THE DIGITAL LOCKSMITH: THE REGULATION OF INDIRECT COLLECTION OF PERSONAL DATA.

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

By

Gachemi Renee Lisa Wanjiku

135937

Prepared under the supervision of

Peter Kiptanui

February 2024

Word count 11495

Table of Contents

Acknowledgement

I would like to thank God for His grace throughout this journey.

I would also like to thank my supervisor, Mr Peter Kiptanui for his guidance during the writing of this dissertation.

Finally, I would like to thank my family members and friends who have offered immense support during this process.

Abstract

Many civilizations have relied on data collecting and usage throughout history. As time progressed, so did the techniques for data gathering, storage, and sharing. The reason behind this achievement being computers and the Internet. Today, data is one of the most lucrative commodities on earth. Not only does data promote innovation, but also productivity, efficiency, and growth in the global economy. 'Big data' is the accumulated large volume of information that has the potential to be mined for information and used.[1] One of the biggest data collectors in the world today is the telecom sector. Telecommunications companies can acquire much more data as mobile phone usage grows. Due to the ease of collecting data directly or indirectly from data subjects, the laws governing the same should be as specific as possible. This study will look at the ambiguity of the phrase "interests" as used in the Data Protection Act. Addressing this gap will benefit lawmakers who are developing measures to fill the gaps that have stemmed from the Data Protection Act. Moreover, it is important for telecom firms to understand the importance of valuing data protection.

[1] https://searchdatamanagement.techtarget.com/definition/big-data on 11 December 2023.

Declaration

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

Signed: .....

Date: ….28th February 2024.....

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

Signed: .....

Peter Kiptanui

List of abbreviations

Artificial Intelligence AI

Communications Authority CA

Communication Privacy Management theory CPM

Closed Circuit Television CCTV

Data Protection Commission DPC

Data Protection Act DPA

European Economic Area EEA

European Union EU

General Data Protection Regulation GDPR

Internet of Things IoT

Kenya Information and Communications Act KICA

Mobile Network Operator MNO

National Integrated Identity Management System NIIMS

National Security Agency NSA

Over-the-top OTT

Revised Federal Data Protection Act revFADP

Secrities Exchange Commission SEC

Terms and Conditions T&Cs

United Kingdom UK

United States US

List of cases

Order Police Department of the Riga Region Administration of the State Police v Riga municipality SIA 'Rīgas satiksme' (2017), Supreme Court, Administrative Division, Latvia.

Safaricom PLC v Simon Billy Kinuthia & 2 others (2021) eKLR.

Joshua Kiprop Kisorio v Safaricom Plc & 4 others; Abdinajib Adan Muhumed (Interested Party) (2021) eKLR.

Olmsted v United States (1938), The Supreme Court of the United States.

Roe v. Wade (1973), The Supreme Court of the United States.

Riley v California (2014), The Supreme Court of the United States.

List of Statutes

General Data Protection Regulation.

Data Protection Act of the United Kingdom, 2018.

General Data Protection Regulation, 2016/679.

Constitution of Kenya (2010).

Data Protection (General) Regulations, 2021 (Legal Notice No 263).

Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021 (Legal Notice No 265).

The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021 (Legal Notice No 264).

Data Protection Act (No 24 of 2019).

Safaricom Data Privacy Statement, 2019.

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

Data Protection Directive 95/46/EC.

Revised Federal Data Protection Act of Switzerland, 2023

Chapter 1

Introduction

1.1 Background

In today's day and age where technology has a great impact on daily lives, the need for personal data has increased.[2] As technology advances, storing and capturing of data increases as the state and corporations become custodians of personal data.[3] Personal data is generally information with respect to or about an individual.[4] The data or information does not have to be secret or private.[5] Today, the telecommunications sector is one of the biggest collectors of personal data[6]. Data obtained from telecommunication operators in Kenya show that 53.2 million SIM cards had their registration details duly updated by end of year 2022.[7] The leading telecom provider Safaricom had 38 million duly registered lines. Airtel follows with 13.4 million while Telkom has 1.8 million SIM cards updated.[8] These figures demonstrate the high number of people who entrust telecommunications firms with their personal information. Often, personal data is collected directly from customers who are referred to as data subjects.[9] This comes in various forms such as

---

[2] Kinyanjui AW, 'Data protection as a human right: Balancing the right to privacy and national security in Kenya' Unpublished, University of Nairobi, Nairobi, 2017, 8

[3] Kinyanjui AW, 'Data protection as a human right: Balancing the right to privacy and national security in Kenya' Unpublished, University of Nairobi, Nairobi, 2017, 12.

[4] Tzanou M, 'Data Protection as a Fundamental Right Next to Privacy? "Reconstructing" a Not SoNewRight' in Binder C (eds) *Elgar Encyclopedia of Human Rights*, Elgar Encyclopedia, UK, 2022, 88, 89.

[5] Abdulrauf L, 'The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa', Unpublished, University Of Pretoria, Pretoria, 2015, 8.

[6] 'The importance of data security for enterprises', Africa Telecom Review, 10 March 2022 -<https://www.telecomreviewafrica.com/en/articles/features/2701-the-importance-of-data-security-for-enterprises>- on 3 January 2023.

[7] Muiruri K, 'Over 11 million SIM cards Set For Deactivation on Registration Deadline', Citizen Digital, 14 October 2022 -<https://www.citizen.digital/business/over-11-million-sim-cards-set-for-deactivation-on-registration-deadline-n307433>- on 2 January 2023.

[8] Muiruri K, 'Over 11 million SIM cards Set For Deactivation on Registration Deadline', Citizen Digital, 14 October 2022-<https://www.citizen.digital/business/over-11-million-sim-cards-set-for-deactivation-on-registration-deadline-n307433>- on 2 January 2023.

[9] Section 28, Data Protection Act (No. 24 of 2019).

questionnaires, surveys and interviews. In the telecommunications sector, personal data is collected directly from the data subject with their knowledge and consent in instances such as when one registers for a service such as SIM- card registration or mobile money services.[10] The information collected includes but is not limited to your name, photograph, address, phone number, email, date of birth, gender, credit or debit card information, transaction information, your voice and call data records just to name a few.[11] This data is then stored and used for purposes such as carrying out credit checks and billing.[12] The collection of personal data has increased in the modern era due to information and communication technologies which necessarily endanger the privacy and sanctity of personal data.[13] The expansion of mobile phone use and technological advancements are major contributors to the success of mobile money in Kenya.[14] The fact that the telecommunications companies providing mobile money services did so in a setting without a clear legislation or regulation on data protection[15] poses a serious threat to this achievement.[16] In cases where the data is not safeguarded, it is increasingly being used for identity theft, phishing scams, fraud,[17] money theft,[18] and harassment and stalking of people.[19] Thus, the need for regulations to protect personal data in this modern era cannot be overstated. Several data breaches have been recorded in the telecommunications industry. The two upcoming cases demonstrate the extent to which data breaches in the telecoms sector can harm millions of individuals. In the case of

[10] Safaricom Data Privacy Statement <https://www.safaricom.co.ke/dataprivacystatement/> on 6 February 2023.

[11] Safaricom Data Privacy Statement <https://www.safaricom.co.ke/dataprivacystatement/> on 6 February 2023.

[12] Safaricom Data Privacy Statement <https://www.safaricom.co.ke/dataprivacystatement/> on 6 February 2023.

[13] Nyemba C, 'Right to Data Privacy in the Digital Era Critical Assessment of Malawi's Data Privacy Protection Regime', Published, University of Pretoria, Pretoria, 2018/2019, 6.

[14] Mbogo M, 'The Impact of Mobile Payments on the Success and Growth of Micro-Business: The Case of M-Pesa in Kenya' 2 *The Journal of Language, Technology & Entrepreneurship in Africa* 1, 2010, 182.

[15] This occurred before the passing of the Data Protection Bill.

[16] Gichaga EW, 'Right to privacy in the wake of mobile money transfers in Kenya: Is the data protection bill a step in the right direction?' Unpublished, Strathmore University, Nairobi, 2018, 22.

[17] Button M and Cross C, *Cyber Frauds, Scams, and Their Victims*, 1 ed, Routledge, London, 2017, 43-45.

[18] Sissing S, 'A criminological exploration of cyber stalking in South Africa', Unpublished, University of South Africa, Pretoria, 2013, 19-20.

[19] Feldstein S, 'The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression' 30 *Journal of Democracy* 1, 2019, 40.

Safaricom PLC v. Simon Billy Kinuthia & 2 others [2021] eKLR,[20] two Safaricom workers fraudulently obtained personal information from as many as 11.5 million subscribers and requested help from a third party in order to sell the information to a betting organisation. Additionally, they made an effort to extort millions from Safaricom under the threat of leaking the data. In the same way, the petitioner in Joshua Kiprop Kisorio v. Safaricom Plc & 4 others; Abdinajib Adan Muhumed (Interested Party) [2021] eKLR[21] contends that the interested party was able to retrieve his call and message history as well as the data of three other people and share it with other parties. These two instances serve as stark reminders of the shortcomings of Kenya's data protection[22] laws in the telecoms industry which eventually allow for the possession of personal information by unauthorised individuals.

