CYBER-SECURITY: AN ANALYSIS OF THE RISK PLACED ON THE RIGHT TO PRIVACY BY TECHNOLOGICAL INNOVATION.

Mwerebi Sean Kabuthi

92885

Proposal submitted in partial fulfillment of the requirements of the Bachelor of Law Degree, Strathmore University Law School

Strathmore Law School

Strathmore University

Nairobi, Kenya

January 2020

DECLARATION

I declare that this study has not been previously submitted and approved for the award of a Bachelor of Laws degree to this or any other university. I believe to the best of my knowledge that this dissertation contains no material previously published by any other person.

SEAN MWEREBI

……..

Approval

The thesis of SEAN MWEREBI was reviewed and approved by my supervisor;

Mr. Claude Kamau

Assistant Lecturer, Strathmore Law School

Strathmore University.

……

Abstract

The internet has become the primary source of information access and communication in most if not all the countries in the world. It has made the world into a global village that has eased communication from different locations on earth and made it seem as if everyone is connected. It has indeed made the world evolve into a dimension very few envisioned. However, with this evolution comes a risk to the basic and fundamental human rights that have been developed overtime to protect human beings. The vast number of constitutions in the world provide for different yet very similar fundamental rights and freedoms that ensure human beings are protected. Amongst these many fundamental rights is the right to privacy which for a long time has been regarded to as a fundamental human right however, the development of technology and the internet is having a negative impact on said right. Data mining is amongst the many technological innovations that pose such a threat to the right to an individual's privacy. Data mining applications involve vast amounts of data, which are likely to have originated from diverse, possibly external, sources. Thus the quality of the data cannot be assured. Moreover, although data pre-processing is undertaken before the execution of a mining application to improve data quality, people conduct transactions in an unpredictable manner, which can cause personal data to expire rapidly. When mining is executed over expired data inaccurate patterns are more likely to be revealed. Data mining by governments and private institutions can result in inaccurate representation of an individual due to inaccurate data consolidation. Data mining for a fact is generally a useful resource as it assist in following up on issues such as tax evasion and terrorism probabilities however the collection of personal data from an individual without the individual's knowledge on such collection may result in inaccurate data projection which may be harmful to an individual.

This research seeks to analyze this risk and how it has come about and consequently find a solution to ensure privacy rights are protected in the online atmosphere as much as they are in the real world. The research also seeks to analyze policies put into place by North America and different common law countries such as the United Kingdom in comparison with Kenya and how they regulate the internet to ensure that data protection is maintained. This analysis will hopefully result in recommendations for the establishment of laws and policies to ensure Kenyan citizens enjoy a safe space when they use the internet for their personal and or work-related matters.

TABLE OF CONTENTS

LIST OF STATUTES

1. *Constitution of Kenya (2010)*
2. *Universal Declaration of Human Rights*
3. *Data Protection Act (2018)*
4. *General Data Protection Regulation (EU) (2016)*

LIST OF CASES

1. *Roberson v. Rochester Folding Box Co. (1902)*
2. *Pavisch v. New England Life Insurance Company (1905)*
3. *Munden v. Harris, 153 Mo.App. 652, 134 S.W. 1076 (1911)*
4. *Gibblett v. Read (1743)*
5. *American Civil Liberties Union et al v. Clapper et al (2015*

LIST OF ABBREVIATIONS

1. UDHR – Universal Declaration of Human Rights
2. KDD- Knowledge discovery from Data
3. HEW- Health Education & Welfare Department
4. FCRA- Fair Credit Reporting Association
5. GDPR- General Data Protection Regulations

ACKNOWLEDGEMENTS

I would like to acknowledge and thank the following important people who have supported me, not only during the course of this research project but thoughout my LLB degree.

First, I would like to express gratitutde to my supervisor Claude Kamau for his unwavering support, guidance and overwhelming insight thoughout this research project. His assistance, guidance and patience the process of writing of this disertation has been instumental for the completion of this work.

Second, I would want to express my gratitude to both my parents and brother; Gideon Mwerebi Kabuthi, Sarah Kinyanjui Mwerebi and Eddie Kinyanjui respectively for providing me with the financial support and emotional support that ensured I overcame all challenges that came my way during the four years in university.

Lastly, I would like to express my gratitude to both the Strathmore law School for providing me with the space and expertise necessary for me to pursue a degree in law and the Strathmore University fratanity as a whole for giving me a chance to pursue my dreams through the University. I am forever grateful.

CHAPTER ONE

1.1 Introduction to the Study

Fundamental rights are natural obligations that are *erga omnes* (towards all or everyone). They are inherent and precede the State, which is formed by the political society for the protection of such rights.[1] The 2010 Constitution has provided Kenyans with fundamental rights and freedoms to ensure their rights as human beings are protected. The rights ideally embody what a free democracy ought to reflect, allowing people to live their lives as they deem fit and express themselves according to their principles and values as long as their achievement of such rights are not repugnant to the spirit of the constitution. Specifically focusing on one right in this study, the right to privacy has ensured people all over the world enjoy their lives without the interference of others and to some extent without the interference of the government. Many scholars insist that encompassed in the right to privacy is the "right to be left alone", which broadly gives a definition to the right to privacy. Over the years as the world has evolved to what it is today, the scope what is entailed by privacy and the right thereof has changed and broadened significantly due to the advancement of technology and the internet. From child rearing, family life and procreation in the first half of the 20th century, to contraception in the 1960s, abortion in the 1970s and homosexuality in the 1980s[2]. The increase in liberties and the ability to make independent private decisions concerning such matters has increased the scope of what in entailed by the right to privacy and consequently this evolution has not clearly marked the outer limits of the right to privacy.

Adam C. Breckenridge explains that, privacy is the rightful claim of an individual to determine the extent to which to share of himself with others and his control over the time, place and circumstances to communicate to others.[3] Black's Law Dictionary defines privacy to mean the right that determines the nonintervention of secret surveillance and the protection of an individual's information.[4] Privacy from different scholars and academics can have different meaning as it has in different sets of laws. In Kenya, privacy has been encompassed in the Act of rights set out in the 2010 Constitution. The 2010 Constitution in article 31 states that:

---

[1] Franchesci L, Lumumba P, *The Constitution of Kenya, 2010, an introductory Commentary*, 143.
[2] Glenn A, *The Right to Privacy: Rights and Liberties under the Law*, 45.
[3] Breckenridge A, '*The Right to Privacy*,' 1.
[4] Black's Law Dictionary, 3 ed.

Every person has the right to privacy, which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed or the privacy of their communication infringed.[5]

This right is also recognized in the UDHR under article 12 as:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation[6].

The same is reflected in the ICCPR and in other international treaties. This right is directly connected to other rights and freedoms such as human dignity, freedom of association and freedom of speech.[7] The right to privacy may be given different definitions by different authors and scholars however, what people call private is not as such universal but has been shaped by the realities of particular historical periods.[8] Depending on the day, age, culture, period or location privacy may be phrased differently and understood differently. Here in Kenya privacy as seen above is a fundamental right in which every citizen should be enjoying courtesy of them being a citizen of Kenya however, as per now the only form of legislation Kenya has is a Data Protection Act which has been in parliament since 2015. Privacy does not necessarily have to be only about history and protecting what we know and understand should be 'private' to us, it should have a normative form to assist in forming laws and policy that gears the society into the future and not only protect what is gone. If we focus simply on people's current expectations of privacy, our conception of privacy would continually shrink given the increasing data collection and processing in the 21st Century. Similarly, the government could gradually condition people to accept wiretapping or other privacy incursions, thus altering society's expectations of privacy." On the other hand, if we merely seek to preserve those activities and matters that have historically been considered private, then we fail to adapt to the changing realities of the modem world.[9]

"While we may long regard certain matters as "private," what it currently means to call them "private" differs from what was meant in other times during history."[10] This is the reason privacy

[5] Article 31(1), Constitution of Kenya (2010).
[6] Article 12, Universal Declaration of Human Rights.
[7] Mbondenyi M & Ambani J, *The New Constitutional Law of Kenya; Principles, Government & Human Rights*, 15.
[8] Solove D, *Conceptualizing Privacy*, 1140.
[9] Solove D, *Conceptualizing Privacy*, 1141.
[10] Solove D, *Conceptualizing Privacy*, 1142.

legislation and prioritization ought to take form in Kenya. In this new millennium; inventions such as mobile phones, cameras, and even mobile phones with cameras, it is very difficult to ensure ones' right to privacy is not infringed and more so as a public figure in society. This has made it slightly difficult for the spirit of the constitution to be upheld.

