya Finance Act, 2016 is one such legislation that mirrors some of the recommendations of the FATF.

---

[15] Financial Action Task Force (FATF), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations 11 and 12,* 2012, 14-15.
[16] FATF, http://www.fatf-gafi.org/about/ on 8 February 2017.
[17] FATF, http://www.fatf-gafi.org/about/ on 8 February 2017.

These recommendations by the FATF are not very new to Kenya as telecommunications were already collecting transaction data through their agents. The only novel addition brought about by the recommendations is the requirement that collected data is maintained for five years and that due diligence is carried out by the relevant parties to a mobile money transfer. Such due diligence should include confirming the identity of clients and scrutinising client transactions.

These requirements, when fully implemented in the Kenyan mobile money sector, will pose a great threat to privacy especially considering that Kenya still doesn't have a comprehensive law on data protection. This threat to privacy is even more imminent considering the recent UN report that noted a lack of legislation amongst the East African Community (EAC), that is Burundi, Kenya, Rwanda Tanzania and Uganda, "that clearly defines who can get access to a mobile money trail, and how, when or under what conditions such access may be obtained."[18]

1.3 JUSTIFICATION OF THE PROBLEM

This study is important because as seen above, with further advancement in technology, so does the risk of information privacy breaches and violations grow imminent. Technology in the 21st century is a force to reckon with and if not used properly it can lead to many human rights violations among them the violation of the right to information privacy. The situation is even more unique to Kenya where mobile money transfers accounts for 3 Billion Kenya Shillings a day.[19] This makes Kenya not only the regional frontier in mobile money transfers but also a global powerhouse in the mobile money sector. With such a huge proliferation of Mobile Money in the country so does the data held by telecommunication companies and/or other third-party data controllers continue to increase.[20] This puts these data controllers in a very precarious position, more so, with the absence of a law on data protection in place. As such there is need to have a data protection framework due to the huge potential for abuse of data held by controllers and/or other agents. This situation also further puts the customers

[18] UN Conference on Trade and Development, 'Mobile Money for Business Development in the East African Community: A Comparative Study on Existing Platforms and Regulations,' *UN Publication UNCTAD/DTL/STICT/2012/2,* 2012, 20.

[19] Mobile Money Transactions Hit 3 Billion Kenya Shillings a Day, https://www.standardmedia.co.ke/business/article/2000197514/mobile-money-transactions-in-kenya-hit-sh3-billion-a-day on 8 February 2017.

[20] Do Mobile Money Clients Need More Protection? http://www.cgap.org/blog/do-mobile-money-clients-need-more-protection on 9 December 2017.

(data subjects) in a disadvantage as there are currently no legal remedies with regards to information privacy rights violations.

In addition, large amounts of personal data generated from Mobile Money transactions are kept across servers, networks and filing systems (electronically and manually), locally and abroad.[21] These can then be shared by different legal and natural persons, across borders and in a manner that a data subject could not have envisaged at the time the initial information is given or collected.[22] These information systems used in the collection and storage of such personal information can therefore pose considerable challenges to one's right to privacy. As mobile money continues to grow, more sophisticated technology with considerable abilities to hold large amounts of information comes along with it, thus it is necessary to address privacy concerns with a law on data protection.

1.4 STATEMENT OF OBJECTIVES

The main objective of this study is to investigate whether there is any law that provides for data protection in Kenya. Data stored by mobile money transfer databases will be of importance as many Kenyans use this service and have their personal information stored by the said databases. The study will also strive to analyse the data protection bill and whether it adequately guarantees the right to privacy.

The specific objectives of this study are:

1. Critically examine the framework for Data protection in Kenya, if any.
2. Determine whether current legislation on privacy adequately provides for Data Protection in Kenya.
3. Establish what has been the best practice with regards to Data Protection in jurisdictions that have progressive Data Protection Laws.
4. Provide recommendations on how to strengthen the Data Protection Bill (2013) based on findings of this study.

1.5 RESEARCH QUESTIONS

This study will seek to answer the following questions:

---

[21] Makin P, 'Regulating Issues Around Mobile Banking: New initiatives to bank the poor are straining the world's financial regulatory systems,' *OECD*, 2009, 13.

[22] Makin P, 'Regulating Issues Around Mobile Banking: New initiatives to bank the poor are straining the world's financial regulatory systems,' *OECD*, 2009, 13.

1. What type of data, associated with mobile money transfers, should be protected by data protection laws?
2. What are pertinent privacy concerns with regards to collection, retrieval, processing, storage, use and disclosure of personal data associated with mobile money transfers in view of a lack of legislation that comprehensively caters for the data protection in the country?
3. What is the current legal, institutional and regulatory framework for the collection, retrieval, processing, storage, use and disclosure of personal data associated with mobile money transfers in the country?

1.6 HYPOTHESIS

This study will test the following hypotheses:

1. There are few laws and regulations governing the collection, storage, processing and use of personal data associated with mobile money transfers or any other personal data held by data controllers and data agencies.
2. Personal data associated with mobile money transfers falls within the realms of data that should be covered by data protection laws.
3. The Data Protection Bill adequately caters for protection of personal data.
4. There is a risk of privacy violations by data controllers or agencies in Kenya.

1.7 RESEARCH DESIGN AND METHODOLOGY

The intended study will be conducted through a desk review of the current laws in the country that specifically promote or threaten the right to information privacy, relevant academic journal articles, and reports concerning data protection with a slight bias towards data collected by telecommunication companies especially those involved in Mobile Money Transfers. A case study will also be incorporated in this study so as to highlight best practice from a jurisdiction that has had similar concerns with regard to data protection and mobile money transfers and already has a data protection framework in place.

1.8 LIMITATIONS

The intended study will be majorly based on internet sources and reliance on best practices from other jurisdictions. The reason for this is because there is little to none about this topic that has been documented in books, of which if any, aren't easily accessible, and there is even less information on the subject in Kenya as it is a rapidly developing area especially due this

age of technological advancements. Reference will be made towards Ghana which has in place a comprehensive law on data protection and has set up a Commission on Data Protection in the country. This Study will also have a look at the United States and other western jurisdictions as a source of legislation, cases and regulatory framework due to their vast development in information privacy. Therefore, secondary sources of information will be the main basis for this research from which inference shall be made.

1.9 CHAPTER BREAKDOWN

Chapter 1: Introduction

This chapter introduces the paper by giving the background of the topic and reasons for the research.

Chapter 2: Conceptual/Theoretical Framework and methodology.

This chapter deals with the different legal theories that can be applied to the right to information privacy and data protection. Also, the principles that should inform a comprehensive data protection law will be discussed within this chapter.

Chapter 3: Study/analysis of the research questions

This chapter will contain an examination of the research questions by discussing case studies from other jurisdictions that have had similar questions to answer. This chapter will also look at the legislative framework with regards to the right to information privacy in Kenya and some of the present laws that threaten the enjoyment of the right to privacy.

Chapter 4: Comparative analysis

This chapter will focus on highlighting the regulatory framework of other jurisdictions with regards to data protection. Best practices from Ghana will be the basis of this comparative study. This will be discussed vis-à-vis the regulatory framework and data protection mechanisms currently in place within Kenya.

Chapter 5: Recommendations and conclusion

This chapter will contain recommendations on what can be improved or changed within the current legal framework on data protection in Kenya so as to carefully and comprehensively provide for a data protection in Kenya. The chapter will also contain recommendations on

how the current Data Protection Bill can be improved to ensure the right to information privacy is adequately safeguarded within the Kenyan legal framework.

CHAPTER 2 – CONCEPTUAL FRAMEWORK

From a reading of article 31(c) of the Constitution, the right to privacy encompasses two main critical aspects. These are; the right to information privacy with regards to one's private affairs and the right not to have information about these affairs revealed unnecessarily. A critical reading of this section clearly shows that the right to privacy is a limitable right. The Constitution requires that where a right is to be limited, it shall only be done so, *inter alia,* by way of law and use of the least restrictive means possible.[23] Currently, there is no enabling law or framework in the country providing for data protection or circumstances under which the right to privacy may be limited. This chapter will deal with the common law legal theory and some of the principles that inform the need for privacy protection and in particular data protection.