The Constitution of Kenya vouchsafes for the right of privacy. Notably, Article 31 enumerates this right.[23] It provides that "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;[24] or the privacy of their communications infringed." [25] This recognition provides an indication of the importance of the right to privacy. [26] In Kenya, the Data Protection Act (DPA) allows for direct (with consent)[27] and indirect collection (without consent)[28] of personal data. Indirect collection can only occur in six circumstances. Of the six circumstances, two circumstances stand out. Section 28(2)(e) on the requirement that the collection would not prejudice the interest of the data subject and section 28(2)(f)(iii) which talks about the protection of the data subject's interests.[29] The term "interests" of the data subject has a very broad definition. Due to its lack of specificity,

[20] Safaricom PLC v Simon Billy Kinuthia & 2 others (2021) eKLR.

[21] Joshua Kiprop Kisorio v Safaricom Plc & 4 others; Abdinajib Adan Muhumed (Interested Party) (2021) eKLR.

[22] Data protection is the process of safeguarding important information from corruption, disruption and/or loss. Juneh H, 'Data Protection and Data Security', Academia Edu, 2018, 5.

[23] Article 3, Constitution of Kenya (2010).

[24] Article 31(c), Constitution of Kenya (2010).

[25] Article 31(d), Constitution of Kenya (2010).

[26] Constitutional Petition No. 53 OF 2017, eKLR.

[27] Section 28(1), Data Protection Act (No. 24 of 2019).

[28] Section 28(2), Data Protection Act (No. 24 of 2019).

[29] Section 28(2), Data Protection Act (No. 24 of 2019).

it is open to abuse. This leaves a legal gap since the data collectors are able to argue that their actions are justified by the interests of the data subject, even though those actions violate the data subject's right to privacy.

1.2 Statement of problem

Collecting personal information from a source other than the individual to whom it relates, such as another institution or a third party, is known as "indirect collection". It is risky to give data collectors unrestricted access to the personal information of data subjects as it might result in a constitutional privacy breach. People's interests are extremely diverse and range from business-related to personal, political, and even health-related. Consequently, using the phrase "interests" in a general sense opens the door to manipulation.

In 2019, it was discovered that AT&T, an American multinational and industry leader in telecommunications, was selling real-time location data about its customers to unaffiliated businesses. User privacy and the potential misuse of personal information were raised by this covert collection and sharing of location data. This serves as a paradigmatic illustration of the harm that results from the collection of data in an indirect manner. The aim of this study is to determine whether Section 28 of the DPA should be changed to specify the precise categories of interests that permit indirect data collection in the Kenyan telecommunications sector.

1.3 Hypothesis

My hypothesis is that Kenya's approach to the indirect collection of personal data as endorsed in Section 28 (2)(e) and Section 28(2)(f)(iii) of the DPA is insufficient and thus violates the right to privacy of the data subject. Insofar as the personal data is protected, the collecting of personal data by telecommunications corporations directly serves the nation. This is appropriate because the data subject voluntarily and knowingly provides the information and is aware of its intended use. In contrast, indirect collection of personal data differs in that it happens without the subject's knowledge or consent and without the subject being aware of what information is being gathered. As it is not from the data subject, the data may not be reliable in and of itself. Additionally, it eliminates the data subject's ability to choose who should access their personal information. As a result, their right to privacy is violated.

1.4 Research Objectives

1. To study the methods of indirectly collecting personal data from a data subject.
2. To investigate the gaps existing in the law on the topic of data subject's privacy interests.
3. To assess what Kenya can learn from the European Union on the question of privacy interests of the data subject.

1.5 Research Questions

1. What are the ways of indirectly collecting personal data from a data subject?
2. What are the gaps existing in the law on the topic of data subjects' interests?
3. What are the lessons to be taken from the European Union on the question of privacy interests of the data subject?

1.6 Justification

There are presently 40 million sim card registrations active across the nation.[30] According to the most recent census, this represents more than 50% of Kenya's population. This indicates that telecommunications corporations have a huge amount of personal information in their possession. As a result, they ought to have enough laws to govern the gathering, handling, and storing of personal data. But nonetheless, if these businesses are not adequately controlled, many people could be impacted if their personal information is misused. Furthermore, because the data subject has no control over who obtains their personal information, the right to privacy is harmed when indirect collection of personal data is permitted without sufficient constraints. It is, therefore, crucial to address the issue of causation to assign liability. This study will be beneficial in as much as it attempts to address the issue by outlining all the harm that could result from not having proper data protection laws as well as highlighting the solutions adopted by other jurisdictions. This study is unique because it will deal with the ambiguity of the phrase "interests" as it is used in the DPA. Addressing this gap will be beneficial to lawmakers who are drafting policies to address different gaps arising from the DPA. Furthermore, it will be vital for telecom companies to comprehend the

[30] Muiruri K, 'Over 11 million SIM cards Set For Deactivation on Registration Deadline', Citizen Digital, 14 October 2022-<https://www.citizen.digital/business/over-11-million-sim-cards-set-for-deactivation-on-registration-deadline-n307433>- on 2 January 2023.

value of data protection. Researchers looking at this novel subject of data protection in Kenya will find an answer to this issue to be helpful as well.

1.7 Scope

In addition to providing suitable and practical remedies to address any issues found with the collection, the study attempts to evaluate the possible impacts of the present standard of indirect collection of personal data.

1.8 Chapter breakdown

The introduction to the dissertation will be provided in this chapter. It includes details on, for example, the theoretical framework that offers the rationale for the main claims that will guide the study. Also, it includes a problem statement, the justification and research objectives.

The theoretical framework of this paper will be examined in chapter two. The theoretical problem creates the vision toward which the problem is focused and serves as a starting point for the research problem. It starts off by outlining the theories and its various components. Finally, it draws a connection between the theory and the privacy and data protection issues as its conclusion.

In chapter three, we'll look at how data is indirectly collected from data subjects by telecommunication entities. Understanding the risks and potential consequences of improper management of personal data will be the next step. We will then look at the various situations where people in real life have suffered as a result of improper handling of personal data. Moreover, we will look at the eminent gaps in the Kenyan laws when it comes to privacy rights. The significance of the right to privacy will be discussed last.

The fourth chapter examines European Union legislation and what Kenya can take away from them. First, a thorough analysis of the EU regulations governing the indirect gathering of personal data will be conducted. The interpretation of the aforementioned statutes will then be examined in an effort to comprehend their rationale. Finally, we'll examine how the rules of the EU have impacted other regions of the globe and how these laws have been incorporated into the legal systems of other nations.

Lastly, chapter five will use recommendations to suggest a better approach for processing personal data as well as a summary of the findings.

Chapter 2

Theoretical framework and methodology

2.1 Introduction

This chapter seeks to provide a specific lens through which one can view this topic. Understanding the philosophical foundations upon which law and policy makers base their decisions is necessary in order to attempt to offer answers to the current issue. Personal data, despite taking on a more modern form, still constitutes a person's private information, so special consideration should be given to the value of its protection.

The overarching issue of the study is data protection, which refers to the development and structuring of data-related regulations, those that are intended to protect said data from manipulation and exploitation. It heavily relies on the constitutional right to privacy. The DPA appears to aim to redress the power disparity and give the data subject significant access to their own data. In this chapter we will explore three theories that will give a view of how data is treated.

2.2 Surveillance Capitalism

This theory, which was created by Shoshana Zuboff, explores the ways in which businesses—including telecommunications companies—extract and sell personal data in order to turn a profit. Surveillance capitalism is the monetization of data gathered via observing people's actions and behaviors both online and in person. The most common application of consumer monitoring is targeted marketing and advertising. In July 2014, John Bellamy Foster and Robert W. McChesney popularized the term surveillance capitalism in Monthly Review, a New York socialist newspaper. Their concept of surveillance capitalism was centred on the US military and citizen surveillance.

It represents the current, mass monetization of raw personal data from individuals in order to predict and change their behaviour. Zuboff defines surveillance capitalism in her 2019 book The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power[31] as

[31] Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019.

a "new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales."

Surveillance capitalism is employed by different companies to gather information from their customers. Examples of such companies are Amazon, Apple, Google, and Facebook. To be specific, the data collected includes search histories, geo locations, social media posts, and product keywords recorded by microphones in smartphones and internet of things (IoT) devices. The data is combined into prediction products, which are then sold to corporations for use in targeted and behavioral marketing. Using prediction goods, businesses may market and advertise to those who are most likely to purchase their products and services. According to Zuboff, “people whose data is collected and monetized in this way are either unaware of it or do not have the option of consenting to its collection and distribution without jeopardizing the functioning of their devices.”