The internet has changed how rights in the 21st century are protected due to the developments it has brought. This study is meant to analyze the risk it has brought in fulfilling the right to privacy, specifically data protection by analyzing existing law. In relatively rapid succession, cable technology, the Internet and mobile phones have increased the scope of the definitions of privacy rights. In the late 20th century as individuals and governments can now access private information with the click of a button or by making a simple call to the right source of information. We are now witnessing a convergence between multiple theories of media, telecommunications and digital information society.[11] These new technologies have broadened the scope of the right to privacy to include areas which people had not anticipated such surveillance and data protection which is the main study and analysis of this study.

1.2. Statement of the Problem

The Data Protection Act is the relevant legislation drafted by parliament to address the matter of privacy, specifically data protection. It was recently consented to by the president after a long nine years in parliament. Other than giving effect of the provisions of article 31 (c) and (d) full effect the purpose and object of this Act is to: regulate the processing of personal data; ensure handling of personal data of a data subject is guided by the principles of: lawful processing; minimization of collection; restriction to further processing; data quality; and security safeguards; establish the legal and institutional mechanism to protect personal data and to provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the act.[12] The Data Protection Act will try to ensure the right to privacy of Kenyan citizens on the internet is not infringed upon by individuals with malicious intentions and more so the government.

[11] Benedek W, Rao M, *Human Rights and Information and Communication Technology*, 57.
[12] Section (b), (c), (d), (e), Data Protection Act, (Act No.24 of 2019).

The Act has come up with laws meant to ensure Kenyan citizens enjoy their right to privacy and that their data, specifically data that is within the sphere of the internet is safe and is not accessed by unauthorized individuals. Section 40 of the Data Protection Act addresses who can process data and information concerning a subject's sensitive personal data. In the Act, sensitive personal data is defined as *data revealing the natural person's race, health status, ethnic social origin, political opinion, belief, personal preferences, location, genetic data, biometrics, sex life or sexual orientation, personal financial expenditures, of the data subject*[13]. In reference to this definition; section 40 legally gives this data processing privilege to foundations, association or any other not-for-profit body with a political, philosophical, and religious or trade union aim to collect such data for use within their organizations. [14] This section specifying the bodies with such legal capability does not reflect the reality of data mining in the Kenyan cyberspace. The section blatantly ignores the existence of body corporates such as Facebook and Cambridge Analytica collecting "big data" and selling it to other companies and the government for the sake of data collection and citizen manipulation. There needs to be regulation other than the little information provide by section 33 on already existing body corporates and not just a mention of the bodies and organizations that ought to be carrying out such activities, especially when such body corporates are dealing with the government. When personal data has been collected it is generally decontextualized and separated from the individual, improving privacy but making misuse and mistakes more likely. Accuracy and the lack thereof is a huge concern when data mining is involved as there is the risk individuals face as a result of inaccurate information collected about themselves. Inaccurate information might result in situations that individuals reputation which they have taken a lifetime to build and mold are spoilt just because of the information collected about them is not accurate. An example would be if a mining exercise erroneously declares an individual a poor credit risk, and decisions may be made prejudicial to that individual on that basis. Such a situation poses a risk to an individual's livelihood. Why hasn't the government mentioned anything on body corporates taking part in data mining and there being any plans to stop or at least regulate the practice in order to perceive its citizens dignity, or is it because the government wants to have such information concerning its citizens?

[13] Section 2, Data Protection Act, (Act No.24 of 2019).
[14] Section 40, Data Protection Act (Act No.24 of 2019)

In reference to the topic of big data and data mining activities and resources, the data protection Act only deals with data mining in section 33 which explains that (a) personal information on a data subject shall not be provided to a third party for the purposes of processing for direct marketing without the data subject's consent.[15] Section (b) continues to say that said data subject is at will to object to the use of his or her information by the third party. This minimal reference to data mining in a whole data protection law that is supposed to be enacted to ensure citizens enjoy surfing the internet without their sensitive information being accessed by corporations with improper intent is just but insufficient.

1.3. Statement of Objectives

This paper seeks to meet the following objectives;

1. To ensure the concept of privacy in the right to privacy is properly understood by a reader in order for an individual to think subjectively towards legislation and regulation of data mining is tackled in a proper manner.
2. To analyze the existing laws and the existing legal regime governing data mining ensure that they are sufficient enough to properly regulate and prevent the infringement of the right to privacy though data mining
3. To successfully offer a conclusive report on the legal regime governing data protection in Kenya and if possible suggest recommendations that may assist the formulation and inclusion of laws that will protect citizens' data and personal information from being preyed upon.

1.4. Justification of the Study

Users of the internet and technology will be the beneficiaries of this paper as they are the targeted people whose right to privacy is at risk.

This study seeks to understand the reason the Kenya government and Kenyan laws do not reflect and or echoes the need for data protection through the right to privacy both of which are mandated

[15] Section 33 (1) Data Protection Act, states that a data controller or data processor shall not provide, use, obtain, procure personal data of data subject for the purpose of direct marketing without prior consent of the data subject.

for and included respectively in the constitution. This has been done through the absence of sufficient and enough legislation put in place by law makers regulating data collection through data mining by big corporations and by the government itself for their own use for example marketing purposes or to influence the outcome of an election. Does the government and big corporations illegally benefit from data mining and if not why hasn't proper legislation been enacted to ensure citizens' data is secure and their right to privacy is protected? This question satisfies the need for such a research to be carried out in order to fix the problem that has been created by human beings as they pursue their wellbeing and common good.

This study may also serve as sufficient proof to alter and or improve the phrasing of local laws, international laws and treaties that are meant to ensure the right to privacy is protected to accommodate the changing times and the presence of technology such as the internet used to collect information through data mining. The pace of change in information and internet technology, services and markets is much faster than normal patterns of change in human behavior, to solve this menace of a problem we may need to at least increase the detail further the scope the right to privacy should entail.[16]

1.5. Research Questions

a) Is conceptualization of the right to privacy as referred to in article 31 of the 2010 Constitution of Kenya in reference to the Data Protection Act adequate?
b) Is the existing regime as it currently is sufficient enough in dealing with the upcoming trend of data mining by corporations and governments
c) Would the review of existing regime and legislation on privacy lead to protection of Kenyan citizens from the privacy risks posed by data mining?

1.6. Research Hypothesis

Considering the above research questions, the hypothesis of the study will be as followed;

[16] Benedek W, Kettemann M, *Freedom of expression and the Internet*, 24

i. The right to privacy should be recognized as having different concepts in different circumstances.
ii. Most jurisdictions including Kenya have not evolved with time resulting in the inadequacy for legal regimes to address data mining properly.
iii. A proper review on legislation on data protection from data mining would ideally improve privacy protection against illegal data mining.

1.7. Conceptual Framework

In this study, I will be using a conceptual framework as it will be able to explain how the whole theory of internet freedom and autonomy has come into play in this day and age.

Daniel Solove, one of the major scholars on privacy came up with a way of understanding the term privacy in order to reduce the confusion experienced by legal regimes in the area. Solove contends that privacy is better understood as drawing from a common pool of similar characteristics. Rather than search for an overarching concept, Solove advances a pragmatic approach to conceptualizing privacy. According to his work, the most prevalent problem with the conceptions of privacy provided by privacy scholars is that they are either too narrow or too broad. The conceptions are often too narrow because they fail to include the aspects of life that we typically view as private, and are often too broad because they fail to exclude matters that we do not deem private. Often, the same conceptions can suffer from being both too narrow and too broad. He contends that these problems stem from the way that the discourse goes about the task of conceptualizing privacy.[17] He explains two existing methods used to conceptualize privacy; the traditional method and the Wittgensteinian Family Resemblances method. The "traditional method," of conceptualizing privacy is understood as an attempt to articulate what separates privacy from other things, what makes it special, and what identifies it in its various manifestations and is the conception of privacy Solove says most theorists use. The this method endeavors to conceptualize privacy by constructing a category that is separate from other conceptual categories (such as autonomy,

[17] Daniel Solove, "Conceptualizing Privacy" 1095

freedom, and so on) and that has fixed clear boundaries so we can know when things fall within the category or outside of it.[18] The Wittgensteinian family resemblances method which states that certain concepts might not have a single common characteristic; rather they draw from a common pool of similar elements.[19] Solove draws his approach from the family resemblances which directs the theorists, policy makers and academics to look to the circumstances. Shifting the focus away from finding a common denominator may prove immensely fruitful. The top-down approach of beginning with an overarching conception of privacy designed to apply in all contexts often results in a conception that does not fit well when applied to the multitude of situations and problems involving privacy.