The theoretical basis for this study is derived from Samuel Warren and Louis Brandeis' widely cited ***The Right to Privacy***. The article was written after Warren and Brandeis began noting new technological advancements that were posing a potential threat to privacy and focused on how the common law could develop to protect the interest then called "privacy". They described the term privacy as the ***right to be let alone***. The main purpose of their article was to demonstrate that many aspects of the right to privacy existed within the common law. The two authors observed and opined that modern enterprise and invention have, through invasions upon his privacy, subjected an individual to mental pain and distress, far greater than could be effected by bodily injury. This type of harm was not provided for under tort law then.[24] Forty years later, Brandeis' wisdom is again seen in his famous dissenting opinion in the case of ***Olmsted v United States***.[25] In this case, the court held that wiretapping was **not** a violation of privacy under the Fourth Amendment as it was **not physical trespass**. Brandeis, in a dissenting opinion, stated that the framers of the constitution *"conferred as against the government the right to be let alone-the most comprehensive of rights and the right most valued by civilized men."* This case demonstrates that the absence of a proper legislative framework on right to privacy, particularly on data protection, might lead to injurious privacy violations by data controllers or agents that go unpunished.

---

[23] Article 24, *Constitution of Kenya,* (2010).
[24] Warren S and Brandeis L, 'The Right to Privacy' *Harvard Law Review,* 1890, 45.
[25] (1938) 277 US Supreme Court.

Another theory that tries to explain the right to privacy is the ***Personhood Theory***. Personhood refers to those attributes of an individual which are irreducible to his selfhood.[26] This hints at the fact that privacy is concerned with the integrity and personality of a person. This personhood conception is further developed by professor Benn who notes that privacy amounts to respect to individuals as choosers. *"Respect for someone as a person, as a chooser, implies respect for him as one engaged in a kind of self-creative enterprise which could be disrupted distorted or frustrated even by so limited an intrusion as watching."*[27] This hints at the fact that consent is a key element of privacy. Individuals should be allowed, under the law, to choose what type of private information they want to share with third parties and for what duration of time such data will vest with such parties.

In addition, data protection should be informed by the **data protection principles** that are at the heart of protection of the right to privacy.[28] These principles are enumerated in laws of the different jurisdictions that have a comprehensive law on data protection in places such as Ghana and the United Kingdom (UK).

One such principle is **accountability** which imposes a duty of care on data controllers and any other person who processes data to ensure that such data is processed; without infringing the privacy rights of the data subject and in a lawful and reasonable manner.[29] With respect to foreign data subjects, a data controller or processor should ensure that personal data is processed in compliance with data protection legislation of the foreign jurisdiction of that subject where personal data originating from that jurisdiction is sent to this country for processing.

Another principle informing data protection is **lawfulness of processing.** This principle provides that data should only be processed if the purpose, for which it is to be processed, is necessary, relevant and not excessive.[30] Also, inherent to this principle is the concept of consent. A person should not process personal data of an individual without the prior consent

---

[26] Freund P, *Privacy: One Concept or Many*, Atherton Press, New York, 1971 42-43.
[27] Benn S, *Privacy Freedom and Respect for Persons*, Atherton Press, New York, 1971, 26.
[28] Data Protection Principles, https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/ on 16 September 2017.
[29] Section 18, Act 843, *Data Protection Act* (Ghana).
[30] The Eight Data Protection Principles, http://www.ed.ac.uk/records-management/data-protection/what-is-it/principles on 16 September 2017.

of the data subject, i.e. the individual, with the exceptions to this to be clearly provided for under written law.[31]

Intrinsic to this principle is also the process of data collection and retention. Data should be collected directly from the data subject always and where such is not possible, the data subject should have consented to indirect collection.

With regards to retention, data collected should not be retained for a longer period than is necessary to achieve the purpose for which the data is collected with exceptions to this to be clearly provided for under written law.[32]

Data protection also requires that collected data be used for a **specific purpose.** Such purpose should be explicitly defined, lawful and related to the activities or functions of the data agent/processor. Further, where data is collected by a third party, such data should be used only for the purposes for which it was collected. This requirement aims to ensure that organisations are open about their reasons for obtaining personal data, and that what they do with the information is in line with the reasonable expectations of the individuals (data subjects) concerned.[33]

Compatibility of further processing with purpose of collection is among the principles informing data protection. This principle proposes that data collectors who hold personal data collected for a specific purpose should ensure that further processing of the personal data is for that specific purpose.[34] This effectively means that data collectors or data agents/processors cannot use already collected data for another purpose, different from initial purpose, without re-seeking consent of the data subject.

It is also incumbent upon the data controller to ensure that collected data is maintained to required standards with regards to **quality.** This principle of **quality of information** requires data controllers to ensure that the data in their possession is complete, accurate, up to date and not misleading having regard to the purpose for the collection or processing of the

[31] Sections 19 & 20, Act 843, *Data Protection Act* (Ghana).
[32] University of Edinburgh: The Eight Data Protection Principles, http://www.ed.ac.uk/records-management/data-protection/what-is-it/principles on 16 September 2017.
[33] Processing personal data for specified purposes (Principle 2), https://ico.org.uk/for-organisations/guide-to-data-protection/principle-2-purposes/ on 16 September 2017.
[34] Data Protection Principles, https://www.dataprotection.org.gh/data-protection-principles on 16 September 2017.

personal data.[35] This principle is also in line with the Constitution of Kenya which stipulates that every person has the right to the correction or deletion of untrue or misleading information that affects the person.[36]

Another overarching principle is **openness.** This principle requires that data controllers should be duly registered by a statutory body in-charge of data protection within a given jurisdiction. The principle also requires data controllers to inform data subjects of nature of data to be collected, name and address of person collecting, purpose of collection, whether the supply of data is mandatory or voluntary, consequences of failing to provide data, requirement by law for its collection, recipients of data, nature or category of the data, and finally, the existence of the right of access to and the right to request rectification of the data collected before the collection.[37]

Data security safeguards, as a principle, requires data controllers to take the necessary steps to secure the integrity of personal data in the possession or control of a person through the adoption of appropriate, reasonable, technical and organisational measures to prevent; loss of, damage to, or unauthorized destruction; and unlawful access to or unauthorized processing of personal data.[38] This in effect means that data controllers are to put up tight security in their storage systems such as firewalls and encryption keys or adopt storage models that will not expose information into risk of external tampering or theft.

Finally, as a principle, the **data subject should be allowed to participate, at will, in the processing of collected data that concerns him.** Such participation shall include access to information held by a data controller or any other third party. A data controller shall comply with such request and give a description of the data in its possession as well as identity of a third party with access to such information. A data subject may also request a data controller to correct information in its possession. A data controller should comply with such request or provide credible evidence in support of such data.[39]

---

[35] Data Protection Principles, https://www.dataprotection.org.gh/data-protection-principles on 16 September 2017.
[36] Article 35 (2), *Constitution of Kenya* (2010).
[37] Data Protection Principles, https://www.dataprotection.org.gh/data-protection-principles on 16 September 2017.
[38] Data Protection Principles, https://www.dataprotection.org.gh/data-protection-principles on 16 September 2017.
[39] Data Protection Principles, https://www.dataprotection.org.gh/data-protection-principles on 16/9/2017. 16 September 2017.

The Data Protection Bill (2013) under clause 4 provides for these principles albeit inadequately. The bill, in outlining the principles, fails to clearly establish who bears the duty of care with regards to personal data already collected by data collectors but not in their possession. It also fails to provide for a principle governing indirect collection of data from data subjects.

The right to be let alone, as propounded by Warren and Brandeis, the personhood theory and the data protection principles as explained above are thus seen to be at the heart of right to information privacy. This right gives rise to a negative obligation against the government and any other person or entity not to interfere with the affairs of an individual without prior consent. With the rising magnitude of information now held by telecommunication companies, banks and other data controllers and/or data agents' due to the rise of mobile money in Kenya, a comprehensive law on data protection needs to be enacted to provide a framework on how to uphold the privacy of such data and any other data that is of a personal nature.

CHAPTER 3 - DATA PROTECTION FRAMEWORK IN KENYA

3.1 Information privacy in a digital space

"The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." - US Supreme Court Chief Justice John Roberts in Riley v California (2014).[40]

The 21st century has become the century of big data.[41] Advanced Information Technology systems now allow for the storage and processing of large amounts of data. The revelations of Edward Snowden[42] have demonstrated that these worries are not only real but also that the technical capabilities to collect, store and search large quantities of data concerning telephone conversations, internet searches and electronic payment, as well as mobile money transfers, are now in place and are routinely used by government in collaboration with corporations.