Companies that use the surveillance capitalism model, follow a three-step procedure. To begin, they collect a vast amount of data by acquiring extra data generated by an individual's interactions with digital devices, websites, and apps. This surplus data is not directly tied to an individual's use of a digital device or service, but rather results from such use, and includes information such as the user's physical location, search history, and habits, such as the timing of their workout routines. The acquired data is then analyzed utilizing advanced machine intelligence manufacturing procedures that use artificial intelligence technologies to create predicted products. These prediction tools can predict an individual's activities in the present, near future, and distant future. Finally, corporations enter what Zuboff refers to as "behavioural futures markets," selling prediction products to companies in industries such as insurance, retail, finance, and e-commerce. These firms use prediction tools to target their goods and services at potential clients and participate in behavioural modification, quietly affecting individuals' behaviour, as evidenced in insurance companies' methods such as behavioural underwriting.

According to Zuboff, “…surveillance capitalism is a separate economic ideology rather than an inherent component of information technology.” Users are frequently provided access to devices, services, and software upgrades only after agreeing to conditions that allow third parties to collect and share their data. While some acquired data may help improve products or services, the vast majority is classified as proprietary behavioural surplus. This classification means that any

personal data obtained through a user's engagement with a company's service is regarded as the company's exclusive property, rather than the user's. The proprietary character of this behavioural surplus emphasises the company's control and ownership of the data, highlighting the uneven power dynamic between users and surveillance capitalist entities.

2.3 Communication Privacy Management

The premise of this study will be the Communication Privacy Management theory (CPM).[32] Simply stated, the theory contends that people believe they own their private information and have the right to regulate it. Managing personal data is not required until other people are engaged. By not framing disclosure as being exclusively about the self, CPM does not restrict an understanding of disclosure. Rather, the CPM theory emphasises that when management is required, others are granted co-ownership status, hence extending the notion of disclosing information.

The theory uses a privacy boundary metaphor to show where personal data is located and how the barrier enlarges to accommodate numerous owners of personal data. The CPM idea has been used in eleven countries and in a wide range of settings where privacy management takes place, including social media, health, families, and organisations. Communication boundary management was the first name of the theory. In order to cover the function of information sharing in private, Petronio later changed the name of the theory to communication privacy management theory in 2002. This theory is distinctive in that it provides a thorough understanding of how the concepts of disclosure and privacy relate to one another.

Privacy ownership, privacy control, and privacy disturbance are the three components of CPM. Privacy ownership refers to the information we hold about ourselves that only we are aware of, privacy control refers to the sharing of that information with others, and privacy turbulence refers to the difficulty of reaching a consensus among the information's owners over its disclosure. Individuals commonly employ a set of privacy guidelines to handle their personal information. The boundary permeability rule determines the scope, breadth, and depth of information

[32] Petronio S, Caughlin JP, *Communication Privacy Management Theory*, Sage Publications, Mahwah, 2006, 35-49.

disclosure. People create a stronger barrier around information in order to maintain tight control and secure that specific information.

The fundamental tenets of CPM are that people believe they have a right to own and control their personal information, that people exercise that right through a set of privacy laws, and that when people share their personal information with others, those other people become co-owners of that specific information. Co-owners of the personal information must negotiate and reach an understanding regarding the privacy rules for disclosing it to others. If the co-owners do not reach an understanding or adhere to the privacy rules, boundary turbulence frequently results.

The theorist has had the opportunity to reply to criticisms of the theory as it has developed over time within the setting of communication privacy management theory. When compared to Relational Dialectics (1996), one critic contends that CPM is not a dialectic theory, but rather is based on dualistic thinking, in which privacy and transparency live in equilibrium. In her essay published in 2002, Petronio responded to these criticisms by stating that "(CPM) instead pushes for collaboration with others that does not propose an optimal balance between transparency and privacy."

Another flaw with the theory is that it's predicated on the idea that people make decisions based on other people as well as on themselves, which means that people who don't fit Petronio's definition of a human are not covered by the theory, and it can't be used to explain them. About the CPM's strength, it is evident from the large number of research articles that have been created that are firmly founded on Privacy Management theory. This theory can be applied to the project to demonstrate understanding of the proper handling of personal data.

2.4 Westin's Theory of Privacy

Prior to the publication of Westin's groundbreaking book "Privacy and Freedom," the dispute over privacy largely focused on how much the government could regulate over an individual's right to bodily autonomy. This debate was particularly prominent in cases such as Roe v. Wade. It also focused on privacy rights related to photography and clandestine operations such as wiretapping. But as the 1960s saw a surge in computer technology, it was evident that the law was lagging

behind. Due to the extensive computerization of financial, medical, legal, and other personal records, people's personal information was now more easily available and subject to abuse and misuse.

In his book, "Privacy and Freedom," Westin defined the concept of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." This method was pioneering. Westin laid the groundwork for modern understandings of online privacy laws long before the Internet existed, arguing that citizens should have final say over how much of their personal data is disclosed and to whom, how it should be maintained, and how it is distributed.

The four purposes of privacy—personal autonomy, emotional release, self-evaluation, and limited and protected communication—are described in detail in Westin's view of privacy. To put it simply, personal autonomy is the ability to resist being controlled, influenced, or exposed by other people. Conversely, emotional release refers to releasing feelings and pressures brought on by societal expectations to ensure you can keep things to yourself. Moreover, the ability to incorporate experiences into significant patterns and impart uniqueness on occurrences can be used to explain self-evaluation. Lastly, communication that is both restricted and secure entails establishing personal boundaries and sharing personal information with someone one trusts.

The notion of privacy as the authority over personal data is typically attributed to Westin. This assertion is significantly less detailed than Westin's thorough definition of privacy, which describes four levels of privacy that can be attained through psychological or physical means: solitude, intimacy, anonymity, and reserve. Achieving a balance between the need for social interaction and disclosure and the urge to retreat into one of the "states" of privacy is necessary for making the "claim" of privacy. The adjustment process is influenced by environmental circumstances, social norms (and the monitoring necessary to enforce social standards), and other people's curiosity.

Finally, he discusses the four states of privacy giving meaning to each. First, solitude, or the condition of not being watched by others. Second, intimacy—the privacy necessary for a close

relationship. The state of remaining unknown and unidentified which is referred to as anonymity. Lastly, reserve, or the intention to restrict information shared with others.

2.5 Methodology

The legal analysis used in this research study will mostly be doctrinal, or "black letter law" analysis. The focus will be on comprehending existing legislation and coming up with practical solutions. An assessment of primary and secondary materials, such as news articles, legal publications, research papers, journals, statutes, and current legislation. To showcase best practices from a jurisdiction that has had comparable concerns over data privacy and already has a data protection framework in place, this study will include a comparative analysis.

2.5 Conclusion

In conclusion, this chapter establishes the theoretical foundation for understanding the framework on personal data and the constitutional right to privacy. Surveillance Capitalism, as conceptualised by Shoshana Zuboff, looks at how firms, especially telecommunication companies, use personal data for profit, revealing power imbalances where consumers frequently unintentionally cede control over their information. The Communication Privacy Management (CPM) theory explains that individuals have ownership and regulatory rights over their personal data, emphasising the dynamic nature of privacy borders and the necessity for consensus when others are involved. Westin's Theory of Privacy, based on "Privacy and Freedom," provides a fundamental concept of privacy as an individual's right to control the sharing of information about themselves. These theories will guide the research, acting as analytical tools to help unfold the intricacies of indirect data collecting and provide comparative analyses of data privacy regulations. The subsequent investigation will strike a careful balance between protecting individual privacy and enabling lawful uses of personal data in the context of telecommunication services. The effectiveness of the DPA will be examined under this view.

Chapter 3

Data Protection Framework In Kenya

"*The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought*_"- US Supreme Court Chief Justice Jo~ Roberts in Riley v California (2014)[33]

3.1 Indirect collection of personal data

Information is gathered indirectly when the user does not directly disclose this information. There are a number of ways in which data can be collected indirectly by telecommunication companies. These include metadata collection, location data tracking, user behaviour analysis, network analysis, and third-party data sharing.

To optimize the network, maintain network security, identify fraud, enhance customer service, and carry out targeted marketing, a mobile network operator (MNO) employs call detail information, sales data, and network performance monitoring. For example, de-identified or aggregated data is usually enough to comprehend traffic volumes in specific areas. However, identifying information is required in other situations, such as when an MNO has to know how the network functions for a certain client in order to offer discounts or credits in the future, or needs to find customers who could be on the incorrect tariff plan.

Metadata is not defined in the Kenyan laws; however, it is a very important aspect of data collection. Data that offers details about other data but not the content of those other data is known as metadata.[34] Communications "metadata" can imply many things and be used for different reasons depending on the context and media employed. It is frequently described as information that describes information.[35]

---

[33] Olmsted v United States (1938), The Supreme Court of the United States.

[34] 'What is Metadata?', GSMA Association, https://www.gsma.com/publicpolicy/metadata on 25 December 2023.

[35] 'Is metadata personal data?', Atlaw, 30 November 2022, https://www.altlaw.co.uk/blog/is-metadata-personal-data on 3 January 2024.