Solove then has his own method which he calls a pragmatic approach which he conceptualizes privacy by seeking to understand privacy in terms of practices and by practices he means traditions, norms and customs. These practices are a product of history and culture and therefore people should consider things to be private or rather conceptualize private matters and activities by looking at certain matters in history long understood as private such as the family, the body, and the home. Stanley Cavell noted that "a new application of a word or concept will still have to be made out, in the particular case, and then the explanations themselves will be sufficient,"[20] and likewise to that Solove's pragmatic conception follows a similar precedent by not focusing on universal application but on specific situations.[21] Solove insists that his conception of privacy (the pragmatic approach) requires a recognition of context and contingency, more of a rejection of knowledge garnered from customs, and a focus on concrete practices that may be occurring in at the specific moment in time. This is where the conception of privacy in the Kenyan legal regime has been lacking prior the formulation of the Data Protection Act. The focus on the universal application of privacy has been done in Kenya for a long time results in the lack of diversification of privacy laws into different areas i.e. the internet consequently leading to insufficient laws on the matter. Likewise goes to different areas in data protection as it is. There are many ways privacy can be infringed upon despite the presence of the Act i.e. through the collection of personal data for financial benefit (data mining). Solove suggested that we should act as map makers and map out the terrain of privacy by examining particular problematic situations rather than trying to fit

[18] Daniel Solove, "Conceptualizing Privacy" 1096
[19] Daniel Solove, "Conceptualizing Privacy" 1126.
[20] Stanley Cavell, Excursus on Wittgenstein's Vision of Language, in THE NEW WITTGENSTEIN
[21] Daniel Solove, "Conceptualizing Privacy."1126.

each situation into a firm predefined categorization.[22] In a Kenya, the right to privacy is used mostly in terms of unnecessary and unwarranted intrusion into people's space. This however has brought up the problematic issue of not considering and understanding privacy in other area i.e. the internet. Understanding privacy in this singular manner results in the lack thereof of proper laws to encompass the entirety of privacy as it is meant to be in this day and age. Privacy in Kenya has in the past been about respecting individuals' space, property and or family matter however if Solove's theory is to be put in context; each situation is deserving of its own understanding of the term in order to ensure the right is protected. Solove's pragmatic approach would ensure that privacy as a right in Kenya is accorded the required scope of expansion to enable the legislature to make relevant laws depending on upcoming and developing problems as the country moves forward. If otherwise not considered in this manner it results in the situation Kenya together with many African countries have had in the past; a lack of sufficient privacy laws addressing most if not all aspects of the term. Knowledge originates through experience is what pragmatists say and the experience of technological advancement requires a broader view on the already established laws in order to avoid inadequacy in legislation. A pragmatic approach to the task of conceptualizing privacy should not, therefore, begin by seeking to shed light on an abstract conception of privacy, but should focus instead on understanding privacy in specific contextual situations[23] such as privacy in the internet. These conceptions of privacy especially Daniel Solove's pragmatic approach is the backbone that holds this study as without a framework of how privacy should be viewed in the world as it is, there definitely would be the idea whatsoever to include privacy on the internet as a category of required privacy. As time progressed and as privacy rights developed the internet came into play bring a whole new dynamic that required understanding. Privacy being understood in the light of circumstances has come to all the evolution and advancement of the term in the 21st Century so as to deal with right infringement in the internet and for purposes of this study, where data mining is involved. Otherwise if this not the case data mining as an activity would be going unchecked without any privacy regulation.

[22] Daniel Solove, "Conceptualizing Privacy."1126.
[23] Solove D. 'Conceptualizing Privacy,' 1128.

1.8. Literature Review

The upheaval in technological advancements has changed society in a general sense and will continue to do so in the foreseeable future. Numerous undertakings have gotten simpler to deal with. Where originally only a few parts of society had supported their working methods with the assistance of technology, presently scarcely any area in the general public has stayed unaffected. Information technology has in one way or the other swarmed pretty much every part of human activities.[24] As technology advances with time, different aspects in life unfold due to these developments leading to the need for a broader and more inclusive right regime in order to prevent the infringement of existing rights and fundamental freedoms. This study is exclusively dealing with the risk posed by technological development on the right to privacy when data mining resources and techniques are used by public and or private entities.

Defining Privacy

Through the years there have been numerous scholars, theorists and academics who have tried their best to define and have an understanding of the concept of privacy. Without properly understanding the term, it is highly unlikely that a law making body would properly be able to establish rules to preserve the right and consequently make regulation of data protection on the internet.

Data Mining as a Legal Risk

Data Mining is an activity that in the current world is gaining a lot of fruition for big corporations and some governments that have invested in the resources.

Kirsten Wahlstrom, explains clearly that data mining ideally is not a problematic activity and is not an unethical activity. This however is dependent on the type of information that is being collected and the purpose it is being collected for. He explains that as because of the development in computing power and storage capacity; organizations are now able to develop data-rich information systems as part of their core business in order to observe the trends within the organization and foretell the needs of the business. This shows the potential data mining has to improve a company's standing in a field. Despite this, he also includes the fact that ethical dilemmas arise when data mining is executed over data of a personal nature. Wahlstrom

[24] Wanjiru R, 'Data Protection and Cyber Crime in Kenya' Published LLB Thesis, Catholic University, Nairobi, 21.

discusses why data mining might cause problems to the right to privacy using three conclusions. The first is that it is impossible to explain the purpose of data mining activities as necessary information is extracted as information is being collected. Second is that data mining is conventionally executed over large amounts of historical data and thus uses data collected for one purpose for another purpose. Lastly, data mining results in the revelation of information that is considered inappropriate by the data subjects of said information. These violations diminish the individual's capacity to determine which, and how much, personal information is known about them, and thus threatens to violate their sense of privacy.[25]

Melanie Rosnay argues in her journal that *Big Data* (extremely large sets of data collected for analysis to reveal patterns and or trends of an individual) provides a huge risk to the world as it is now.[26] She comments that some of the risks of data sharing have been addressed by different legislation however, states that there is a huge challenge when it personal and confidential information that individuals do not what to be exposed into the public domain. Legal solutions to preserve personal rights against the collection and processing of their own data could be the extension of moral rights of personality and destination. She states that a method that could help ensure personal rights are preserved against data mining could be the extension of moral rights of personality and destination towards the control of one's own information. This can be done through creation of a copy-left license towards ones' own personal data.[27]

In light of all the invasion of privacy that is going on by the use of data mining processes by state and non-state actors, CXOtoday News Desk reported the Supreme Court of India concluded some years ago that privacy even though it is not absolute it is a fundamental human right. The apex court did not hide its concerns on data handling while dealing with the topic of privacy and argued for striking a balance between data regulation and individual privacy as it raises complex issues requiring delicate balance between the legitimate concerns of the state and individual interest in the protection of privacy.[28] The judges mentioned that other both non-state and state

[25] Wahlstron K, Roddick J, Sarre R, Estivill-Castro V and deVries D '*On the Ethical and Legal Implications of Data Mining*' Febuary 2006, 5.
[26] Rosnay M, 'The legal and policy framework for scientific data sharing, mining and reuse' HAL Archives-Ouvertes, 2007.
[27] Rosnay M 'The legal and policy framework for scientific data sharing, mining and reuse'
[28] https://www.cxotoday.com/story/right-to-privacy-what-it-could-mean-for-big-data-and-protection/ in January 2018

actors may actually be legally allowed to collect data however that does not mean when “one person is allowed into the bedroom of an individual it gives permission to the whole world to enter.” This being said the Supreme Court insisted that there ought to be consent from the owners of said information and other than consent the data mining agencies i.e. the government and data mining companies ought to ensure anonymity from the public with the information collected. This begs the introduction of laws that govern and regulate data mining as it is an activity that is both valuable and dangerous at the same time. The Supreme Court of India gives examples such as medical data collection and national security as perfect examples of good use of data mining however there is a lot of harm such an activity can cause on the privacy of an individual.

1.9. Approach and Methodology

The main method of research that will be used for this research is desk research and the main source of information that will be collected and used to carry this research will be from literature that is available on the topic. Such literature will include books, journals and articles concerning the impact of the internet of the said fundamental rights. The researcher will also use authoritative publications, relevant legislation around the world, principles of common law and case law available on the topic at hand. In addition to written sources the research will also use textbooks and commission reports to research on the topic.

The researcher will use a qualitative method of research in order to come up with an accurate depiction of how to solve the problem posed by the topic. Qualitative research will be used to uncover trends in thought and opinions, and dive deeper into the problem. This is necessary to ensure the researcher get an even deeper understanding on how to solve the problem at stake and come up with viable solutions that will be used for long term purposes and not just for the moment the fundamental right is infringed upon.