Technological innovation has, over time, triumphed over our privacy protections.[43] This has resulted in our digital footprint being vulnerable to tracking by the government and telecommunications or other corporations in ways that were once unfathomable.

This digital footprint is constantly growing, containing more and more data about the most intimate aspects of our lives. This is especially more true for mobile money transactions in Kenya. Other such data that can be held by corporations includes our communications, whereabouts, and online searches among others. When the government has easy access to this information, we lose more than just privacy and control over our information. Free speech, security, and equality might end up suffering as well.

M-PESA, a mobile-enabled money transfer and payment service by Safaricom Limited [44], is considered to be the pioneer mobile-money platform in Kenya.[45] With nearly 40% of the

---

[40] Olmsted v United States (1938) 277 US Supreme Court 438.

[41] Big data is data sets that are so voluminous and complex that traditional data processing application software are inadequate to deal with them. Big data challenges include capturing data, data storage, data analysis, search, sharing, transfer, visualization, querying, updating and information privacy.

[42] Edward Snowden: Leaks that exposed US spy programme, http://www.bbc.com/news/world-us-canada-23123964 on 13 December 2017.

[43] Privacy and Technology, https://www.aclu.org/issues/privacy-technology on 13 December 2017.

[44] Safaricom is Kenya's largest telecommunications company by net profit as well as the most profitable company in East Africa, https://www.businessdailyafrica.com/Safaricom-sets-new-record-as-market-value-hits-Sh630bn/-/539552/2658306/-/2rh06j/-/index.html on 13 December 2017.

[45] Muthiora B, *Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Mooney for the Unbanked*, Bill & Belinda Gates Foundation 2015, 9.

adult population excluded from financial inclusivity.[46] M-PESA was revolutionary in that it increased financial inclusion in the country to more than 60% of the adult population when it came into operation around March 2007.[47] Unfortunately, this mobile money platform, as well as many others in the country, operates in an environment where there is no specific law that protects customer data considering the huge volumes of data that they handle.

While the Central Bank of Kenya Act gives the Central Bank of Kenya (CBK) discretion to *"formulate and implement such policies as best promote the establishment, regulation and supervision of efficient and effective payment, clearing and settlement systems"*,[48] the Act is weak on the statutory authority required for the CBK to issue regulations on payment services generally. As such, privacy concerns as well as other issues such as safety of customer funds were not well addressed. As will be discussed later in this paper, this statutory authority was granted when the National Payment System Act was enacted in 2012. However, privacy concerns were not adequately catered for as will be discussed later.

A look at the business model adopted by most Mobile Money Operators (telecommunications) and approved by the CBK, reveals that the CBK allows telecommunications to issue mobile money in exchange (at par value) for cash held in a trust account under the custody of a trustee. Because the funds held in trust are separated from the funds of the service provider, the service provider is unable to use the funds and the money is safe from claims by creditors in the event of insolvency. Over time, as the size of the trust account increases, as the mobile money service grows in popularity, the trustee, in consultation with the CBK, makes a decision to spread the funds across several banks to reduce the risk of a single custodial bank failure.[49] This model, albeit guaranteeing the safety of customer funds, would see telecommunications collect a lot of customer personal information. This is because telecommunications would oversee all mobile money transactions carried out by their subscribers (customers).

In March 2014, there were 26.2 million mobile money accounts in Kenya and an estimated 12.5 million unique active users. That same month, 73.9 million transactions were reported, with a daily average of 2.38 million transactions or 27.5 transactions per second and a

---

[46] Muthiora B, *Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Mooney for the Unbanked*, 9.
[47] Muthiora B, *Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Mooney for the Unbanked*, 9.
[48] Section 4(A) and (d), *Central Bank of Kenya Act* (CAP. 491).
[49] Muthiora B, *Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Mooney for the Unbanked*, 11.

throughput value of KES 192.6 billion (USD 2.2 billion), primarily low-value retail transfers.[50] Mobile money users can make peer-to-peer (P2P) transfers, bill payments, and merchant payments, as well as receive social disbursements and international remittances. With 26.2 million mobile money accounts and 12.5 million active mobile money users, Kenya now has one of the highest mobile money penetration rates anywhere in the world.[51]

The success that mobile money has had on enabling the access to financial services for millions of Kenyans who were previously unbanked is unparalleled. Access to formal financial services has increased from 26% of Kenya's bankable population in 2006 to 67% in 2013.[52] Mobile phone financial services have played a key role in this. What began as money transfer services has now become a platform with a menu of financial services that includes money transfers, payments of goods and services, savings, credit, insurance, pensions, and even capital market products.[53]

More often than not, personal data is usually linked to mobile money transfers. Such data can include, date of birth, gender, whereabouts, the Internet Protocol (IP) address of your mobile device and metadata pertaining to the various kind of transactions involved.[54] Data which is used to secure other information, for example passwords, will not be discussed in this paper.

3.2 Privacy Concerns

a. Transparent Use without Privacy Protection

According to FATF Recommendations 10 and 11, financial institutions should not allow customers to conduct business anonymously; and they must maintain user transaction records for five years.[55] In most traditional banking settings, this requirement is both sensible and non-controversial. It does, however, raise significant questions for mobile money operators, particularly considering the limitations of privacy protections in Africa and in particular Kenya. For instance, a recent UN report noted that amongst the members of the EAC —

---

[50] Muthiora B, *Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Mooney for the Unbanked,* 15.

[51] Muthiora B, *Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Mooney for the Unbanked,* 6.

[52] Muthiora B, *Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Mooney for the Unbanked,* foreword.

Muthiora B, *Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Mooney for the Unbanked,* foreword.

[54] Privacy and Information Technology, https://plato.stanford.edu/entries/it-privacy/ on 13 December 2017

[55] FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations,* 2012, 16.

Burundi, Kenya, Rwanda, Tanzania, and Uganda—there is no legislation "that clearly defines who can get access to a mobile money trail, and how, when or under what conditions such access may be obtained."[56] Inadequate privacy protections can lead to abuse by governments and data brokers as well as leave personal information susceptible to theft or leakage, ultimately damaging user trust and limiting adoption and use.[57]

b. Limited Privacy Protections

A number of reasons can be given to try and explain the limits of privacy protection in Kenya. First, a strong communitarian strain exists throughout much of Africa as in Kenya. This mind set deemphasizes the rights of individuals in favour of those of community. In such a context, the privacy of individuals is given little consideration.[58] Second, traditional economies with limited electronic communication and commerce have less need for individual privacy protection as there are few means to collect, use, and exploit sensitive information. Until very recently, the vast majority of Africans did not engage in data compiling transactions. For both of the reasons above, there are few established legal protections in African nations, Kenya included. Most nations do not formally recognize a right to personal privacy, and most do not have laws or regulators in place to monitor abuse.[59] Compounding the lack of legal protections is the relative absence of public interest groups to monitor government behaviour, propose public policy, and promote awareness. This leads to situations where serious abuses can occur with little impediment. Even in South Africa or Ghana, where some legal protections are in place, illegal interception and abuse of electronic communications by intelligence agencies is routine.[60] While a limited privacy protection regime may have caused little concern just a short time ago, the African boom in mobile telephony significantly heightens the risk to consumers operating in an ecosystem without protection. This is especially true for Kenya where mobile money use and uptake is unparalleled.

---

[56] UN Conference on Trade and Development, 'Mobile Money for Business Development in the East African Community: A Comparative Study on Existing Platforms and Regulations,' 20.

[57] Harris A, Goodman S and Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa' *Washington Journal of Law, Technology and Arts* 2013, 249.