An individual can be identified using metadata. Not only may it be private information, but it may also be extremely sensitive.[36] Even though this information would not be visible to the naked eye, it might be retrieved and read, which could have unintended repercussions.[37] When retrieved from electronic correspondence, it may disclose extremely private and sensitive data. This includes the phone numbers dialed, the websites visited, the location, the time, date, and length of each call, [38] among other details that allow precise conclusions to be drawn about the private lives of the individuals engaging in the electronic communication, including their social relationships, daily routines and activities, interests, and preferences.[39]

Four primary forms of metadata are call and SMS metadata, email metadata, user activity or behavior metadata, and location or network metadata in the context of telecommunications.[40] Information on the creation, delivery, and distribution of a message is provided via metadata. Consequently, it can contain information such as the time and date of a phone conversation or the address from which an email was accessed.[41] The following metadata is generated when a phone call is placed: the caller's phone number, the phone number(s) called, the distinct serial numbers of the phones involved, the call's time and length, the participants' locations, and the calling card numbers.[42]

---

[36] 'What is metadata?', Privacy Proficient, 24 May 2019, https://privacyproficient.com/what-is-metadata/ on 18 December 2023.

[37]'Is metadata personal data?', Atlaw, 30 November 2022, https://www.altlaw.co.uk/blog/is-metadata-personal-data on 3 January 2024.

[38] 'What is metadata?', Privacy Proficient, 24 May 2019, https://privacyproficient.com/what-is-metadata/ on 18 December 2023.

[39] 'What is metadata?', Privacy Proficient, 24 May 2019, https://privacyproficient.com/what-is-metadata/ on 18 December 2023.

[40] 'What is Metadata?', GSMA Association, https://www.gsma.com/publicpolicy/metadata on 25 December 2023.

[41]'Metadata and Privacy: A Technical and Legal Overview', Office of the Privacy Commissioner of Canada, October 2014, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/ on 18 December 2023.

[42] Metadata and Privacy: A Technical and Legal Overview', Office of the Privacy Commissioner of Canada, October 2014, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/ on 18 December 2023.

The Data Protection Act of the United Kingdom[43] sees the implementation of the GDPR and defines an identifiable person as someone who can be either directly or indirectly identified by their name, identification number or geolocation.[44] It further defines a data subject as the identified or identifiable living individual to whom personal data relates.[45] Therefore, a conclusion that can be deduced is that metadata can be used to reveal information that can identify a person who would be termed as a data subject. Therefore, metadata is personal data.

Technology has transformed marketing. Marketers can gain a unique understanding of customers' needs and behaviors by analyzing the vast amounts of data at their disposal. Behavioral analytics benefits both organizations and consumers. It enables businesses to enhance sales and conversion rates while providing clients with services tailored to their preferences and needs.[46] However, the use of behavioral analytics poses significant data privacy concerns.[47] In addition to posing ethical questions, collecting excessive amounts of data can get companies in trouble with the law.

Behavioural analytics is gathering and analyzing data on how customers use a digital product, such as an app or website.[48] Organizations can then use this information to better understand how users interact with the digital service and make informed decisions about changes. Many firms employ event-driven behavioral analytics to gain insights into their customers' preferences, intents, and habits. It enables the creation of behavioral profiles. This information may be used for targeted

[43] Data Protection Act of the United Kingdom, 2018.

[44] Section 3(3), Data Protection Act of the United Kingdom, 2018

[45] Section 3(5), Data Protection Act of the United Kingdom, 2018

[46] Breaker- Rolfe J, 'The Thin Line Between User Behavioral Analytics and Privacy Violation', Fortra, 10 July 2023, https://www.tripwire.com/state-of-security/thin-line-between-user-behavioral-analytics-and-privacy-violation on 19 December 2023.

[47] Breaker- Rolfe J, 'The Thin Line Between User Behavioral Analytics and Privacy Violation', Fortra, 10 July 2023, https://www.tripwire.com/state-of-security/thin-line-between-user-behavioral-analytics-and-privacy-violation on 19 December 2023.

[48] Breaker- Rolfe J, 'The Thin Line Between User Behavioral Analytics and Privacy Violation', Fortra, 10 July 2023, https://www.tripwire.com/state-of-security/thin-line-between-user-behavioral-analytics-and-privacy-violation on 19 December 2023.

advertising, manipulation, or other harmful purposes.[49] An ordinary telecommunications firm collects vast amounts of information on a regular basis. This data contains vital information about client behavior, network operations, equipment status, and service quality.[50] Analytics enables them to collect, analyze, and interpret data more deeply in order to reduce pain points and forecast future outcomes, resulting in better decision-making in real time and in the future. Precedence Research estimates that the telecom analytics industry would be worth $23.66 billion by 2023, up from $6.19 billion in 2022.[51] The use of telecom analytics is widely regarded as one of the most important ways to improve company, but it also presents a number of challenges for telecom operators to overcome.

As consumers began interacting with their banks' mobile applications on a daily basis to check balances, make payments, and move funds across accounts, all of the data created by those activities became a holy grail for any parties interested in analyzing user behavior.[52] Mobile behavioural analytics are far more intimate than the web, especially as there are a lot more sensors involved.[53] Examining this highly personalised data provides profound insights into a user's daily routines and behaviours, including details such as posture (sitting or standing), handedness (right or left), waking and sleeping patterns, and even specific daily activities like using the restroom or leaving for work. The storage of such intimate and extremely sensitive data on centralised servers carries substantial dangers, including a potential violation of security and user privacy.

Globally, telecommunications industry revenues are falling in key business services such as SMS and voice calls due to the availability of alternatives and competition from over-the-top (OTT) services such as WhatsApp, Skype, Zoom, Google Chat, and others. These factors have forced carriers to seek other revenue streams.[54] At the same time, we've become reliant on mobile phones

[49]'Understanding Privacy Violations through Metadata Analysis in Communication', Utilities One, 22 November 2023, https://utilitiesone.com/understanding-privacy-violations-through-metadata-analysis-in-communication on 20 Decemeber 2023.

[50] Grischina A, 'Data Analytics in the Telecom Industry: Use Cases, Challenges, and Trends', Softteco, 2023, 1.

[51] Grischina A, 'Data Analytics in the Telecom Industry: Use Cases, Challenges, and Trends', Softteco, 2023, 1.

[52] Dutt D, ' Behavioral Analytics: A Privacy-First Approach', Forbes, 2020, 2.

[53] Dutt D, ' Behavioral Analytics: A Privacy-First Approach', Forbes, 2020, 2.

[54]Akindele L, ' Commercialisation of data in the telecommunications sector', PwC, 2020,1.

because of their sophistication and increased data connectivity. They have become a ubiquitous tool for communication, transportation, shopping, entertainment, news, banking, insurance, and money transfer services, providing telecom corporations with data monetization options based on insights into user behaviours and usage patterns.

Leading telecom operators are investing heavily in data analytics and technologies, as well as exploring new methods to use data to improve their businesses by deriving relevant insights and creating value in order to achieve a competitive advantage. Telcos gather many types of data, including customer information, device data, use data, and location data.[55] The initial classification of location data collection can be based on the two primary approaches for locating a mobile device: by internal and autonomous means within the device, or externally through communication with other devices.[56] Controlling the disclosure of location data is harder once it has been gathered and retained than if it hadn't been done so in the first place.[57]

Legal and ethical issues surrounding the use of location data in diverse contexts demand rigorous analysis to guarantee individuals' rights are safeguarded while also permitting beneficial uses of this information.[58] Location data, particularly when acquired over time and connected with additional information from freely available web sources, can expose much sensitive information about individuals and their habits: where they live and work, their interests, their religion, etc.[59]

The fundamental problem in gathering location information for a device is who decides whether to enable location determination. Exceptions include legal requirements, such as non-removable monitoring devices for parolees. External location determination does not provide for user choice, whereas regulated communication systems do. Some questions must be asked to determine the

[55] Akindele L, ' Commercialisation of data in the telecommunications sector', PwC, 2020,1.

[56] Privacy Issues in Location-Aware Mobile Devices https://ics.uci.edu/~ics215/papers/privacy-issues.pdf

[57] Privacy issues in Location-Aware Mobile Devices https://ics.uci.edu/~ics215/papers/privacy-issues.pdf

[58]Minch R, ' Privacy Issues in Location-Aware Mobile Devices', Hawaii International Conference on System Sciences, Hawaii, 2004, 1.

[59]Tsohou A and Kosta E,'Enabling valid informed consent for location tracking through privacy awareness of users: A process theory' 33 *Computer Law & Security Review* 4, 2017, 435.

intensity of the problem. Should users of location-enabled devices be notified when location tracking is being used? Should they be allowed to turn it off? Should an opt-in or opt-out approach be taken? What factors will influence the answers?

While metadata analysis can give vital information for legitimate reasons such as law enforcement investigations, it also presents substantial privacy concerns.[60] Here are some key concerns associated with metadata analysis:

a. Lack of Consent: Users may not be aware that their metadata is being collected and analyzed, and explicit consent is not always requested.
b. Granularity of Information: Combining seemingly minor metadata points might disclose intricate details about an individual's habits, routines, and personal life.
c. Third-Party Access: Third-party service providers often collect and store metadata, which raises concerns about who has access to it and how it is utilized.
d. Unintended Connections: Metadata analysis might unintentionally connect persons to others they don't want to be linked with, perhaps leading to false accusations or other unwanted outcomes.