1.92. Limitations

The limitations the researcher may experience when carrying out this research have been minimized because most of the research being carried out is on internet users hence research will be carried out online. This does not however mean there are none. Information gathering concerning the topic may be tedious as it is not a topic well vast in African legislation and specifically in Kenya. This however being a limitation will not prevent the proper analysis of the

study as the topic is well vast in other regions of the world, especially in the European Union with much knowledge on the topic at hand.

1.93. Chapter Breakdown

Chapter 1; the objectives of this study are met within six chapters. The current chapter, which is the first, is an introduction and points out the background to the problem, the research problem, the hypothesis, the research questions and methodology that is used by the researcher to carry out the research. This chapter will assist a reader to understand the problem that the researcher seeks to address and his opinion before the research is carried out.

Chapter 2; the second chapter will be on the conceptualization of exactly what privacy is and should be and what is entailed in the right to privacy.

Chapter 3; the third chapter of this study will be on the current existing legal regime in Kenya and whether the laws put in place are sufficient enough to deal with the current trend in technological innovation, specifically data mining occurring in Kenya by corporations and the government,

Chapter 4: the forth chapter of this study will focus on a comparative analysis between the Kenyan legal regime on privacy and the much better established European legal regime on privacy. This will be done in order to compare and contrast the systems so as to build suggestions for more suitable system in Kenya

Chapter 5; the last chapter in this study will seek to analyze whether the review of the existing laws and suggestions to them would be sufficient enough to provide proper privacy protection to Kenyan citizens. It will be by responding to the research questions as the analysis of the findings has been completed. Recommendations will be made by the researcher on how the problem stated by the topic may be solved and also recommend policy changes to the current Kenyan policy to ensure that human rights are protected online as much as they are protected in the real world.

1.94. Duration

This research will be carried out between the periods of August 2019 to November 2019

CHAPTER 2: CONCEPTUALIZATION AND MEANING OF PRIVACY IN THE 21ST CENTURY

2.1. Introduction

This chapter explores the foundations behind the conceptions of the right to privacy and their relevance in the 21st Century as they are to be used in the formulation of the legal regime seeking to protect individuals' fundamental right to privacy in all relevant areas expected. It proceeds to entail why previous conceptions by different scholars are important to the data protection rights of people in the 21st Century.

2.2. Chaos in the Realm of Privacy

The reality of the presence of a debate on the accurate extent of the meaning of "privacy" shows in a lighting up way the controversy that has been accompanied with the arrangement of protection approaches across the world. Strategies are planned as per the substance of the ideas being referred to, along these lines, challenges in characterizing them has evident repercussions on the aims of the laws or policies that every legislator shapes. Political, social and economic changes involve the acknowledgement of new rights, even customary law in its everlasting youth, develops to satisfy the needs of society. Gradually as time has come to pass and legal regimes across the world develop to meet the needs of the society, rights have grown to increase their scope from not only a tangible state but to what is intangible also (essentially). The reference herein is to elaborate the advancement of the scope of laws as time advances. The right of life for instance has come to mean the right to enjoy life, the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession-intangible, as well as tangible.[29] Just as the right to life has grown from the protection against actual injury to the prohibition of mere attempts to do such injury, the legal conception of privacy should also broaden its scope considering times have changed from to a more technological innovative and advanced age.

[29] Brandeis L, "*The Right to Privacy'*, 193.

Time and again philosophers, legal theorists, and jurists have lamented the great difficulty in reaching a satisfying conception of privacy.[30] This is due to the many differences in opinions and theories of ideally what privacy ought to be. Privacy as a term has not been given a proper and or subtle description as many different scholars have many different theories of what exactly privacy actually is and what it entails. Various scholars and theorists having different views have spoken out so as to project their theory of the ideal meaning the term should have. Robert Post stated that privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that he sometimes despaired whether it can be usefully addressed at all.[31] According to Julie Inness, the legal and philosophical discourse of privacy is in a state of "chaos"[32] While other scholars who are primarily known for discussing the conceptions of privacy insist that the widespread discontent over conceptualizing privacy persists even though the concern over privacy has escalated into an essential issue for freedom and democracy.[33] This clearly shows that for many scholars, philosophers and or theories across the world settling upon any one of the conceptions would result in either a reductive or an overly broad account of privacy.[34] The lack of clarity of the understanding of privacy by all these legal theorists poses a huge threat to the right itself as factions such as data mining and the threat it poses cannot be addressed without a proper understanding of the right that protects people from such threats.

2.3. Foundations the Conception of the Right to Privacy

There being scholars and philosophers who have found it difficult to define the term privacy does not necessarily mean that the term cannot be defined as there those who have tried.

Daniel Solove approaches privacy from what he referred to as a pragmatic approach as we have seen in the conceptual framework. His theory as it has been explained in this study has affected how privacy is viewed across the world. This has resulted to countries making and forming laws on privacy not using a singular approach but by understanding the problem areas privacy need to be addressed. From the conceptual framework, it can be noted that the approach Solove chooses to take in conceptualizing privacy is one that deals with specific problematic situations that would

[30] Solove D, 'Conceptualizing Privacy'.
[31] Post R, 'Three Concepts of Privacy', Yale Law School Legal Scholarship Repository, Faculty Scholarship Series, 2001. 2092
[32] Inness J, "Privacy, Intimacy, and Isolation' Oxford Scholarship Online, November 2003, https://www.oxfordscholarship.com/view/10.1093/0195104609.001.0001/acprof-9780195104608.
[33] Solove D, 'Conceptualizing Privacy.' 1126.
[34] Solove D, 'Conceptualizing Privacy.' 1126.

occur from privacy (experience) rather than using an abstract assumptions of what privacy may be or what it has been normalized by the world to mean. The approach is more of understanding privacy rather than defining the term. This pragmatic approach is from the analysis the reason the term privacy has expanded its scope as time has moved as the approach dwells on problems as they come and not as they were. The pragmatic approach is an ideal understanding of privacy when dealing with the legal threat of data mining as it is a threat that has occurred as a result of technological innovation. Solove's understanding of privacy includes data protection specifically the protection of privacy rights at risk when data mining is used as a resource.

Another privacy scholar Robert Post suggests that privacy prevents the disclosure of the kind of information that cannot be adequately understood in the absence of special circumstances, like intimacy.[35] This is a theory that is very similar to Solove's as Robert insists that information that is let out into the public by someone (involved or otherwise) might be misunderstood by said public because they are not in that specific situation. Just as Solove does. Robert reiterates the importance of relating privacy to specific situations in order to achieve a proper solution depending on the problem that has arisen. Data mining being an IT related issue cannot definitely be controlled by privacy laws relating to property and or family however, if privacy laws relating to the specific field and area are to be developed, there is a high likelihood that adequate laws would come up to control and or regulate the problem at hand. The lack of proper understanding to what exactly the term privacy refers to in a specific area could be dangerous as it would result in legislation and or regulation that does not properly address the problem.

Another conception of privacy would be that of William Beaney. William Beaney the scholar who previously said mentioned that "even the most strenuous advocate of a right to privacy must confess that there are serious problems of defining the essence and scope of this right,"[36] says that the right to privacy as a legal concept can be defined as the legally recognized freedom or power of an individual (group, association, class) to determine the extent to which another individual (group, class, association, or government) may (a) obtain or make use of his ideas, writings, name, likeness, or other indicia of identity, or (b) obtain or reveal information about him or those for

[35] Post R, 'Three Concepts of Privacy,' 2085.
[36] Beaney W, 'The Right to Privacy and American', Duke Law Scholarship Repository, 31, 1966, 253-271.

whom he is personally responsible, or (c) intrude physically or in more subtle ways into his life space and his chosen activities.[37] Ideally this shows that the lack of clarity in the conception of privacy is just but a momentarily predicament, however, so is all sorts of definitions. He tries to ensure no "individual" is left out from his conception of privacy. In furtherance to his conception he established that the earliest mention and or recognition of the right to privacy was from Samuel D. Warren's and Louis D. Brandeis' famous article "The Right to Privacy" which from written history is what is recorded in the United States as the onset of privacy. The duo invoked in their works that it is our purpose as human beings to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is,

2.4. Importance of Previous Conceptions of Privacy.

There are many conceptions of the term privacy from many different scholars and different writers. Despite there being a very in depth debate or clear confusion from the different perceptions on what many of them deem what privacy is, their conceptions and theories cannot be taken for granted as they have gradually helped to establish the wide and ever growing conception of what privacy can and could be. After the appearance of computers in the 70s, it was questioned whether the right to privacy is capable of ensuring the protection of private life, and this technological change led to the appearance of a separate right whose subject is also the protection of private life: the right to data protection.[38] Economic development, which came along with technological advances, brought threats to individual privacy that is now seen from a different perspective as people poured into the cities creating a new model of urban life that created a novel need of citizens for some private space. As seen from previous revelation in the above text, this technological innovation that has led to various privacy infringement mechanisms such as surveillance, wire-tapping and recently data mining. The previous conceptions of privacy through the years have made it clear that privacy can be viewed in many different angles and has many different concepts. This plurality in privacy conceptions has allowed what the term currently entails in the 21st century to include data protection due to the introduction of the internet. If the understanding of the term was restricted upon one specific conception there would be a huge gap in what is required to be

[37] Beaney W, 'The Right to Privacy and American' 253-271.
[38] Lukács A, 'What is Privacy? The History and Definition of Privacy.'

protected; bigger than the future beholds as protection would not be provided to scenarios and or activities happening in the current time.