[58] Goodman S and Harris A, 'Emerging Markets: The Coming African Tsunami of Information Insecurity,' Vol 53 No 12, *Communications of the ACM*, December 2010, 24

[59] Hanno N, Olinger, Johannes J. Britz & Martin S Olivier, 'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa,' 39:1, *The International Information & Library Review*, 2007, 35

[60] Heidi Swart, *Secret State: How the Government Spies on You*, Mail & Guardian (14 October 2011), http://mg.co.za/article/2011-10-14-secret-state/ on 18 December 2017.

c. Potential for abuse

In the context of limited privacy protections and because FATF requires identity verification and data collection, data subjects may find their privacy threatened by governmental and corporate abuse. In cash-based economies, like Kenya, the spending and savings activities of individuals are known to an interested third party only with great effort.[61] This is the environment that most Africans have come to understand, developing social behaviours reflective of spending that is anonymous to government and corporate entities. Despite a lack of privacy protections, the inherent anonymity of cash prevents any other entity from knowing the extent of an individual's transactions. However, due to FATF requirements, the service provider can and must record every detail of a user's transactions in a mobile money environment. It is also important to note that the initial wave of mobile phone adoption was anonymous, as the vast majority of users purchased and used unregistered pre-paid phones. Many African nations, including Kenya, are now reversing this initial trend by requiring SIM-card registration, further reducing anonymity and potentially limiting private use.[62] The availability of mobile-money transaction data opens the door for abuse by an unscrupulous government, which could gain access to transaction records with little effort.[63] This information could then be used in a number of ways to harass, intimidate, or manipulate the violated citizen.

A fully employed mobile money ecosystem can include a mobile network operator (Telecommunications Company), financial institution, trusted service manager, marketer, retailer, and the data subject or customer. Each of these entities (other than the customer) has a growing interest in collecting personal information tied to mobile money transactions. With so many interested parties and little consumer protection, the opportunities for data leakage and subsequent abuse are abundant.[64]

It is vital to be cognisant of the fact that the threats of data leakage are amplified in a mobile money environment because how we spend is an important predictor of who we are and how

---

[61] Harris A, Goodman S and Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa' 250.

[62] Hemeson C, 'Directive on Consumer Data for SIM Card Registration in the Telecommunications Sector: An African Perspective,' *Chikaodili J Hemeson* , 2012, 7. Available at http://ssrn.com/abstract=1982033 on 18 December 2017.

[63] Koker L and Jentzsch N, 'Financial Inclusion and Financial Integrity: Aligned Incentives?' Proceedings of the 2011 Shadow conference, Munster, Germany, 28-31 July 2011, 24.

[64] Harris A, Frank S, Goodman Y, Traynor P, 'Emerging Privacy and Security Concerns for Digital Wallet Deployment' in Aspray W, Doty P (eds), *Privacy in America: Interdisciplinary Perspectives*, Scarecrow Press, 2011, 185.

we will spend or possibly otherwise behave in the future. Since FATF requires recording of user transactions by mobile money operators, this information is necessarily compiled and available for use. The ability to connect basic personal information to spending records obtained through mobile phones has great commercial use—and potentially misuse. In places where mobile money is not yet extensively used, like North America and Europe, a spending record connected to the user's mobile phone is less accessible or not available at all, so nations in these regions have not yet needed to wrestle fully with the implications of mobile money data.[65] But in Africa, particularly Kenya, mobile money data sets are quickly growing.[66] As Kenyans also begin to use their phones to access the Internet, the incentives to commoditize this data will grow and present challenges yet unseen in Western nations.

The great potential for abuse of personal information can harm not only the violated data subjects, but also the overall economy. If governments and telecommunications as well as other corporations abuse users' trust, they will curtail adoption and limit the utility of mobile money, thus limiting the application's utility and holding back development within the country. In most African nations, there is little to stop governments or corporations from pushing the boundaries of acceptable use with regards to revealing mobile money data.[67] If widespread abuse becomes commonplace, users may walk away from mobile money and all its enormous benefits.

3.3 The need for data protection in Kenya

Kenya's current legislation does not define who can get access to a mobile money trail and how, when or under what conditions such access may be obtained. This complicates efforts to keep consumer information private while at the same time conflicts with the desire for regulators to keep customer funds safe against financial crimes. In addition, the privacy regulations that apply to commercial banks in respect of customer financial records do not extend to telecommunications dealing with mobile money transfers.[68]

---

[65] Harris A, Goodman S and Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa' 251.

[66] Harris A, Goodman S and Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa' 251.

[67] Harris A, Goodman S and Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa'252.

[68] Malala J, 'Consumer Protection for Mobile Payments in Kenya: An Examination of the Fragmented Legislation and the Complexities it Presents for Mobile Payments' Kenya Bankers Association, KBA Centre for Research on Financial Markets and Policy Working Paper Series WPS/02/14, 2013, 34 - http://www.kba.co.ke/downloads/Working%20Paper%20WPS-07-13.pdf on 20 December 2017.

Andrew Harris, Seymour Goodman, and Patrick Traynor in their paper on *Privacy and Security Concerns Associated with Mobile Money Applications in Africa* note that, in a cash based economy, such as Kenya, the spending and savings activities of individuals are known to an interested third party only with great effort as stated before. Spending is anonymous to government and corporate entities. However, with mobile money transfers, which are very prevalent in Kenya, the service provider can and must record every detail of a user's transactions in a mobile money environment.[69] This in effect eliminates the anonymity that would have been there had cash been used as some personal data might be recorded by the service provider e.g. name of person doing the money transfer, item purchased (if it was a sale), place of transaction, and amount spent among other data usually collected. The availability of transaction data opens the door for abuse by an unscrupulous government, which could gain access to transaction records with little effort. This information could then be used in a number of ways to harass, intimidate, profile or manipulate the violated data subject.

Corporate abuse of personal information can similarly have insidious effects in the mobile money environment of Kenya without legal safeguards. Mobile money services necessarily operate in a data rich environment that incentivises for the commodification of personal information from and thus targeted advertising. Liberal collecting and sharing policies result in electronic dossiers useful for not only providing targeted advertising, but also for making decisions regarding employment or credit worthiness as well as for committing fraud.[70]

Mitake, in his paper, *Mobile cellular Communication and its Effect on Personal Data Protection in Tanzania* notes that, when personal data is protected, automatically the right to privacy is guaranteed.[71] He further notes that the Electronic and Postal Communications Act of Tanzania mandatorily requires that every holder of a SIM card to register the SIM card. In Tanzania, the registration data is a very huge collection of personal data including information and copies of documents such as driving license, traveling pass, social security ID card and so on, all which can be subject to misuse if not properly protected.[72] However,

---

[69] Harris A, Goodman S and Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa' 250.

[70] Harris A, Goodman S and Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa' 252.

[71] Mitake M, 'Mobile cellular Communication and its Effect on Personal Data Protection in Tanzania' Unpublished LLM Thesis, Faculty of Law, University of Oslo, 15 May 2014, 20.

[72] Mitake M, 'Mobile cellular Communication and its Effect on Personal Data Protection in Tanzania' Unpublished LLM Thesis, Faculty of Law, University of Oslo, 15 May 2014, 24.

there is a provision in the same law which provides for protection of such data after it has been collected by the relevant authorities from misuse and abuse by the collecting authorities and other third parties.[73] Due to absence of such a law in Kenya as earlier stated, this makes personal data collected by telecommunication companies involved in mobile money transfers vulnerable to misuse and abuse.

It is however prudent to bear in mind that the above article only considers personal data that is used when registering a SIM card in Tanzania and not personal data associated with mobile money transfers as is the case with this study.

Paul Makin, a principal consultant at Consult Hyperion, which was the firm charged with overseeing the conception and development of M-PESA,[74] raises some various issues in his analysis about regulation of the mobile money services. He notes that with mobile money services there is huge comprehensive set of reporting and management tools, which allow detailed views and reporting of every aspect of every transaction, both individually and en masse. Customer information is also stored in true end-to-end encrypted SIMs, where all confidential customer data is held.[75] Insofar as this is a very progressive step in curbing money laundering or financing of terrorist activities as it puts a check to the trail of money, it would be very unfortunate if such data is not further protected though data protection law. Such data would be prone to abuse and misuse by telecommunications companies, the government or data brokers.

The following are moral reasons for the protection of personal data and for providing direct or indirect control over access to those data by others include;[76]

i. Prevention of harm: Unrestricted access by others to one's passwords, characteristics, and whereabouts can be used to harm the data subject in a variety of ways.

---

[73] Section 93, *Electronic and Postal Communications Act* (Tanzania, 2011).