Much of the data utilized in big data services is not personal data. Weather sensor readings, for example, do not constitute personal information. Non-personal data can become personal data if it is linked to a specific individual, such as when a traffic management system detects the location of a connected car and combines it with the vehicle registration number and ownership records. When the data is merged with other data sets, big data analytics services should include measures against re-identification of individuals.[61]

[60] 'Understanding Privacy Violations through Metadata Analysis in Communication', Utilities One, 22 November 2023, https://utilitiesone.com/understanding-privacy-violations-through-metadata-analysis-in-communication on 20 Decemeber 2023.

[61] 'Mobile Privacy and Big Data Analytics', https://www.gsma.com/publicpolicy/resources/mobile-privacy-big-data-analytics on 18 December 2023.

3.2 Privacy concerns

Breach notifications are essential to data protection law and to ensure transparency on part of the data controller.[62] However, the criterion for only notifying when there is a "real risk of harm to the data subject" is ambiguous, as the clause contains no risk or likelihood criteria. The vagueness can create loopholes for data controllers who hide behind subjective risk assessments. For a breach notice to be meaningful to data subjects, it must be written in clear and simple language and include guidance and resources for taking precautions to avoid harm and seeking redress if harm has occurred. Consideration must be given to ensure that illiterate individuals are not excluded, and that the data controller takes the necessary steps to keep them informed.

Indirect collection, however, does not operate in the same way in the telecommunications industry. This is because the law does not consider this a breach. This is especially concerning given that there have already been several examples globally of how individual data can and is exploited and abused by governments, businesses, and individuals alike. Ideally, a data subject should be informed of who possesses their data, how it was gathered, and how it is utilized. However, whether or not such is the case is another thing.[63] An example would be the texts individuals receive from fast food chains, the government, or the National Integrated Identity Management System (NIIMS) system, which is being rolled out in our country without the knowledge of many people, as well as its safeguard.

Internationally the best example would be Edward Snowden's exposé on the United States violation of data privacy in the early 2010s.[64] In the early 2010s, Edward Snowden's exposé revealed widespread and systematic violations of data privacy by the US government. Snowden, a former National Security Agency (NSA) contractor, disclosed a trove of sensitive documents that revealed massive monitoring techniques employed by US intelligence agencies. The allegations

[62] Jarameel K and Kibet B, 'Defining Data Protection in Kenya: Challenges, Perspectives and Opportunities', SSRN, 2022, 4.

[63] Munir A, 'The Consent Model Under the Data Protection Act; Introducing Complementary Provisions to Enhance Protection', Unpublished LLB Dissertation, Strathmore University Law School, 2021, 4.

[64] Satter R, 'U.S. court: Mass surveillance program exposed by Snowden was illegal', Reuters, 2020, 1.

principally concerned two major surveillance programs: PRISM and the mass collecting of telephone metadata.[65]

The 21st century has become the century of big data.[66] Edward Snowden's revelations[67] demonstrate that the government and corporations routinely gather, store, and search vast volumes of data derived from phone calls, internet searches, electronic payments, and mobile money transfers. Technological advancement has overtaken our privacy safeguards.[68] As a result, the government and companies may now track our digital presence in ways that were previously inconceivable.[69] This digital footprint is continually expanding, including more and more information about the most personal elements of our lives. This applies to our conversations, whereabouts, online searches, purchases, and even our bodies. When the government gets ready access to this data, we lose more than just privacy[70] and control over our data.[71] Free speech, security, and equality suffer as well.[72]

Large-scale government surveillance has always been associated with authoritarianism. North Korea, the People's Republic of China, and the Soviet Union are examples of authoritarian nations that have significant monitoring systems in place.[73] In recent decades, however, established liberal democracies have been increasingly eager to monitor their citizens on a huge scale.[74] Government surveillance and the erosion of privacy it entails are being discussed as a source of distrust and

[65] Satter R, 'U.S. court: Mass surveillance program exposed by Snowden was illegal', Reuters, 2020, 1.

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

[67] Satter R, 'U.S. court: Mass surveillance program exposed by Snowden was illegal', Reuters, 2020, 3.

[68] https://www.aclu.org/issues/privacy-technology on 10 January 2024.

[69] https://www.aclu.org/issues/privacy-technology on 10 January 2024.

[70] Königs P, 'Government Surveillance, Privacy, and Legitimacy' 35 *Philosophy and Technology* 8, 2022.

[71] Königs P, 'Government Surveillance, Privacy, and Legitimacy' 35 *Philosophy and Technology* 8, 2022.

[72] https://www.aclu.org/issues/privacy-technology on 10 January 2024.

[73] Dunnage J,' Policing and surveillance',in Corner P and Lim J (eds) *The Palgrave Handbook of Mass Dictatorship,* Palgrave Macmillian, Ohio, 2016, 122.

[74] Königs P, 'Government Surveillance, Privacy, and Legitimacy' 35 *Philosophy and Technology* 8, 2022.

feelings of vulnerability, as a potential source of discrimination and unjust dominance, and as a threat to democracy and the integrity of the public sphere, to name a few.[75] Modern government surveillance relies increasingly on technology rather than human spies and informers.[76] Surveillance approaches include monitoring public locations with CCTV cameras, automatically intercepting and retaining internet and telecommunication traffic, and using Artificial Intelligence (AI) to make sense of massive volumes of data acquired.

3.3 Real Life Situations

To understand the effects of poor protection of personal data, a few real life examples will be explored.

3.3.1 Targeted Advertising and Profiling:

Targeted advertising is a powerful tool that allows advertisers to present consumers with ads tailored to their specific traits, interests, and shopping behaviour.[77] This concept works on the principle of "surveillance," where customer data is collected to segment audiences based on demographics, interests, and browsing behaviour, resulting in unique ads for each segment. Telecommunications companies that engage in surveillance capitalism may collect personal data about users indirectly in order to develop detailed profiles. In real life, this can result in extremely personalised advertising, with individuals receiving ads based on their habits, preferences, and location. For example, a person may receive advertisements for certain items or services depending on their internet behaviours and mobile device usage. A good example would be receiving advertisements through messages from different companies that you have not opted-in to.

Recently, the Irish Data Protection Commission (DPC) imposed a fine of $400 million on Microsoft for using targeted advertising practices that violated GDPR on its subsidiary social media website, LinkedIn. A similar case involved Meta (the parent company of Facebook and

[75] Königs P, 'Government Surveillance, Privacy, and Legitimacy' 35 *Philosophy and Technology* 8, 2022.

[76] Königs P, 'Government Surveillance, Privacy, and Legitimacy' 35 *Philosophy and Technology* 8, 2022.

[77] https://rainmaker.co.in/blog/view/a6bf5b46-ab33-47c2-bc07-2ed66c006892/the-price-of-personalization-how-targeted-advertising-breaches-data-privacy-and-challenges-the-gdprs-shield on 18 December 2023.

Instagram), which was fined €390 million (€210m for Facebook and €180m for Instagram) by the DPC. Meta utilised Article 6(1)(b) of GDPR, which allows data processing if 'necessary for the performance of a contract,' to process users' personal data for profiling purposes without clear consent.[78]

3.3.2 Data breaches and identity theft:

Hackers target indirectly collected personal data held on centralised computers. Data breaches can compromise sensitive information such as user locations, communication patterns, and even biometric data. This can result in identity theft, fraud, and the improper use of personal information. A data breach occurs when unauthorized parties gain access to sensitive information. A data leak can have serious and widespread implications.[79] A common motivator for attackers is financial gain. They may attempt to steal critical financial information, such as credit card numbers, bank account logins, or personal information, and then sell it on the dark web or use it for criminal purposes. Some hackers work for the government, collecting intelligence and spying on competing countries. Others may want to prove their skills and test their limits.[80]

Yahoo! suffered the greatest data breach in history between 2013 and 2014. Attackers gained unauthorized access to names, email addresses, passwords, and security questions, affecting more than 3 billion user accounts. The incident was not publicized until 2016, when Verizon was negotiating to acquire the tech behemoth. Verizon reduced its prior offer by $350 million as a result of the data leak and paid $4.48 billion for Yahoo!

3.3.3 Invasion of Privacy:

The communication privacy management theory highlights the importance of allowing people control over their personal information. In practice, the indirect acquisition of data may result in a breach of privacy since people assume their every move is being monitored. This invasion can spread to sensitive areas such as health regimens, personal routines, or even the timing of daily activities, weakening a person's sense of independence. In July 2022, mobile communications

[78] https://rainmaker.co.in/blog/view/a6bf5b46-ab33-47c2-bc07-2ed66c006892/the-price-of-personalization-how-targeted-advertising-breaches-data-privacy-and-challenges-the-gdprs-shield on 19 Decemeber 2023.