The absence of the different conceptions would also result in the backlog of important laws that are required to protect sensitive personal information from being acquired and used by unauthorized individuals for their selfish gains. Ideally human being should not allow the possibility of having technology that is capable of infringing upon any fundamental right and or freedom to exist without having laws and or regulations that govern such scientific creations. This was one of the greatest contribution of Brandeis in his famous Olmstead dissent" which drew the distinction between the interest to be protected and particular forms of invasion of that interest. In his view, the devising and ingenuity of man in substituting new scientific techniques for the older, heavy-handed secret observation of the thoughts, words, and acts of others should not be allowed to succeed in out-flanking the law.[39]

[39] The essence of Brandeis's position is that provisions protecting individual and group rights should be interpreted in the light of changing conditions just as provisions granting power are interpreted to reflect social and economic changes. Justice Black in Griswold asserts that government can do anything not prohibited by a specific provision. 381 U.S. at 51o. Brandeis would reject that position in favor of one that envisages both restrictions on, and powers of, government as subject to continued re-interpretation and changing application

CHAPTER THREE: DATA PROTECTION PRINCIPLES, DATA MINING AND ITS EFFICIENCY

3.1. Introduction

Understanding privacy in data protection from a data mining perspective requires understanding how privacy can be violated and the possible means for preventing privacy violation.[40] For a proper understanding of what data mining is, there needs to be a discussion on privacy as it is the fundamental right this study is trying to preserve. As understood before, every human being has a right to privacy in line with the UDHR article 12, however, with the on-set of technological innovation, a lot has come to be questioned on what exactly is entailed by the right to privacy. For this exact reason, states around the world have included in their legislation, policies on data protection because of the risk posed by technological innovation. Infringement of privacy rights as a result of technological advancement can result from many activities such as surveillance, wiretapping etc. This study will primarily deal with data mining as a legal threat and how it has been addressed in the Kenyan legal regime, whether there is need to address it and consequently will try to make proper recommendations to ensure the activity is addressed and that legislation does not remain silent on it resulting in future misgivings.

3.2. What is Data Mining

The term "data mining" is often treated as a synonym for another term ``knowledge discovery from data" (KDD) which highlights the goal of the mining process.[41] As a definition though data mining refers to the process of discovering interesting patterns and knowledge from large amounts of data collected over the internet. The huge measure of data made each second by the 'technological augmentations' of people, has before long demonstrated to be a gold mine for a determinedly developing field of public and private enterprise.[42] This large database of data being uploaded onto the internet is a source of information required by both public and private institutions so as to analyze future developments in their fields. The combination of different datasets through mining techniques makes it possible to extract from the analyzed datasets hidden in-formation as well as productive correlations[43] for the benefit of those interested i.e. corporations, governments even

[40] Oliveira M, Zaïane O, "Toward Standardization in Privacy-Preserving Data Mining"
[41] Tarique M, Saleem M, Kankale A, 'Privacy Preserving and Data Mining In Big Data'
[42] Pasquale M, 'The Black Box Society- The Secret Algorithms that Control Money and Information'Cambridge: Harvard University Press, 2015.
[43] McKinsey Global Institute, "Big Data: The Next Frontier for Innovation, Competition and Productivity"

individuals in some cases. The very component of data mining techniques lies in their ability to "identify invisible patterns and fine-drawn relationships in data, and to infer an analysis that allows for the prediction of future results.[44]

Among the many uses of data mining include fraud detection, financial banking, corporate surveillance, research analysis and criminal investigations. Despite there being many uses presented by data mining, there are concerns about the risk it poses to the right to privacy. The more and more information is available and easily accessible in electronic forms present on the internet and as increasingly powerful data mining tools are developed and used in the data mining process; a threat to user privacy and data security emerges.[45] This concern is specifically directed to the access of personal information that is not meant to be accessed by unauthorized personnel for example health record, financial records, legal issue records etc.

The legal regime in Kenya as said before does not have a lot of history into data protection as it is just but a recent development in the country's infrastructure. The Data Protection Act has information and laws in it that deal with data protection and from a long shot also deals with data mining, however, the legislation is not efficient as the Kenyan government does not address the threat posed by data mining adequately despite the recent passing of the Act, Kenya's right to privacy and their data security may still be at risk. There are certain principles that the Data Protection Act ought to follow in order to ensure that personal information of citizens is not accessed without the necessary authorization for the benefit of business corporations and other institutions.

3.3. The Data Protection Act and Its Inadequacy

Data mining itself isn't morally hazardous. The moral and lawful predicaments emerge when mining is executed over information of an individual sort. Privacy protection involves singular observation, a reliable and all-inclusive answer for this dichotomy is infeasible. In any case, there are measures that can be embraced to upgrade data protection.[46] Normally, an individual must have a proactive and self-assured disposition all together to maintain their privacy, ordinarily starting correspondence with the holders of their information to apply any limitations they think about

[44] T. Zarsky, "Mine your own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion', Yale Journal of Law and Technology 5(2) (2003) 2, 6-7.
[45] IJESMT Journal,"Information Privacy & Security in Data Mining"
[46] Wahlstrom K, Roddick J & Sarre R '*Legal and Technical Issues of Privacy Preservation in Data Mining*'.

proper. Generally, people are ignorant of the extent of the personal data put away by governments and private entities. It is only when things turn out hazardous that people practice their privileges to access this data and right it.

Data mining can result in a great number of privacy violations in which internet users may find to be an intrusion of their fundamental right. The access of personal information such as health records, bank information and even online searches for the purposes of marketing and predicting individual patterns and trends may seem as a violation to many if not all people within a specific jurisdictional sphere of influence. This was seen in Europe in 2014 where more than 90 percent of Europeans advocated for the development data protection rights across the EU.[47] Such a survey shows that there is a common need for data protection and security of people's personal information across the European Union. This observation ought to be extended to the whole would as the unauthorized access of individuals' personal information is an infringement of their right to privacy protected in article 12 of the Universal Declaration of Human Rights.

Kenya as is, has had the legislature go through the law making process and develop a statute that ought to try and hopefully succeed to ensure that privacy online is protected as much as it is protected in reality. The legislature came up with the Data Protection Act a while ago when the need to protect its citizens as they access the internet came up. This was the time internet coverage in the country became widespread. The Act is supposed to ensure personal information is secured and unauthorized individuals do not manipulate said information to the detriment pf the data subject.[48].

Data mining as described in this study is the collection of information of individuals on the internet with the intention of predicting future trends, patterns and or behavior for the benefit and or use of the data collecting entity. Many institutions including companies and governments use data mining as a resource so as to gain an advantage for purposes of future planning, an example would be companies using data mining as a resource to try and market their products to their consumers. Using previous searches and or internet access, data mining resources can be uses to predict future behavior and or habits such as; the type of products an individual is interested in. Even though

[47] See European Commission, 'Reform of EU data protection rules,' at http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[48] According to the Data Protection Act, Section 2 the term in reference to data protection "Data Subject" refers to an identified or identifiable natural person who is the subject of personal data

ideally it would be beneficial to a consumer to have access to products he or she would be interested in, companies many times do not have the permission of the data subject to have this information creating a risk of privacy invasion.