[74] M-PESA is a Mobile Money Service offered by Kenya's leading Telecommunications Company, Safaricom. It began running on March 2007 as the first of its kind in Kenya and Africa at large. It facilitates Mobile Money Transfers among subscribers to the network cheaply and reliably through their mobile phones. It also offers other facilities such as the ability to store small amounts of money in one's phone and to pay for services using money loaded in one's mobile wallet - https://www.safaricom.co.ke/personal/m-pesa/getting-started/experience-m-pesa on 13 December 2017.

[75] Makin P, 'Regulating Issues Around Mobile Banking: New initiatives to bank the poor are straining the world's financial regulatory systems,' *OECD*, 2009, 7.

[76] Privacy and Information Technology, https://plato.stanford.edu/entries/it-privacy/ on 13 December 2017.

ii. Informational inequality: Personal data have become commodities. Individuals are usually not in a good position to negotiate contracts about the use of their data and do not have the means to check whether partners live up to the terms of the contract. Data protection laws, regulation and governance aim at establishing fair conditions for drafting contracts about personal data transmission and exchange and providing data subjects with checks and balances, guarantees for redress.

iii. Informational injustice and discrimination: Personal information provided in one sphere or context (for example, health care) may change its meaning when used in another sphere or context (such as commercial transactions) and may lead to discrimination and disadvantages for the individual.

iv. Encroachment on moral autonomy: Lack of privacy may expose individuals to outside forces that influence their choices.

These formulations all provide good moral reasons for limiting and constraining access to personal data and providing individuals with control over their data. This is more so true looking at the current situation in Kenya with regards to mobile money transfers.

3.4 A look at current data protection framework and legislation that threatens information privacy

Currently, there is no legislation that specifically caters for data protection within the country. However, as stated earlier the Constitution outlines the entrenching provision with regards to data protection under article 31(c) & (d).

The failure of a comprehensive law on data protection is further aggravated by various legislations that threaten the right to privacy.

The Registration of Subscribers of Telecommunications Services Regulations (2014) of the Kenya Information and Communications Act (1998) requires operators to provide the Communications Authority "access to its systems, premises, facilities, files, records and other data to enable the Commission inspect..."[77] This provision puts individuals' privacy at risk as it is not clear as to the limitations of data, which is usually contained in the systems, which a telecommunications should provide for inspection.

[77] Section 13, *Kenya Information and Communications Act* (*Registration of Subscribers of Telecommunications Services Regulations*, 2014) (Act No. 2 of 1998).

The National Intelligence Service Act (2012) establishes the authority of the Director-General to intercept individual communications when he or she "has reasonable grounds to believe that a covert operation is necessary to enable the National Intelligence Service (NIS) to investigate or deal with any threat to national security or to perform any of its functions."[78] This provision again further delimits the right to information privacy as mobile money transfers as primarily communication between ones phone and his or her mobile service provider (Telecommunication Company). This communication is subject to interception by the NIS by virtue of this provision. This power, however much checked by the judiciary,[79] can still be abused as it is commonly alleged that the NIS possesses direct access to telecommunications networks today and are capable to obtain digital content and data without prior judicial notice or authorisation. An enactment of a law on data protection would however criminalise unauthorised access of data thereby making the NIS liable to pay compensation for any damage it might occasion an individual by such a breach of his or her privacy. Such a law would most certainly make mobile money transfer records safer as it would reduce the likelihood of potential abuse by state apparatus. Privacy violations by government would thus only be done in matters that are of utmost importance for which it can be proven so.

The Prevention of Terrorism Act (2012) was amended by the adoption of the Kenya Security Laws (Amendment) Act of 2014. A new provision was introduced which allows for interception of communication by the National Security Organs. These organs may now intercept communication for the purposes of detecting, deterring and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary.[80] Also, the same provision provides that, the right to privacy under Article 31 of the Constitution shall be limited for the purpose of intercepting communication directly relevant in the detecting, deterring and disrupting terrorism. This limitation, in and of itself, is unconstitutional by virtue of article 24 (1) (e) of the Constitution in that it doesn't expressly state whether only article 31 (d) is limited or the whole of article 31 which goes beyond only privacy of communication but also includes privacy of person, home, property and information relating to an individual's family and/or private affairs.

[78] Section 42(2), *National Intelligence Service Act* (No. 28 of 2012).
[79] Section 42(3) and (d), *National Intelligence Service Act* (No. 28 of 2012).
[80] Section 36A, *Prevention of Terrorism Act*, (No. 30 of 2012).

Article 35 of the Constitution of Kenya provides that every citizen has the right of access to information held by the state and information held by another person and required for the exercise or protection of any right or fundamental freedom. This provision, in and of itself, would perhaps work against the principles of data protection enumerated in chapter 2 of this study. The Access to Information Act 2016, which is the entrenching law with regards to article 35 provides for the framework under which information may be obtained. The act guarantees the freedom to information by every citizen and mandates public or private entities to provide information sought at a reasonable cost.[81] The act further provides that, pursuant to article 24 of the Constitution on limitation of rights, the right of access to information under article 35 of the Constitution shall be limited in respect of information whose disclosure is likely to involve the unwarranted invasion of the privacy of an individual, other than the applicant or the person on whose behalf an application has, with proper authority, been made.[82] Certainly, information relating to an individual's mobile money transactions, if acquired arbitrarily would amount to an unwarranted invasion of privacy of an individual. Additionally, it is not clear how one should go about in obtaining authority of an individual with regards to the limitation in section 6(1) (b). This again leaves individuals in a precarious position as the law provides that prior authorisation is needed for privacy sensitive information acquisition but it doesn't provide a framework for obtaining such authority.

These legislations clearly show that there is indeed a dire need for a data protection law in the country that not only protects individuals' data, but also outlines the procedure for the collection, retrieval, processing, storage, use and disclosure of such data.

[81] Section 4 (2), *Access to Information Act* (Act No 31. of 2016).
[82] Section (1) (d), *Access to Information Act,* 2016 (Act No.31 of 2016).

CHAPTER 4 - COMPARATIVE STUDY OF LEGISLATION IN GHANA AND KENYA'S DATA PROTECTION BILL

Data protection laws are present in most developed economies with advanced payment systems. The centrally unifying moral principle underlying these laws is the requirement of informed prior consent for processing by the data subject.[83] More to obtaining consent, processing of personal information mandates that its purpose be specified, its use b limited, individuals be notified and allowed to correct inaccuracies, and the holder of the data be accountable to oversight authorities.[84] Because it is not possible to guarantee compliance of all types of data processing in all these areas and applications with these rules and laws in traditional ways, so-called privacy-enhancing technologies and identity management systems are expected to replace human oversight in many cases. Thus the challenge we are now faced with regarding privacy in the twenty-first century, world over, is to assure that technology is designed in such a way that it incorporates privacy requirements in the software, architecture, infrastructure, and work processes in a way that makes privacy violations unlikely to occur.

Over the last decade, mobile telephony has enjoyed phenomenal adoption rates across most of Africa. Since 2005, there has been a five-fold increase in the number of African mobile phone subscriptions resulting in 53.1 mobile phone subscriptions per 100 inhabitants in 2011.[85] While other parts of the world have embraced mobile phones to a greater degree, the relative impact in the African Continent, where fixed telephone lines are available to less than 2 per cent[86] of the population, is perhaps greater than anywhere else. As the primary means of communication for most Africans, mobile phones have become a source of significant economic growth and a platform for innovation. One of the most dynamic of these innovations has been mobile money, as highlighted earlier in this paper, the use of mobile phones to send and receive money as well as purchase goods or services through funds connected to the user's account. With a broad base of mobile phone users, already in place, the widespread adoption of mobile money could have enormous positive impacts across Africa. On a continent with too few banking options necessary for a dynamic and modern economy, mobile money has the potential to address long-existing gaps in African

---

[83] Privacy and Information Technology, https://plato.stanford.edu/entries/it-privacy/ on 13 December 2017.

[84] Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm on 13 December 2017.

[85] Key Global Telecom Indicators for the World Telecommunication Service Sector, http://www.itu.int/ITU-D/ict/statistics/at_glance/keytelecom.html on 13 January 2018.

[86] Harris A, Goodman S and Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa' 247.

economies.[87] Unfortunately, the rapid growth of mobile telephony in Africa has largely not been accompanied by appropriate consideration for privacy and security concerns, opening the door for abuse and erosion of the application's utility.