[79]Danao M and Aditham K, 'What Is A Data Breach? Definition, Examples & Prevention', Forbes Advisor, 2023.

[80] Danao M and Aditham K, 'What Is A Data Breach? Definition, Examples & Prevention', Forbes Advisor, 2023.

company T-Mobile disclosed the terms of a settlement for a consolidated class action lawsuit following a data breach that happened in early 2021 and affected an estimated 77 million users.[81] The incident involved "unauthorized abbaccess" to T-Mobile's servers after a piece of customer data was advertised for sale on a known cybercriminal forum. According to an SEC filing, T-Mobile would pay a total of $350 million to finance class member claims, plaintiffs' counsel's legal fees, and settlement administration costs. The corporation would also commit to an aggregate increased expenditure of $150 million for data protection and related technology in 2022 and 2023.[82]

3.4 Conclusion

Finally, the chapter goes into the complex world of indirect personal data collecting in the telecommunications sector, highlighting the great influence of technical improvements on privacy rights. The chapter methodically investigates several aspects of indirect data collecting, including as metadata, location tracking, user behaviour analysis, and third-party data sharing, giving light on the multiple issues and ethical implications involved. The chapter emphasises the potential sensitivity and identifiability of metadata, highlighting its critical role in constructing user profiles. Furthermore, the topic expands to the emerging subject of behavioural analytics, recognizing its benefits while emphasising the crucial data privacy concerns it raises. Real-life examples of the consequences of poor data protection range from targeted advertising and profiling to data breaches and identity theft, emphasising the importance of strong legal frameworks and ethical considerations when navigating the complex landscape of data collection, usage, and its implications for individual privacy. The exploration of breaches, such as those experienced by Microsoft and Meta, serves as cautionary examples, emphasising the need and importance of stringent measures to safeguard data subject's against unauthorised access and malicious exploitation of personal data. It concludes by emphasising on the importance of privacy in the

[81] Hill M, " The biggest data breach fines, penalties, and settlements so far', CSO, 18 Septemeber 2023 https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html on 18 December 2023.

[82]Hill M, " The biggest data breach fines, penalties, and settlements so far', CSO, 18 Septemeber 2023 https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html on 18 December 2023.

digital environment, highlighting the importance of striking a careful balance between technical advancement and protecting individual privacy rights.

Chapter 4

Comparative Analysis

With the emergence of huge tech corporations, the platform economy, and the processing and storing of exabytes of data, the 21st century has become the century of big data and advanced information technology.[83] The increasing power of new technology and the fading clarity and agreement on privacy give rise to difficulties involving law, policy, and ethics.[84] Many of these conceptual arguments and difficulties are set in the context of interpretation and analysis of the GDPR, which was enacted by the EU in spring 2018 as the successor to the EU 1995 Directives and has far-reaching implications beyond the European Union's boundaries.[85] Recognizing that there are moral reasons for safeguarding personal data, data protection regulations are in existence in practically every country.[86] The essentially unifying moral concept underlying these rules is the requirement for informed prior consent or processing by the data subject.[87] In addition to getting consent, the processing of personal information requires that its purpose be identified, its use be limited, individuals be notified and given the opportunity to remedy inaccuracies, and the data holder be accountable to oversight authorities.[88] Since it is impossible to ensure compliance of all forms of data processing in all these sectors and applications with these regulations and laws in traditional ways, so-called privacy-enhancing technologies and identity management systems are projected to replace human oversight in many circumstances.[89] As a result, the global challenge we face in the twenty-first century in terms of privacy is to ensure that technology is designed to integrate privacy requirements into the infrastructure, software, architecture, and work processes in such a way that privacy violations are unlikely to occur.

---

[83]Hoven, Jeroen, Blaauw M, Pieters W, and Warnier M, 'Privacy and Information Technology', *The Stanford Encyclopedia of Philosophy*, 2020, https://plato.stanford.edu/entries/it-privacy/ on 13 December 2023.

[84] Hoven, Jeroen, Blaauw M, Pieters W, and Warnier M, 'Privacy and Information Technology.

[85] Hoven, Jeroen, Blaauw M, Pieters W, and Warnier M, 'Privacy and Information Technology.

[86] Hoven, Jeroen, Blaauw M, Pieters W, and Warnier M, 'Privacy and Information Technology.

[87] Hoven, Jeroen, Blaauw M, Pieters W, and Warnier M, 'Privacy and Information Technology.

[88]Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 on 13 December 2023.

[89] Gichaga EW, 'Right to privacy in the wake of mobile money transfers in Kenya: Is the data protection bill a step in the right direction?' Unpublished, Strathmore University, Nairobi, 2018, 22.

The rapid adoption of mobile money use in Africa raises concerns regarding the privacy and security of users, particularly in light of Financial Action Task Force recommendations requiring user transparency and the collection of transaction data. The transparency required of the now-financially-included—particularly in nations with weak adherence to the rule of law and limited privacy protections—leaves users vulnerable to abuse.[90] Over the last decade, mobile telephony has enjoyed phenomenal adoption rates across most of Africa. Since 2005, there has been a fivefold increase in the number of African mobile phone subscriptions resulting in 53.1 mobile phone subscriptions per 100 inhabitants in 2011 and has doubled since then.[91] While other areas of the world have adopted mobile phones to an even greater degree, the relative impact in Africa, where fixed telephone lines are available to less than 2 percent of the population, is perhaps greater than anywhere else. [92] As the primary means of communication for most Africans, mobile phones have become a source of significant economic growth and a platform for innovation. One of the most dynamic of these innovations has been mobile money, the use of mobile phones to purchase goods or services through funds connected to the user's account. Mobile money adoption has the potential to significantly benefit Africa, given the large number of existing mobile phone users. On a continent with too few banking options necessary for a dynamic and modern economy, mobile money has the potential to address long-existing gaps in African economies.[93]

This goes to show how the telecommunication industry in Africa keeps growing. With Kenya as one of the leading countries in this transition, the law should be able to keep pace with it.

With programs like the GDPR, the European Union (EU) has been setting the standard for data privacy regulation in recent years. Global companies who operate in the digital sphere as well as those within the EU are greatly impacted by these regulations. The GDPR, which was implemented

[90] Harris A, Goodman S & Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa', 8 *Washington Journal of Law, Technology & Art* 3, 2013, 1.

[91]Global ICT developments https://www.itu.int/ITU-D/ict/statistics/ict/ on 20 December 2023.

[92] Harris A, Goodman S & Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa', 246.

[93]'Mobile Money in Africa: Press 1 for Modernity',The Economist, 28 April 2012 http://www.economist.com/node/21553510 on 10 December 2023.

in 2016 by the EU, is the most recent example of a comprehensive data protection and privacy framework that has established new standards for global best practices. Expanding upon established tenets (such as the OECD Privacy Principles), it has emerged as a crucial point of reference for worldwide efforts in this domain. With some of the highest fines ever recorded, it is among the strictest data protection regulations in existence. Sweden and Canada, for example, drew inspiration from the GDPR when drafting their own data privacy legislation. This demonstrates how beneficial these laws are for both those who are affected by them and those who are not. This is why the EU was the most appropriate parallel to Kenya for this topic.

4.1 European Union

The European Union enacted its GDPR to protect the personal data of citizens and harmonise privacy policies across member states.[94] The regulation strengthened consumers' privacy rights and required app developers to ask customers' permission before they could use their data to target online ads or conduct other revenue-producing activities.[95] Developers also had to guarantee that customers could access, rectify, erase, and restrict the processing and portability of personal data.[96] The law was enacted in 2016 and implemented two years later. The GDPR is a law that established protections for privacy and security of personal data about individuals in the European Economic Area ("EEA")-based operations and certain non-EEA organisations that process personal data of individuals in the EEA.[97] It applies to the collection and use of personal information:

1. Through activities within the borders of EEA countries
2. That is related to offering goods and services to EEA residents, or

[94] Belsie L, 'Impacts of the European Union's Data Protection Regulations', National Bureau of Economic Research, 2022.

[95] Belsie L, 'Impacts of the European Union's Data Protection Regulations', National Bureau of Economic Research, 2022.

[96] Belsie L, 'Impacts of the European Union's Data Protection Regulations', National Bureau of Economic Research, 2022.

[97]The European Union (EU) General Data Protection Regulation (GDPR) https://www.hrpo.pitt.edu/european-union-eu-general-data-protection-regulation-gdpr on 10 December 2023.

3. That involves monitoring the behaviour of EEA residents.[98]

Just last year, the EU slapped Meta, the owner of Facebook, with a 1.2 billion euro fine, the largest in GDPR's history, for illegally transferring personal data from the EU to the US.[99] This goes to show that personal data is subject to some of the most stringent regulatory standards on the planet.