The fact that the Data Protection Act has not expressly mentioned data mining raises questions as to the adequacy of the law and the plans the government has to ensure personal information is protected from unauthorized access by corporations and commercial enterprises. Notwithstanding the lack of mention, the law does touch on data mining in section 33. Section 33 of the data protection Act explores the aspect of collection and processing of data for direct marketing.[49] This indirectly refers to data mining from the many descriptions and definitions of data mining in existence. Section 33 (a) states that personal information on a data subject shall not be provided to a third party for the purposes of processing for direct marketing without the data subject's consent.[50] Section (b) continues to say that said data subject is at will to object to the use of his or her information by the third party.[51]

Section 33 is the only mention of data mining in the Act which is a disappointment considering the huge risk the activity places on the fundamental right to privacy. Moreover, the section lacks enough depth to ensure data mining if done, does not infringe on people's privacy. The mention of "direct advertising" as the only aspect of data mining shows a complete lack of depth of the Act into ensuring data privacy is achieved successfully. Direct marketing is not the only reason data mining can be used by public and private entities. There are many different uses of data mining which are mentioned in this study. Data mining can be used for; health forecasting for the purposes of medical research and planning and also for credit evaluation and fraud detection by providing meaningful patterns to banks and necessary authorities. These uses ought to have been mentioned in the Act so as to be laws and regulations governing these activities. This is an inadequacy the Act has shown as it does not properly analyze data mining and its different functions in order to properly address the issue of privacy and to ensure its protection. Section 33 should have spoken on data mining as a whole; discussing profiling in detail, sale of personal information to buyers

[49] Section 33 (4) Data Protection Act, defines "direct marketing" as the communication of any advertising or marketing material which is directed to any particular individual.
[50] Section 33 (1) Data Protection Act, states that a data controller or data processor shall not provide, use, obtain, procure personal data of data subject for the purpose of direct marketing without prior consent of the data subject.
[51] Section 33 (2) Data Protection Act, states that a data subject may object to processing of their personal data for such marketing, which includes profiling to the extent related to direct marketing

with interest and even gone ahead to discuss the government's use of data mining and its legality. The fact that the data protection Act has not addressed the various threats data mining would bring about and the risk to the right to privacy raises the question of whether the government benefits from the activity of data mining as a resources. Ideally, that would be the only explanation

CHAPTER FOUR: COMPARATIVE ANALYSIS OF DIFFERENT DATA PROTECTION REGIMES

4.1. Introduction

Despite that the fact that information discovered by data mining can be very valuable to many applications, people have shown increasing concern about the other side of the coin, namely the privacy threats posed by data mining.[52] In many countries across the globe, the enthusiasm towards data protection policies and laws is increasing. This is because increasingly sensitive and personal data is collected by organizations.[53] The rapid adoption of these new technologies used by businesses as well as government agencies played an integral role in sparking fears of deleterious effects. Some of the major potential dangers associated with computerized databases include data errors and surveillance of personal data by commercial entities and state bodies. Both tend to have chilling effects not only on individual privacy, but also personal freedoms. Therefore, it is important for citizens and states to safeguard and manage personal information. Different countries have taken different routes and methods in ensuring that the right to privacy of their citizens are not infringed upon by the lack thereof of data protection laws and policies. However, despite the increased interest in privacy due to evolving times, countries have still chosen to understand privacy differently. The USA for instance understand privacy in a manner that is completely different from that of the member state of the European Union. The United States level of privacy is not as intense as that of the European Union as in the past the country has been victim to terrorist attacks hence the theory of ensuring putting national security first as a priority before discussions of data privacy and security.

Through this study we have seen countries such as the United States, Canada and even Japan being included in the list of countries that have regulation to ensure citizens are protected. Amongst the many countries in the world, some of the countries have already implemented robust data protection laws while some are moving in that direction.[54]This form of advancement is necessary as the risk of unauthorized access to personal data is at a fast rate becoming one of the biggest risks posed by technological innovation as it is today. The importance of data protection is seen with the advancement of laws in the world; an example of this would be the fact that the primary subject

[52] Tarique M, Saleem M,.Kankale P 'Privacy Preserving and Data Mining In Big Data'.
[53] Singh H, 'Data Protection and Privacy Legal-Policy Framework in India: A Comparative Study vis-à-vis China and Australia' 24.
[54] Singh H, 'Data Protection and Privacy Legal-Policy Framework in India' 24.

of discussion in both litigation and legislation in the United States and the European Union for the past four decades has so far remained to be the issue of data protection laws and how to ensure personal data privacy.[55] The serious and acrimonious discussion on data privacy is attributed to the interests of various constituencies, including government agencies, national security services, individuals, law enforcement and commercial entities.[56] This chapter of this study is meant to analyze data protection laws and what impact they have on upholding the right to privacy through data protection in two different countries apart from Kenya. Its objective is to compare and contrast the different legal regimes in order to come up with a conclusive report on how the Kenyan legal framework ought to be structured in order to ensure data mining by different organizations and institutions does not cause an infringement upon the citizens' fundamental right to privacy.

4.2. United States of America

The US data privacy legislation is arguably one of the most incomplete and complex, something that has attracted criticism, especially from countries with comprehensive data protection laws. Such follows the fact that America still lacks a single regulatory authority tasked with the responsibility of overseeing and providing relevant reports on federal data protection law. It means that the power to play an oversight by regulatory authorities at the US federal level depends a great deal on the regulation as well as law in question.[57] With the United States history on surveillance and data collection by the government, it would actually be expected that the laws required to be in place to prevent the infringement of the right to privacy to be rather vague in order to allow the government to have loop holes for its own interests. Primarily, the reason the US government values information and access to data through all forms i.e. surveillance and data mining would be for national security reasons as the country has been at risk of terrorist attacks for well over two decades now. Other than the external threats to the citizens of the nation, the country also has numerous occurrences of internal incidents resulting in the death of its own. An example of such occurrences would be the numerous mass shootings that leave many Americans dead and many more injured. The US government defends its breach of privacy law with the excuse of national security however; does this excuse warrant all forms of privacy breaches citizens in the US experience in their day to day lives?

[55] Elmarado E, 'Data Protection Law in the United States' 2.
[56] Elmarado E, 'Data Protection Law in the United States' 2.
[57] Elmarado E, 'Data Protection Law in the United States' 2.

This being said however, with the rapid development of data processing and communication technologies, the US is no exception when it comes to breach of data privacy, resulting from agencies' interference, cyber-attacks, and electronic surveillance failures. The US is in need of a single comprehensive regulatory entity to actively oversee its data protection law with the sole purpose of meeting the needs of the various stakeholders.[58] Few years down, the first case concerning the right to privacy was tabled in the US court system. *Roberson v. Rochester Folding Box Co.* (1902) tested the right to privacy under common law in the United States. In that case, the New York Court of Appeals refused (with a four to three majority) to acknowledge that at Common Law such a right existed, stating: *that the so-called "right of privacy" has not as yet found an abiding place in our jurisprudence, and, as we view it, the doctrine cannot now be incorporated without doing violence to settled principles of law by which the profession and the public have long been guided.* [59] After a year (1903) the main United States protection laws restricting the unlawful use of individuals' "name and resemblance" were passed in New York, what's more, two years from that point forward, in *Pavisch v. New England Life Ins. Co. (1905),* the Supreme Court of Georgia "unanimously affirmed the existence of the right"[60] Other earlier cases concerning the right included Munden v. Harris (1911)[61] and Kunz v. Allen (1918). From then on this marked the advancement of the right to privacy as a right entitled to US citizens however, most of these cases were tortious claims. First forward years later to the Obama administration, the president ordered the United States security agencies to review their programs. In his public statement he upheld that there is no evidence indicating that US "intelligence community has sought to violate the law." In his public statement he upheld that there is no evidence indicating that US "intelligence community has sought to violate the law." A year after said proclamation in (*American Civil Liberties Union et al v.)* The Court of Appeal held that the bulk collection of telephone metadata by the NSA is unlawful and infringes upon citizens' right to privacy. Over the years, the United States courts have used cases decided to advance the whole idea of the right to privacy and data protection and because the country lacks a comprehensive data privacy legislation, the 4th amendment has become

[58] Elmarado E, 'Data Protection Law in the United States' 2.
[59] Roberson v. Rochester Folding Box Co. (1902).
[60] Pavisch v. New England Life Insurance Company (1905).
[61] Munden v. Harris, 153 Mo.App. 652, 134 S.W. 1076 (1911).

the heart of privacy litigation in the country.[62] This being said, data privacy protection from the wide range of harmful consequences resulting from systems of automated personal data began in 1973 when the country's health, education and welfare department (HEW) first published a distinct report about the computers, their potential dangers, and the rights of individual Americans. The report provided a most efficient time for the advancement and creation of a legal regime to guide data security to ensure people's personal data does not get in the hands of unauthorized entities. The 1970 Fair Credit Reporting (FCRA) is considered the initial legislation in the US to specifically address the dangers and consequences of storing personalized data in computerized databases. Despite being passed a long time ago the FCRA remains a common practice with regard to the US legal regime of data protection. The FCRA has assisted in creating a data protection regime in the United States and it has done this by addressing an individual citizen's interest by providing a great deal of consent to as well as notice of a particular record of personal data. HEW and FCRA function as the foundational documents for US data protection laws as they have successfully formalized and made public the principle that all forms of personal data should remain protected at all cost by default.[63]

The legal regime of the United States shows a similarity to that of Kenya as both countries have not had legislation ensuring data protection for the longest of time.