Ghana, just like Kenya, has robust mobile money operations. According to the most recent Financial Inclusion Insights (FII) survey, access to formal financial services in Ghana increased by 41 per cent between 2010 and 2015, largely thanks to the uptake of Mobile Money.[88] FII is the leading program produces original data and practical knowledge on trends in mobile money and other digital financial services for over 10 African countries.[89] In June 2016, the Central Bank of Ghana released figures showing that Mobile Money transactions in Ghana had grown 20 per cent since the end of 2015, reaching 679.71 million Ghanaian Cedi ($177.9 million).[90] This, compared to Kenya's mobile money transactions of the same year makes Ghana the second country after Kenya in terms of volumes of mobile money transactions in Africa[91] and hence the reason to look at Ghana in comparison to Kenya. Despite Kenya's huge mobile money transfer volumes. Ghana unlike Kenya has a legal framework already in place for data protection.

4.1 Ghana

The Data Protection Act, 2012 (Act 843)[92] sets out the rules and principles governing the collection, use, disclosure and care an individual's personal data or information by a data controller or processor. It recognises a person's right (data subject rights) to protect their personal data or information by mandating a data controller or processor to process (collect, use, disclose erase, etc.) such personal data or information in accordance with the individual's rights. The Act also established the Data Protection Commission as an independent statutory body to ensure and enforce compliance.

In Ghana, the recognition of the right to privacy with respect to the processing of personal data or information led to the passage of the Act 843 to further guarantee the right to privacy

---

[87] Mobile Money in Africa: Press 1 for Modernity, The Economist, http://www.economist.com/node/21553510 on 13 January 2018.
[88] How Ghana is using Mobile Money to go cashless, http://africa.businesschief.com/technology/2521/How-Ghana-is-using-Mobile-Money-to-go-cashless on 14 January 2018.
[89] Practical Insightful Research to change the course of Lives http://finclusion.org/ on 14 January 2018.
[90] How Ghana is using Mobile Money to go cashless, http://africa.businesschief.com/technology/2521/How-Ghana-is-using-Mobile-Money-to-go-cashless on 14 January 2018.
[91] Ghana Banking Survey: How to Win in an Era of Mobile Money, A 2016 report by PwC on Ghana's Banking Industry, https://www.pwc.com/gh/en/assets/pdf/2016-banking-survey-report.pdf on 18 January 2018.
[92] Preamble, Act 843, *Data Protection Act,* 2012 (Ghana).

enshrined under Article 18(2) of the 1992 Constitution. Large amounts personal data generated in the country are kept across servers, networks and various filing systems in different locations (electronically & manually), locally and abroad. These have the potential of being shared by different legal and natural persons, across borders in a way that violates the right to privacy.

The Act provides standard principles that must be complied with by all who process personal information across the country and beyond.[93] The law applies to all forms of personal data or information stored on both electronic and non-electronic platforms including mobile money related information.[94]

The Act is premised on the fundamental rule that all who process personal data must take into consideration the right of that individual to the privacy of his or her communications. This recognition by a data controller or processer should lead to the application of the Eight (8) Basic Principles whiles processing such information highlighted in chapter 2.

The Act guarantees individuals' right to privacy by giving individuals the power to access and control how their personal information is processed, collected, used and disclosed.[95]

Some of the key rights guaranteed by the act include[96];

i. Access to personal information,
ii. Right to amend your personal information,
iii. Right to prevent processing of your personal information,
iv. Rights to freedom from automated decision making,
v. Right to prevent processing of personal data for direct marketing purpose,
vi. Right to seek compensation through the courts, and,
vii. Right to complain to the Data Protection Commission.

4.2 Kenya

The Data Protection Bill is proposed legislation intent on giving effect to Article 31 of the Constitution of Kenya.

---

[93] Part 2 (Sections 17-27), Act 843, *Data Protection Act 2012* (Ghana).
[94] Section 21, Act 843, Data Protection Act 2012 (Ghana).
[95] Section 18, Act 843, *Data Protection Act 2012* (Ghana).
[96] Part 2, Act 843, *Data Protection Act 2012* (Ghana).

The Bill as established is meant to be enforced by the Commission on Administrative Justice[97] unlike the Ghanaian law which created a Data Protection Commission. The Key principle behind it is that in the automatic processing of data, the data should not be disclosed to any third parties without the permission or consent of the person to whom the information is obtained.[98] It has been drafted as a bill to regulate the collection, processing, keeping, use and disclosure of certain information relating to individuals that is processed automatically.[99] Such data includes mobile money transfer information as demonstrated earlier.

The bill, as currently drafted, incorporates most of the fundamental features of a data protection law. These include;[100]

i. It allows for the collection or storage of data provided it is done so lawfully and does not intrude upon the privacy of data subject to an unreasonable extent. With regards to mobile money transfers this provision is important in that it stops data holder or agents from unlawfully using data in their possession to infringe on the privacy of individuals i.e. data subjects.

ii. Information must be collected directly from and with the consent of the data subject. This provision stops telecommunications, which hold mobile money customer data, from using the data in their possession without the consent of the data subject. More to that, this provision requires that telecommunications or other third parties dealing with customer mobile money metadata, to get data directly from the data subject where possible.

iii. The bill also requires that the data subject be informed of the purpose for which data is to be collected prior to collection. This is crucial especially since telecommunications deal with big data concerning mobile money transfers which as outlined earlier have a high potential for abuse.

iv. Lastly, the bill requires that appropriate technical and organizational measures have to be taken to safeguard the data subject against the risk of loss, damage, destruction of or unauthorized access to personal information. This is very important especially for telecommunications dealing with customer data on mobile money transactions. Currently, the National Payment Systems Regulations (NPS) of 2014 provide for consumer protection. Section 42 of the regulations

[97] Clause 20, *Data Protection Bill (2013).*
[98] Clause 5, *Data Protection Bill (2013).*
[99] Clause 8, *Data Protection Bill (2013).*
[100] Clause 3, *Data Protection Bill (2013).*

provide that disclosure of confidential customer information is prohibited except under the following circumstances;

a. To the customer concerned,
b. To the central Bank,
c. When authorised in writing by the customer concerned, or
d. As required by law.

These circumstances however fail to capture the overarching principle of consent which is very crucial in data protection. Before any dissemination of personal data the person(s) holding the data must seek the consent of the data subject.

A look at M-PESA's terms and conditions (T&Cs) of service, which mirrors most mobile money platforms T&Cs, will reveal that in deed there is a privacy policy.[101] The privacy policy recognises the importance of protecting the privacy of all information provided by users of M-PESA. In the policy, Safaricom, the telecommunication company offering the M-PESA service, admits to collect personally identifiable information that it uses to profile M-PESA users and administer individual M-PESA accounts, update M-PESA databases, and provide user support.[102]

The policy however guarantees that Safaricom doesn't share user personal information with unauthorised persons and adequate safeguards have been put in place to prevent unauthorised access and to ensure confidentiality of your personal information.[103]

The privacy policy also provides that Safaricom shall have the right to monitor user account usage and may disclose personal information to local law enforcement or investigative agencies or any competent regulatory or governmental agencies to assist in the prevention, detection or prosecution of money laundering activities, fraud or other criminal activities.[104] This leaves the personal information of a data subject vulnerable to governmental seizure in the name of 'prevention, detection or prosecution of money laundering activities, fraud or other criminal activities'.

---

[101] Section 4.0, *Safaricom M-PESA Customer Terms and Conditions*, 2007.
[102] Section 4.2, *Safaricom M-PESA Customer Terms and Conditions*, 2007
[103] Section 4.3, *Safaricom M-PESA Customer Terms and Conditions*, 2007
[104] Section 4.6, *Safaricom M-PESA Customer Terms and Conditions*, 2007.

The wording of the policy under section 4.7 states that "Safaricom employees who handle personal information are under an obligation to treat it confidentially and may not disclose it to unauthorized third parties." The use of the word 'may' again leaves the data subject in a precarious position as it leaves the personal information to the whims of Safaricom employees.