There are a number of countries outside of the EU that have implemented similar data protection laws.[100] Some of the countries include Switzerland, Egypt, Turkey, Nigeria, South Africa, and Kenya.[101] The country with the strictest data privacy laws related to the internet is Iceland.[102] Many people have referred to Iceland as Switzerland for data. It has incredibly strict privacy laws, and these laws were passed in 2000. Therefore, it has one of the oldest data privacy laws on the books as well. This law states that information can only be obtained for specific purposes. Furthermore, this information can only be collected if the user gives unambiguous, informed consent. Instead of asking people to opt out of having their information collected, they need to opt in to having their information collected. This is what makes Switzerland different from some of the other countries in the world. [103] On September 1, 2023 the revised Federal Data Protection Act (revFADP) entered into force. The revFADP aligns Swiss data protection law with the European GDPR and thus enables it to maintain a free flow of data between the EU and Switzerland.[104] While essentially equivalent in most respects, in part the revFADP also deviates from the GDPR and goes a step further in regulating data protection.

[98] The European Union (EU) General Data Protection Regulation (GDPR) https://www.hrpo.pitt.edu/european-union-eu-general-data-protection-regulation-gdpr on 10 December 2023.

[99]The Thin Line Between User Behavioral Analytics and Privacy Violation https://www.tripwire.com/state-of-security/thin-line-between-user-behavioral-analytics-and-privacy-violation on 10 December 2023.

[100]GDPR Countries 2024 https://www.gdpradvisor.co.uk/gdpr-countries on 24 December 2023.

[101]GDPR Countries 2024 https://www.gdpradvisor.co.uk/gdpr-countries on 24 December 2023.

[102]Data Privacy Laws by Country 2024 https://worldpopulationreview.com/country-rankings/data-privacy-laws-by-country on 15 Deceber 2023.

[103] Data Privacy Laws by Country 2024 https://worldpopulationreview.com/country-rankings/data-privacy-laws-by-country on 15 Deceber 2023.

[104]Meier K, 'A new Era for Data Protection in Switzerland – Are you ready?',EY Switzerland, 2023.

According to the GDPR, data processing is considered lawful only if specific conditions are met. These conditions include obtaining the data subject's consent for specific purposes,[105] processing is necessary for contractual obligations or pre-contractual steps,[106] compliance with legal obligations,[107] protection of vital interests,[108] performance of tasks in the public interest or official authority,[109] and pursuing the controller's or a third party's legitimate interests.[110] However, the legitimacy of processing for the controller's or a third party's interests is conditional on those interests not outweighing the data subject's fundamental rights and freedoms, particularly if the data subject is a minor. While being one of the more well-known legal bases for processing personal data, consent is only one of six bases mentioned in the GDPR.[111] The others are: contract, legal obligations, vital interests of the data subject, public interest and legitimate interest as stated in Article 6(1) of the GDPR.[112]

Focusing on the term "interests" we will look at vital interests, public interest and legitimate interests.

i) Vital interests

Article 6(1)(d) provides a lawful basis for processing where:

"processing is necessary in order to protect the vital interests of the data subject or of another natural person".[113]

Recital 46 provides some further guidance:

[105] Article 6(1)(a), General Data Protection Regulation, 2016/679.

[106] Article 6(1)(b), General Data Protection Regulation, 2016/679.

[107] Article 6(1)(c), General Data Protection Regulation, 2016/679.

[108] Article 6(1)(d), General Data Protection Regulation, 2016/679.

[109] Article 6(1)(e), General Data Protection Regulation, 2016/679.

[110] Article 6(1)(f), General Data Protection Regulation, 2016/679.

[111] Consent, General Data Protection Regulation, 2016/679.

[112] Article 6(1), General Data Protection Regulation, 2016/679.

[113] Article 6(1)(d), General Data Protection Regulation, 2016/679.

"The processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis…"[114]

It's clear from Recital 46 that vital interests are intended to cover only interests that are essential for someone's life. So this lawful basis is very limited in its scope, and generally only applies to matters of life and death.[115] It is likely to be particularly relevant when you need to use a person's personal data for emergency medical care, but they are unconscious or otherwise incapable of giving consent to the processing.[116] Article 9(2)(c)[117] specifies that special category data may be processed if it is required to protect someone's vital interests. However, this is only applicable if the data subject is physically or legally unable to provide consent. This means that express consent is preferable in many circumstances, and you cannot rely on vital interests for special category data (including health data) if the data subject refuses to consent, unless they are unable to do so.

ii) Public interest

Article 6(1)(e) gives you a lawful basis for processing where:

"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"[118]

[114] Recital 46, General Data Protection Regulation, 2016/679.

[115] Vital interests, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/vital-interests/#:~:text=another%20legal%20basis%E2%80%A6%E2%80%9D-,What%20are%20'vital%20interests'%3F,matters%20of%20life%20and%20death on 15 December 2023.

[116] Vital interests, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/vital-interests/#:~:text=another%20legal%20basis%E2%80%A6%E2%80%9D-,What%20are%20'vital%20interests'%3F,matters%20of%20life%20and%20death on 15 December 2023.

[117] Article 9(2)(c), General Data Protection Regulation, 2016/679.

[118] Article 6(1)(e), General Data Protection Regulation, 2016/679.

This can apply if you are either carrying out a specific task in the public interest which is laid down by law; or exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.[119] If you can show you are exercising official authority, including use of discretionary powers, there is no additional public interest test. However, you must be able to demonstrate that the processing is 'necessary' for that purpose. 'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You do not have a lawful basis for processing if there is another reasonable and less intrusive way to achieve the same result.[120]

iii) Legitimate interests

Article 6(1)(f) states:

"1.Processing shall be lawful only if and to the extent that at least one of the following applies:

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[121]

[119] Public task, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/public-task/#:~:text=What%20is%20the%20'public%20task'%20basis%3F,-Article%206(1&text=This%20can%20apply%20if%20you,is%20laid%20down%20by%20law on 15 December 2023.

[120] Public task, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/public-task/#:~:text=What%20is%20the%20'public%20task'%20basis%3F,-Article%206(1&text=This%20can%20apply%20if%20you,is%20laid%20down%20by%20law on 15 December 2023.

[121] Article 6(1)(f), General Data Protection Regulation, 2016/679.

Legitimate interests is different to the other lawful bases as it is not centred around a particular purpose (eg performing a contract with the individual, complying with a legal obligation, protecting vital interests or carrying out a public task), and it is not processing that the individual has specifically agreed to (consent).[122] Legitimate interests is more flexible and could in principle apply to any type of processing for any reasonable purpose. Because it could apply in a wide range of circumstances, it puts the onus on you to balance your legitimate interests and the necessity of processing the personal data against the interests, rights and freedoms of the individual taking into account the particular circumstances.[123] This is different to the other lawful bases, which presume that your interests and those of the individual are balanced.

The key elements of the legitimate interests provision can be broken down into a three-part test. Whilst a three-part test is not explicitly set out as such in the GDPR, the legitimate interests provision does incorporate three key elements.

1. Purpose test – is there a legitimate interest behind the processing?
2. Necessity test – is the processing necessary for that purpose?
3. Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms?

This concept of a three-part test for legitimate interests is not new. In fact the Court of Justice of the European Union confirmed this approach to legitimate interests in the Rigas case[124] in the

[122] What is the legitimate interests basis?, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/what-is-the-legitimate-interests-basis/#:~:text=Legitimate%20interests%20is%20different%20to,the%20individual%20has%20specifically%20agreed on 15 December 2023.

[123] What is the legitimate interests basis?, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/what-is-the-legitimate-interests-basis/#:~:text=Legitimate%20interests%20is%20different%20to,the%20individual%20has%20specifically%20agreed on 15 December 2023.

[124] Order Police Department of the Riga Region Administration of the State Police v Riga municipality SIA 'Rīgas satiksme' (2017), Supreme Court, Administrative Division, Latvia.

context of the Data Protection Directive,[125] which contained a very similar provision. This means that simply deciding that it is in your legitimate interests and proceeding with the data processing is insufficient. You must be able to pass all three portions of the test before proceeding with the process. Whilst any purpose could potentially be relevant, that purpose must be 'legitimate'. Anything illegitimate, unethical or unlawful is not a legitimate interest. For example, although marketing may in general be a legitimate purpose, sending spam emails in breach of electronic marketing rules is not legitimate.[126]

4.2 Kenya

The DPA of Kenya was enacted in November 2019. The purpose of the Act is to give effect to Article 31(c) and (d) of the Constitution that contains the right to privacy which is a fundamental human right.[127] The DPA 2019, has in many ways drawn from the GDPR of Europe. The act, as currently enacted, incorporates most of the fundamental features of a data protection law.[128] The frameworks and laws have developed mainly in response to technological advances which increase the collection, holding and dissemination of personal information as well as surveillance of people.[129] The Act imposes a number of obligations on data processors and data controllers in respect of the manner in which personal data is processed and sets out their duties to the data subjects.

As a rule, a data controller or data processor ought to collect personal data directly from the data subject.[130]

[125] Article 5, Data Protection Directive 95/46/EC.

[126] What is the legitimate interests basis?, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/what-is-the-legitimate-interests-basis/#:~:text=Legitimate%20interests%20is%20different%20to,the%20individual%20has%20specifically%20agreed on 15 December 2023.