4.3. **European Union**

For quite some time now, the European Union has had very intense privacy and data protection laws meant to ensure the countries preserve the privacy rights of the citizens within compared to Kenya and the United States. Numerous recommendations, working papers and directives have been passed in regard to data protection and privacy. The matter of consent given by individuals on the collection of personal data being a key issue of discussion. This consequently led to the creation of the General Data Protection Regulation (GDPR) which is meant to improve use security and privacy to ensure that users on the internet have the confidence to use the internet without being at risk of an infringement on their personal information

The GDPR was implemented on the 25th of May 2018 approximately a year after its creation on the 14th of April 2016 and was meant to ensure that data processing by various companies are

[62] Elmarado E, 'Data Protection Law in the United States' 4.
[63] Elmarado E, 'Data Protection Law in the United States' 5.

consented upon by internet users before collected for processing. Ideally it requires data to be processed in a manner that does not unnecessarily expose a user without consent and that the data acquired is processed in a manner that ensures security. The regulation shifts the power balance to consumers on the internet and does not leave them wondering what information big tech-companies such as Google and Facebook know about them. It focuses on ensuring users of the internet know, understand and consent to the data collected about them.[64] Under the regulation users are not to be subjected to pages of fine print they neither understand nor are forced to accept to because the need to access the information that comes thereafter.[65]

The GDPR has put into place regulations to require companies to inform internet users and or consumers of why their data is being collected and if it will be used to make profiles of people's actions and habits for future use[66], which is ideally the essence of data mining as a whole. Moreover, consumers will gain the right to access data companies store about them, the right to correct inaccurate information, and the right to limit the use of decisions made by algorithms, among others.[67] Other than the consent fact that the GDPR requires of companies, it also sets aside principles that ensure the data collected on an individual is not only collected in a lawful manner[68] but also it is used for the necessary means and not more[69], this includes insisting that data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed data collected for processing is not kept for a period longer than is required by the collecting company.[70]

On matters of consent the GDPR exclusively reiterates what many other countries in the world have including Kenya; the fact that all users ought to give their consent to matters of data collection and processing and ought to understand the purpose of such data collection and processing. The GDPR however calls on companies that are collecting data on its users to expressly ensure that if said consent is amongst other matters in a written declaration, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible

[64] Tiku N, '*Europe's New Privacy Law Will Change the Web, and More'* February 2018.
[65] Tiku N, '*Europe's New Privacy Law Will Change the Web, and More'.*
[66] Tiku N, '*Europe's New Privacy Law Will Change the Web, and More'*
[67] Tiku N, '*Europe's New Privacy Law Will Change the Web, and More'*.
[68] Article 5 (1) (a) GDPR (2016).
[69] Article 5 (1) (c) GDPR (2016).
[70] Article 5 (1) (e) GDPR (2016).

and easily accessible form, using clear and plain language.[71] All these restrictions and regulations brought forward to be adopted in EU countries are meant to ensure that companies do not use data mining tools to access personal information of individuals for their monetary use without the proper consent and if consent is provided the right data should be collected and used in a lawful and transparent manner.

The GDPR has already contributed to positive change by tech-giants in their data collection and data handling practices, not only in Europe but across the world as it is rather expensive to have create different systems for different locations as opposed to having one system across the board. In June 2018, Google announced that it would stop mining emails in Gmail to personalize ads and later on in September of the same year revamped its privacy dashboard, first launched in 2009, to be more user-friendly.[72] The GDPR's emphasis on consent, control, and clear explanations could prompt users to better understand and reconsider the ways they are surveilled online which in turn would provide for a much better space for internet users to enjoy their freedom on the internet without their privacy being infringed upon. Most of the data rights enshrined under GDPR were already created in the EU, but went unenforced for an unreasonable amount of time. The GDPR standardizes data rights across all EU countries, empowering regulators with the capability of ensuring internet users are protected against corporates that are out to get them. Violators face fines of up to 4 percent of annual global revenue. For Facebook, that would be $1.6 Action; for Google, $4.4 Action.[73]

[71] Article 7 (2) GDPR (2016).
[72] Tiku N, '*Europe's New Privacy Law Will Change the Web, and More'*.
[73] Tiku N, '*Europe's New Privacy Law Will Change the Web, and More'*.

CHAPTER FIVE: REVIEW AND RECOMMENDATIONS TO THE KENYAN LEGAL FRAMEWORK ON DATA PROTECTION

5.1. Introduction.

This final chapter will reflect on the discussions in the study, outlining the findings in a clear and holistic manner as they have been developed and explained in previous chapters. It will go ahead and suggest some recommendations that the Kenyan legal regime out to take up in order to ensure illegal data mining in the country is controlled enough to ensure the right to privacy as outlined in article 33 of the 2010 constitution is preserved not only in reality but in the online world as well.

5.2. Review

This study has in general investigated the right to privacy in the online world that is the internet and how the inherent right to privacy can be protected online. The study has specifically dealt on the matter of data mining as a risk to the right to privacy as it is an upcoming method and or activity that is used by companies and governments across the world to collect data from internet users.

Chapter one of this study has laid the background of the study by explaining the right to privacy and its importance to the human race, especially in this new digital age that the world is in at the moment. It has explained when and how the right to privacy came about and its relation to other laws around the world. The chapter has also highlighted the reasons the study has been selected by the author as one that ought to be investigated which is; the fact that Kenya for a long time did not have a properly incorporated internet privacy law and when incorporated into the laws of the land the law has some sort of inefficiency that does not properly ensure internet users are protected. The chapter explains all the laws that are in play in the Kenyan legal regime so as to ensure citizens' right to privacy is protected. The chapter established the questions that directed the research, the objectives of the research, reviewed necessary literature on the study and laid out the conceptual framework for that study. This study is meant to answer three research questions that were set out in this chapter. The first question to be answered is whether the conceptualization of the right to privacy as referred to in article 31 of the 2010 Constitution of Kenya is adequate enough to ensure the right is fully protected in the developing world. The second question the study ought to answer is whether the existing regime is sufficient enough to deal with the data mining as a legal thread as it is an upcoming trend of data collection and handling by many corporations and governments.

Lastly, the study is meant consider whether an increment and or review pf existing legislation on data privacy would lead to the protection of Kenyans from the privacy risks posed by data mining.

Chapter two analyzed the meaning of privacy as it is in the current digital age and how it was conceptualized in the past. Privacy being a term in which many scholars and academics have found difficult to give a definite definition, this chapter analyses the reasons behind this difficulty and why said scholars, writers and academics found it difficult to do so. Moreover, chapter two discusses ideally what privacy ought to have been in the past without the technology of the current time we are in and what privacy ought to be now in the digital age, whether the term would be sufficient as it was other whether there is need to broaden the scope of the term in order to incorporate the changes that have come about due to technological advancement as time advances. This was done using information collected from written articles and documents from famous scholars such as Daniel Solove and Brandeis who helped develop the foundations of what privacy should be. The chapter also discusses the importance of the previous conceptions of privacy by different scholars in order to help the reader understand how the many conceptions established in the past have built up to privacy being as it is in the present day. The chapter answered the question of exactly what privacy is by referring to different scholars and legislation across the border. Though it was difficult to give the term privacy an exclusive definition, the finding was that privacy is a broad ever evolving term that encompasses different meanings depending on the context it is being used in.

Chapter three of the study is meant to analyze the efficiency of the current regime in ensuring that data mining as a resource and or activity by companies and the likes do not infringe internet users' right to privacy. The chapter began by expressly explaining to the ready in more detail than done before what exactly data mining is and what it entails. This is to assist the reader to understand how data mining can be classified as a legal threat to internet users' privacy rights. The chapter goes further to highlight legislation put into place by Kenyan law makers in order to ensure data protection in the internet is achieved and in this context data mining is controlled enough to ensure there are no infringement of internet users' privacy rights. The legislation existing is then put to task in the chapter and analyzed so as to identify how effective it is to prevent illegal data mining by companies on internet users. The findings of this chapter were that the data protection Act as it is inadequacy in ensuring data mining is properly controlled in the country as it minimally refers

to the issue. Other than section 33 of the Act, it does not mention exclusively how individuals are meant to ensure their personal data is not unlawfully collected through data mining i.e. internet users being exposed to fine print that they do not understand and are coerced to provide consent for data collection within such fine print in order to access different websites.