Additionally, it would be neater and tidier for the bill to insert provisions on the fundamental Right to Data Protection in the following terms;

i. Every person shall have the right to secrecy for the personal data concerning him especially with regard to his or her private and family life, in so far as he or she has an interest deserving such protection. Such data can include; medical payments, insurance payments, certain online purchases among others. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject.

ii. In so far as personal data is not used in the vital interest of the data subject or with his consent, restrictions to the right to secrecy are only permitted to safeguard overriding legitimate interests of another. But even in the case of permitted restrictions, the intervention with the fundamental right shall be carried out using only the least intrusive of all effective methods.

These two provisions will provide the much needed clarity as to what persons holding customer data can or cannot do with such data. This is especially more apparent to the Kenyan situation considering that there are currently no rules for agents of mobile money transactions.[105]

Also, these two provisions will hopefully ensure design and enforcement of data privacy and security rules contained in the T&Cs of the various mobile money platforms, which require some level of coordination between supervisory and regulatory authorities, as mobile payments cuts across different sectors such as banking and telecommunications. If the current privacy provisions of the various T&Cs of mobile money platforms could be amended to include rules as to right to secrecy as provided above, then much needed clarity would be available to the agents handling customer data as relates to mobile money transfers.

[105] Malala J, 'Consumer Protection for Mobile Payments in Kenya: An Examination of the Fragmented Legislation and the Complexities it Presents for Mobile Payments' 35.

In summary, regulators and mobile money providers, in Kenya, need to work together to understand security concerns and maintain the integrity of customer data, just like in Ghana. In both countries, mobile money operators have developed various systems to protect customer privacy. Typically, they back up their IT systems (at least) daily, and the Unstructured Supplementary Services Data (USSD) and the SIM Application Tool Kit (STK) channels used to transact mobile money customer orders have so far proven to be sufficiently secure, over the years. USSD is also session-based, which leaves no traces of the transaction once the session is closed. SMS (Short Messaging Service) is encrypted over secure links.[106] Customers are also responsible for protecting their password, PIN number, and other sensitive information. This however doesn't eliminate the need to have a Data Protection Act for Kenya as such a law will bring with it the much needed clarity on who is responsible if data associated with mobile money falls into the wrong hands.

[106] Malala J, 'Consumer Protection for Mobile Payments in Kenya: An Examination of the Fragmented Legislation and the Complexities it Presents for Mobile Payments' 36.

CHAPTER 5 - CONCLUSIONS AND RECOMMENDATIONS

The importance of digital technologies in driving the economy cannot be overemphasised. While perhaps one of the most dynamic and compelling, mobile money is just one of many technologies with the power to help transform African economies. Privacy and data protection concerns are distinct issues that arise in any electronic platform especially payment systems. Due to the convergence of the industries, consumer protection policies are not specific to the needs of mobile payments.[107] However, with financial resources understandably limited, parliament should take policy and/or legislative actions that will increase user trust and privacy protections within the mobile money sector which is prevalent in Kenya and Africa at large and more akin to African payment systems.

Primary amongst these steps is instituting a comprehensive but flexible privacy regime and in particular enacting a law on Data Protection. In reviewing the lack of privacy regulation in East Africa, the United Nations Conference on Trade and Development (UNCTAD) declares that "simple and transparent mechanisms are needed through which users can authorize an entity to access" data associated with mobile money.[108] Individuals should be empowered through national legislation to control their personal information and corporations should be required to use that information only in contextually appropriate ways. Licensing for mobile money services should include explicit rules for the collection and sharing of personal information.

Crucially, it is imperative that parliament implements comprehensive regulations rather than taking a sectorial approach, as has unfolded in the United States.[109] Sector-specific laws may prove inadequate for converged technologies like mobile money transfer, leaving banks, telecommunications companies, and data brokers with differing requirements leading to inconsistent treatment of user data.[110] The NPS regulations are indeed welcomed but, there needs to be a more comprehensive legal document dealing only with mobile money transactions so as to eradicate any room for doubt amongst the relevant players in the industry.

---

[107] Malala J, 'Consumer Protection for Mobile Payments in Kenya: An Examination of the Fragmented Legislation and the Complexities it Presents for Mobile Payments' 37.
[108] UN Conference on Trade and Development, 'Mobile Money for Business Development in the East African Community: A Comparative Study on Existing Platforms and Regulations,' 35.
[109] Harris A, Frank S, Goodman Y, Traynor P, 'Emerging Privacy and Security Concerns for Digital Wallet Deployment' 185.
[110] Harris A, Frank S, Goodman Y, Traynor P, 'Emerging Privacy and Security Concerns for Digital Wallet Deployment', 185.

Kenya should follow in the steps of Ghana which enacted its Data Protection law in February 2012.[111] This is a comprehensive law that establishes users' rights of data access, control, and consent of use.[112] The Ghanaian law, as highlighted, creates a Data Protection Commission to enforce and regulate the provisions of the Ghana Data Protection Act, 2012.

While protecting citizens should be a primary concern for policymakers, they must also seek balance in any law, working to ensure that new legislation is not overly prescriptive or burdensome for corporations bringing innovative tools to the marketplace. For instance, while many international businesses welcome the European's new privacy plans to streamline privacy rules in a more centralized manner, these same companies also protest the regulation's more stringent guidelines such as the proposal for an individual's "right to be forgotten."[113] While the proper balance between adequate protection and flexible business operations is certainly delicate, parliament must act in order to ensure the ultimate success of mobile money.[114]

Following four years of development, the European Union (EU) General Data Protection Regulation (GDPR) was adopted on 27 April 2016 and is set to come into force across the EU on 25 May 2018. The GDPR aims to consolidate and strengthen data protection rights for individuals within the EU. One striking feature that we could borrow from the GDPR is that consent has been made more onerous for organisations to satisfy and the requirements for the content of privacy notices are changed meaning all organisations will likely need to amend their existing privacy notices and terms.[115] The importance of consent cannot be overemphasised. Consent is the hallmark of data protection. As such it should be carefully crafted in our data protection bill as well as the T&Cs of mobile money platforms.

Regulations adopted should be consistent and robust enough to hold providers responsible for data privacy, and they should be liable for privacy breaches and misuse of customer data. Regulation also needs to be technology neutral, since imposition of specific standards and protocols in a rapidly evolving industry is likely to hinder innovation.

---

[111] Daily Guide, *Data Protection Bill Passed*, Ghanaweb (10 Feb 2012), http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=229717 on 23 December 2017.

[112] Data Protection Act 843 of 2010 (Ghana) http://www.parliament.gh/assets/file/Bills/Data%20Protection%20Act,%202010.pdf on 3 January 2018

[113] Privacy Laws: Private Data, Public Rules, The Economist (28 January 2012), http://www.economist.com/node/21543489 on 3 January 2018.

[114] Harris A, Goodman S and Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa' 258.

[115] Article 32, *General Data Protection Regulations*, 2018 (European Union).

To address the lack of technical capacity, policy makers should stress the study of security, privacy, computer science and information programs in universities. There is a growing demand for African app developers, and universities will train many of them. These universities should insist on strong privacy and security backgrounds. These courses of study should be promoted as holding particular import for future development with incentives created to draw in prospective students. To help facilitate a greater emphasis on privacy and security at the university level, policy makers should encourage empowering partnerships with international institutions that excel in the field. For instance, the Rwandan government recently sponsored a Carnegie Mellon University campus in Kigali with the government committing to offer substantial scholarships to qualifying applicants. Carnegie Mellon's Rwanda campus offers Masters of Science in Information Technology with the option to focus on cyber-security and began classes in the fall of 2012.[116] This action is a clear indication that the Rwandan government understands that technological advances must be accompanied with sufficient human capacity. Similar partnerships coupled with the promotion of security and privacy studies can help African nations make strides in addressing human capacity issues.[117]

African application developers and service providers can of course begin to place a greater emphasis on personal privacy and security by designing solutions to protect networks and data and providing users tools to protect themselves and their devices. In considering the problems of transparency in mobile money applications in the African context, developers could explore some of the benefits of e-cash, a primarily conceptual digital currency in which transactions are anonymous and funds cannot be double-spent. Bitcoin is the most prominent manifestation of e-cash, although numerous technical and regulatory problems exist with this particular implementation.[31] With proper research, mobile money applications may find some of the principles and features of e-cash useful in introducing layers of anonymity and protection for users.