Chapter four of the study is meant to be a comparative analysis between the Kenyan legal regime on data mining in comparison to the United States and the European Union. In the comparison, it was found out that just like Kenya, the United States did not have proper regulations and safe guards on data mining and companies and the government could easily collect information on internet users without facing any risk. This most was the case because of the excuse of terror threats which the United States has faces in the past. However, this lack thereof of laws that ensure the privacy of individuals on the internet is dangerous as collected information on the internet may be acquired and used for illegal means without the users' knowledge and ability to change. The European Union on the other hand has a very strong policy on data security and data protection within its member states. The GDPR is the law that is used within the union and it has put in place strict regulations on the data mining activities that may compromise the privacy of citizens within the member states. The chapter has brought insight into the type of regulation and measures other states such as Kenya ought to take in order to ensure privacy is protected in the cyberspace as much as it is protected in reality. The different positions of the two comparative states in the chapter shows the position that Kenya ought to take in order to ensure legal threats to privacy that come from data mining are averted. The comparison made between the two legal regimes in the chapter advices the wat forward necessary for the Kenyan legal regime to ensure privacy right online are protected and that users of the internet in Kenya are safe from any invasion of their privacy; consented without knowledge or otherwise,

The present chapter concludes the study by reviewing the findings, suggesting recommendations to the existing gaps in legislation and giving concluding remarks in general.

5.3.Recommendations

The above study proposes the following remedies to remedy the gaps presented by the data protection Act on data protection against data mining:

1. The Kenyan legal regime needs to use Solove's pragmatic approach in understanding privacy as a concept so as to avoid situations in the future where the law is rigid on evolving to different problematic situations as has in the past. If the pragmatic approach had been used in the past, the Data Protection Act would have been enacted years ago giving it time to be amended when as new legal threats on privacy come up.
2. There is an inadequacy of proper regulations on data mining as the study has shown and for these to be solved, Kenyan legislators ought to create laws and regulations immediately a legal threat is discovered in order to have sufficient time observe, analyze and amend said laws when need arises so as to prevent situations in which the law does not address matters that should have been addressed.
3. The formulation of section 33 of the data protection Act is not limited only to direct marketing which refers to companies using data mining as a tool for collecting and processing data but should also include measure to control data mining as a whole from companies that us data mining as a resource to garner information without the consent of users
4. The data protection Act should include measures to ensure that internet users do not just consent to collection, handling and processing of personal data in the terms and conditions of websites and internet applications but that if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.
5. Include in the data protection Act a regulation on allowing a data subject to have the right to withdraw his or her consent at any time and to be fair, the consent withdrawal at the time will not affect the lawfulness of data processing that occurred before the consent was withdrawn.

5.4. Conclusion

In conclusion, the study has found a general lack of urgency in the Kenyan legal regime in developing proper legislation concerning the right to privacy and to be specific data protection and

privacy. The amount of time the Act spent in parliament to be passed clearly shows data protection is not a very important subject in the Kenyan legislature despite the need for it.

That being said, it is also commendable that the legislature has brought forward and developed an Act directly tackling issues of data privacy and protection. This shows a willingness to improve the conditions of its citizens in the online would as much as it has tried with the laws that affect reality. Hopefully this willingness and show of improvement will lead to the development and amendment of the Act to include legislation covering data protection as a legal threat on its own.

Bibliography

A. Constitutions

1. *Constitution of Kenya (2010)*

B. Books

1. L. Franchesci, PLO Lumumba,"The Constitution of Kenya, 2010.An introductory Commentary",
2. Richard A. Glenn, "The Right to Privacy: Rights and Liberties Under the Law"
3. Adam Carlyle Breckenridge "The Right to Privacy,"
4. M Kiwinda Mbondenyi & J Osogo Ambani, "The New Constitutional Law of Kenya; Principles, Government & Human Rights"
5. Daniel Solove, Conceptualizing Privacy."
6. Wolfgang Benedek and Madanmohan Rao "Human Rights and Information and Communication Technology,"
7. Prof. Wolfgang Benedek, Dr Matthias C. Kettemann "Freedom of expression and the Internet,"
8. Lawrence Lessig, "Code is Law"
9. Samuel D. Warren; Louis D. Brandeis, "The Right to Privacy".
10. Robert C. Post, Three Concepts of Privacy,
11. Julie C. Inness, "Privacy, Intimacy, and Isolation.
12. William M. Beaney, "The Right to Privacy and American.
13. Adrienn Lukács, "What is Privacy? The History and Definition of Privacy.
14. Jeffrey Rosen, "The Unwanted Gaze: The Destruction of Privacy in America (2000)

C. Journals

1. Stanley R. M. Oliveira and Osmar R. Zaïane, “Toward Standardization in Privacy-Preserving Data Mining
2. Mohammad Tarique Mohammad Saleem, Prof.A.P.Kankale “Privacy Preserving and Data Mining In Big Data
3. F. Pasquale, The Black Box Society- The Secret Algorithms that Control Money and Information (Cambridge: Harvard University Press, 2015)
4. T. Zarsky, “Mine your own Business!”: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion’, Yale Journal of Law and Technology 5(2) (2003)
5. Kirsten Wahlstrom, John F. Roddick & Rick Sarre “Legal and Technical Issues of Privacy Preservation in Data Mining
6. Oliveira M, Zaïane O, “Toward Standardization in Privacy-Preserving Data Mining”
7. Pasquale M, ‘The Black Box Society- The Secret Algorithms that Control Money and Information’Cambridge: Harvard University Press, 2015.
8. McKinsey Global Institute, “Big Data: The Next Frontier for Innovation, Competition and Productivity”
9. Tarique M, Saleem M, .Kankale P ‘Privacy Preserving and Data Mining in Big Data’.
10. Singh H, ‘Data Protection and Privacy Legal-Policy Framework in India’
11. Elmarado E, ‘Data Protection Law in the United States’
12. Tiku N, ‘Europe's New Privacy Law Will Change the Web, and More’.
13. Reed Christopher, Internet Law: Text and Materials, Butterworths, London, 2000’
14. Azmi Madieha Ida, E-Commerce and Privacy Issues: An analysis of the personal data protection bill, Computer and Telecommunications Law Review
15. Tsatsou Panayiota. Internet Studies: Past, Present and Future Directions, Routledge, 2014,

16. John Perry Barlow, “Declaration of the Independence of Cyberspace.”

17. Johnson, D. Robert Post, “Law and borders: the rise of law in cyberspace. Stanford Law Review

18. Teh Jeanette, Privacy Wars in Cyberspace: An examination of the Legal and business tensions in information privacy, Yale Journal of Law & Technology

19. B. Roessler, ‘The Value of Privacy’, Polity Press, Cambridge,2005.

20. Elmarado E, ‘Data Protection Law in the United States’

21. Murphy U, ‘United States: Privacy and Data Protection in United States, International Court of Justice, United Nations, Data Protection, Human Rights, Compliance and the Hypothetical’.

22. Needham B ‘The European Commission’s rationale for strengthening data protection rules for the EU’.

23. Stanley Cavell, Excursus on Wittgenstein's Vision of Language, in THE NEW WITTGENSTEIN.

D. Newspapers

1. Nation Reporter ‘Chris Wylie says he regrets his role in setting up Cambridge Analytica’ https://www.nation.co.ke/news/Chris-Wylie-and-Cambridge-Analytica-/1056-4349336-c0jug9/index.html Daily Nation, Tuesday 20th 2018.
2. Vincent Achuka, ‘How Jubilee reaped poll wins from ties with Cambridge Analytica,’ https://www.nation.co.ke/news/politics/Mystery-men-behind-Uhuru-poll-strategy/1064-5407174-u76bnq/index.html Sunday Nation 5th January 8, 2020.

E. International Instruments

1. Universal Declaration of Human Rights.
2. General Data Protection Regulations (EU).

F. Organizational Reports

1. IJESMT Journal, “Information Privacy & Security in Data Mining.

2. McKinsey Global Institute, “Big Data: The Next Frontier for Innovation, Competition and Productivity”.

G. Websites/Links

1. https://bigdata-madesimple.com/14-useful-applications-of-data-mining/
2. http://ec.europa.eu/justice/data-protection/reform/index_en.htm

H. Dictionaries

1. Black’s Law Dictionary.

.