Parliament in conjunction with the relevant state agencies such as the Communications Authority of Kenya should commission public awareness campaigns focused on cyber-security and personal data. Public awareness campaigns can increase digital literacy, informing consumers of basic dos and don'ts to protect themselves and others.

---

[116] Carnegie Mellon University in Rwanda, http://www.cmu.edu/rwanda/ on 10 January 2018.

[117] Harris A, Goodman S and Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa' 258.

Finally, there is no doubt about the enormous potential for mobile money in Kenya and Africa at large. For a country that was plagued by limited banking options, mobile money has in just a short time brought millions to the ranks of financial inclusion. The increased data collection, record keeping and transparency as required by FATF, renders mobile money users in Africa particularly vulnerable to governmental or corporate abuse of the data generated by mobile transactions. Equally troubling are cyber-security concerns, leaving mobile money users in a double precarious position. Should mobile money platforms come to be inundated with privacy breaches and malware, users will lose trust in the application, reversing adoption trends and eliminating potential gains. It is therefore incumbent for all to act—government, human rights watchdogs, corporations, and individual citizens—to address existing deficiencies and ensure that the enormous power of mobile money will be enjoyed in Kenya and across Africa at large.

BIBLIOGRAPHY

Books and Book Chapters

1. Harris A, Frank S, Goodman Y, Traynor P, 'Emerging Privacy and Security Concerns for Digital Wallet Deployment' in Aspray W, Doty P (eds), *Privacy in America: Interdisciplinary Perspectives*, Scarecrow Press, 2011.
2. Freund P, *Privacy: One Concept or Many*, Atherton Press, New York, 1971.
3. Benn S, *Privacy Freedom and Respect for Persons*, Atherton Press, New York, 1971.

Journal articles

1. Harris A, Goodman S and Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa' *Washington Journal of Law*, Technology and Arts 2013.
2. Hemeson C, 'Directive on Consumer Data for SIM Card Registration in the Telecommunications Sector: An African Perspective,' *Chikaodili J Hemeson*, 2012.
3. Hanno N, Olinger, Johannes J. Britz & Martin S Olivier, 'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa,' 39:1, *The International Information & Library Review*, 2007.
4. Goodman S and Harris A, 'Emerging Markets: The Coming African Tsunami of Information Insecurity,' Vol 53 No 12, *Communications of the ACM*, December 2010.
5. Warren S and Brandeis L, 'The Right to Privacy' *Harvard Law Review*, 1890.
6. Fried C, ' Privacy' *77 The Yale Law Journal* 1968.
7. Gerety T, 'Redefining Privacy' *12 Harvard Civil Rights-Civil Liberties Law Review* 1977.
8. Nissenbaum H, 'Protecting Privacy in an Information Age: The Problem of Privacy in Public' *17 Law and Philosophy* 1998.
9. Westin AF, 'Privacy and Freedom' 25 *Washington and Lee Law Review* 1968.
10. Reiman JH, 'Privacy, Intimacy and Personhood' *6 Philosophy & Public Affairs* 1976.
11. Gavison RE, 'Privacy and the Limits of the Law' *89 The Yale Law Journal* 1980.

Legal Instruments

1. Constitution of Kenya 2010.

2. African Union Convention on Cyber Security and Personal Data Protection.

3. Access to Information Act (Act No. 31 of 2016).

4. Central Bank of Kenya Act (CAP 491).

5. Data Protection Act, Act 843 (Ghana).

6. Electronic and Postal Communications Act (Tanzania).

7. Kenya Information and Communications Act (Act No. 2 of 1998).

8. National Intelligence Act (No. 28 of 2012).Prevention of Terrorism Act (No. 30 of 2012).

9. Universal Declaration of Human Rights, UN GA res 217A (III), UN Doc A/810.

Internet Sources

1. Carnegie Mellon University in Rwanda, http://www.cmu.edu/rwanda/.

2. Daily Guide, *Data Protection Bill Passed*, Ghanaweb (10 Feb 2012), http://www.ghanaweb.com/GhanaHomePage/NewsArchive/artikel.php?ID=229717 on 23 December 2017.

3. Data Protection Principles, https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/.

4. Do Mobile Money Clients Need More Protection? http://www.cgap.org/blog/do-mobile-money-clients-need-more-protection.

5. Right to Privacy is a fundamental right; it is intrinsic to the right to life: Supreme Court, https://timesofindia.indiatimes.com/india/right-to-privacy-is-a-fundamental-right-supreme-court/articleshow/60203394.cms on 9 December 2017.

6. 1791: US Bill of Rights (1st 10 Amendments) - with commentary http://oll.libertyfund.org/pages/1791-us-bill-of-rights-1st-10-amendments-with-commentary.

7. Stanford Encyclopaedia of Philosophy: Privacy and Information Technology, https://plato.stanford.edu/entries/it-privacy/.

8. FATF, http://www.fatf-gafi.org/about/.

9. Mobile Money Transactions Hit 3 Billion Kenya Shillings a Day, https://www.standardmedia.co.ke/business/article/2000197514/mobile-money-transactions-in-kenya-hit-sh3-billion-a-day.

10. University of Edinburgh: The Eight Data Protection Principles, http://www.ed.ac.uk/records-management/data-protection/what-is-it/principles.

11. Processing personal data for specified purposes (Principle 2), https://ico.org.uk/for-organisations/guide-to-data-protection/principle-2-purposes/.

12. Edward Snowden: Leaks that exposed US spy programme, http://www.bbc.com/news/world-us-canada-23123964.

13. Privacy and Technology, https://www.aclu.org/issues/privacy-technology.

14. Safaricom is Kenya's largest telecommunications company by net profit, https://www.businessdailyafrica.com/Safaricom-sets-new-record-as-market-value-hits-Sh630bn/-/539552/2658306/-/2rh06j/-/index.html

15. Heidi Swart, Secret State: How the Government Spies on You, Mail & Guardian (14 October 2011), http://mg.co.za/article/2011-10-14-secret-state/.

16. M-PESA is a Mobile Money Service offered by Kenya's leading Telecommunications Company, Safaricom, https://www.safaricom.co.ke/personal/m-pesa/getting-started/experience-m-pesa.

17. Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.html.

18. Key Global Telecom Indicators for the World Telecommunication Service Sector, http://www.itu.int/ITU-D/ict/statistics/at_glance/keytelecom.html.

19. Mobile Money in Africa: Press 1 for Modernity, The Economist, http://www.economist.com/node/21553510.

20. How Ghana is using Mobile Money to go cashless, http://africa.businesschief.com/technology/2521/How-Ghana-is-using-Mobile-Money-to-go-cashless.

21. Practical Insightful Research to change the course of Lives http://finclusion.org/.

Conference Reports, Reports and Working Papers

1. Scharwatt C, Katakam A, Jennifer F, Murphy A, and Naghavi N, 'Global System for Mobile Phone Communication Association: Mobile Money for the Unbanked, Mobile Money Definitions, GSMA, 2010.

2. Financial Action Task Force (FATF), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*: The FATF Recommendations, 2012.

3. Makin P, 'Regulating Issues Around Mobile Banking: New initiatives to bank the poor are straining the world's financial regulatory systems,' *OECD*, 2009.

4. UN Conference on Trade and Development, 'Mobile Money for Business Development in the East African Community: A Comparative Study on Existing Platforms and Regulations,' *UN Publication UNCTAD/DTL/STICT/2012/2*, 2012.

5. Makin P, 'Regulating Issues Around Mobile Banking: New initiatives to bank the poor are straining the world's financial regulatory systems,' OECD, 2009.

6. Muthiora B, *Enabling Mobile Money Policies in Kenya: Fostering a Digital Financial Revolution, GSMA Mobile Mooney for the Unbanked*, Bill & Belinda Gates Foundation 2015.

7. Koker L and Jentzsch N, 'Financial Inclusion and Financial Integrity: Aligned Incentives?' Proceedings of the 2011 Shadow conference, Munster, Germany, 28-31 July 2011.

8. Malala J, 'Consumer Protection for Mobile Payments in Kenya: An Examination of the Fragmented Legislation and the Complexities it Presents for Mobile Payments' Kenya Bankers Association, KBA Centre for Research on Financial Markets and Policy Working Paper Series WPS/02/14, 2013.

9. Ghana Banking Survey: How to Win in an Era of Mobile Money, A 2016 report by PwC on Ghana's Banking Industry.