[127] Kanji C and Njenga R, 'The Data Protection Act 2019 Kenya', A.B. Patel & Patel LLP, 2021.

[128] Kanji C and Njenga R, 'The Data Protection Act 2019 Kenya', A.B. Patel & Patel LLP, 2021.

[129] Kanji C and Njenga R, 'The Data Protection Act 2019 Kenya', A.B. Patel & Patel LLP, 2021.

[130] Section 28(1), Data Protection Act (Act No 24 of 2019).

Notwithstanding the general rule on collection of data directly, the Act provides that personal data may be collected indirectly where the:- [131]

i) data is contained in a public record, or the data subject has deliberately made the data public;
ii)data subject or their duly appointed guardian has consented to the collection from another source;
iii)collection from another source would not prejudice the interests of the data subject;
iv) collection of data from another source is necessary for the-

a) prevention, detection, investigation, prosecution and punishment of crime;
b) enforcement of a law which imposes a pecuniary penalty; or
c) protection of the interests of the data subject or another person.

Since the Data Protection Commissioner's (DPC) appointment on 16 November 2020, significant efforts have been made in developing regulations for the implementation of the Act. They include:-

i) Data Protection (Compliance & Enforcement) Regulation, 2021 – sets out the complaints handling procedures and enforcement mechanisms in the event of non-compliance with the provisions of the Act;[132]

ii) Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021 – provides for the registration of data controllers and data processors with the DPC. The threshold for mandatory registration is also set out under these regulations;[133] and

iii) Data Protection (General) Regulations, 2021 – elaborates in more detail the rights of data subjects, restrictions on commercial use of personal data, duties and obligations of data controllers and data processors, elements of implementing data protection by design

[131] Section 28(2), Data Protection Act (Act No 24 of 2019).

[132]The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021 (Legal Notice No 264).

[133] Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021 (Legal Notice No 265).

or default, notification of personal data breaches, transfer of personal data outside Kenya, conduct of data protection impact assessment and other general provisions. [134]

The Data Protection (General) Regulations further elaborates on the different basis of collecting personal data. Section 6 focuses on the mode of collecting data.

6. (1) Pursuant to section 28(2) of the Act, a data controller or data processor may collect personal data indirectly from
(a) any person other than the data subject;
(b) publications or databases;
(c) surveillance cameras, where an individual is identifiable or reasonably identifiable;
(d) information associated with web browsing; or
(*e) biometric technology, including voice or facial recognition*[135]

(3) Where a data controller or data processor collects personal data indirectly, the data controller or data processor shall within fourteen days inform the data subject of the collection[136]

In Kenya, the recent DPA of 2019 has been greatly influenced by the GDPR which already allows it to take advantage of the many years of development that the GDPR underwent.[137] The DPA passed in November 2019 is an important breakthrough but one must not settle for surface level protection simply because one lacked protection in the first place. The act and its consequences must be effective. Given that Kenya has for the most part uprooted the EU's GDPR, the question is whether the DPA is sufficient or must it undergo further specialisation and importantly, localization[138]

[134] Data Protection (General) Regulations, 2021(Legal Notice No 263).

[135] Section 6(1), Data Protection (General) Regulations, 2021(Legal Notice No 263)

[136] Section 6(3), Data Protection (General) Regulations, 2021(Legal Notice No 263)

[137]Munir A, 'The Consent Model Under the Data Protection Act; Introducing Complementary Provisions to Enhance Protection', Unpublished LLB Dissertation, Strathmore University Law School, 2021, vi.

[138]Munir A, 'The Consent Model Under the Data Protection Act; Introducing Complementary Provisions to Enhance Protection', Unpublished LLB Dissertation, Strathmore University Law School, 2021, 1.

The Kenya Information and Communications Act, 1998 (KICA) came into effect in February 1999.[139] KICA is the overarching law for the information and communications technology industry in Kenya. It outlines the requirements and compliance standards by which licensed information and communication service providers who are data collectors and controllers must abide.[140] The provisions of KICA are enforced through its regulations, including, the Kenya Information and Communications (Consumer Protection) Regulations of 2010 ('the Kenya Information and Communications Regulations') and the Kenya Information and Communications Act (Registration of SIM Cards) Regulations 2015 ('the SIM Cards Regulations'). KICA applies to telecommunication service providers that have been granted an operation licence from the Communications Authority ('CA'). Licensed providers include mobile network operators, content service providers, applications service providers, submarine cable landing rights-holders, and international gateway systems service providers.[141]

Taking a look at Safricom's Data Privacy Statement which mirrors most of the telecommunication companies, one can deduce that privacy is important to them. However, the ambiguity also reflects here. For instance, under collection of information, the first sub clause reads
We collect your personal information with your knowledge and consent when you do any of the following (please note that this list is not exhaustive):[142]

The policy goes ahead and lists eight ways in which they collect data from customers, suppliers, agents, merchants, dealers and all visitors frequenting any Safaricom premises.[143] However, as earlier preempted, the list is not exhaustive. This seems to be very questionable as Safaricom would be able to give out all the different ways in which data is collected. In a modern society with

[139] Kenya Information and Communications Act (No 2 of 1998).

[140] Kenya Information and Communications Act (No 2 of 1998).

[141] Mweu N, 'Kenya - Data Protection Overview', OneTrust DataGuidance, 2023.

[142] Section 3.1.1, Safaricom Data Privacy Statement, 2019.

[143] Section 1.0, Safaricom Data Privacy Statement, 2019.

technology at arms length, it would not be a difficult task to take note of every method of collecting data. It further discusses what type of information is collected.[144] The clause begins with *The information we collect and store about you includes but is not limited to the following:*[145]

The policy outlines sixteen different types of data collected including call data records, your approximate location and your preferences. The privacy policy also provides that Safaricom shall have the right to monitor user account usage and may disclose personal information to local law enforcement or investigative agencies or any competent regulatory or governmental agencies to assist in the prevention, detection or prosecution of money laundering activities, fraud or other criminal activities.[146] This leaves the personal information of a data subject vulnerable to governmental seizure in the name of 'prevention, detection or prosecution of money laundering activities, fraud or other criminal activities' .

From this, one can deduce that due to the ambiguity in the law, telecommunication companies are able to get away with not correctly informing their customers. Moreover, it shows that data subjects are not in charge of who gets their personal data and how it is collected. Instead, the act should be more detailed in describing the various methods for indirectly collecting data. By defining the types of interests to be considered while collecting data without the data subject's awareness, personal data is protected and misuse is eliminated. Furthermore, ensuring that there is a particular penalty for indirectly collecting data in situations other than those described would ensure that unlawful data collection has direct consequences.

Also, these two provisions will hopefully ensure design and enforcement of data privacy and security rules contained in the Terms and Conditions (T&Cs) and privacy policies of the various telecommunication companies. This requires some level of coordination between supervisory and regulatory authorities, as telecommunications is a very crucial area of data right now. If the current privacy provisions of the various T &Cs of telecommunication platforms could be amended to

[144] Section 3.2, Safaricom Data Privacy Statement, 2019.

[145] Section 3.2, Safaricom Data Privacy Statement, 2019.

[146] Section 4.0, Safaricom Data Privacy Statement, 2019.

include rules as provided above, then much needed clarity would be available to the entities handling customer data.

4.3 Conclusion

There are major similarities and differences between the European Union's GDPR framework and Kenya's Data Protection Act (DPA). Both legislative frameworks seek to preserve individuals' privacy rights and govern the processing of personal information. The GDPR, implemented in 2016, establishes comprehensive rules that apply across all EU member states and beyond, emphasising concepts like informed consent, purpose limitation, and data subject rights. Kenya's DPA, enacted in 2019, is inspired by the GDPR but customised to the Kenyan context, reflecting the country's unique legal, cultural, and technological backdrop. While both laws share fundamental ideas, such as transparency and accountability for data processors, they differ in scope, enforcement procedures, and specific clauses.

When comparing the European Union's GDPR to Kenya's Data Protection Act (DPA) pertaining to the indirect collection of personal data, differences in procedure and specificity emerge. The GDPR's rigorous regulations cover indirect collection of data extensively. It highlights the importance of informed consent and transparency, requiring data controllers to openly state the reasons for data gathering and acquire approval from individuals. Furthermore, the GDPR places tight restrictions on the collecting of personal data from third-party sources, highlighting the importance of legitimate and justified reasons for such operations. In contrast, Kenya's DPA, which draws influence from the GDPR, varies in its detail addressing indirect data gathering. While the DPA recognizes that indirect collection may be lawful in certain instances, such as when data is contained in public records or consent is received from the data subject, it does not provide comprehensive rules or constraints on the scope and circumstances of indirect data collection. This mismatch may provide ambiguity and potential vulnerabilities in data protection policies, raising questions about the effectiveness of safeguards for individuals' privacy rights in Kenya's legislative framework. Thus, while both legislative frameworks recognize the necessity of controlling indirect data gathering, the GDPR's detailed rules provide better clarity and robustness than Kenya's DPA.

In summary, Kenyan laws do not delve as deep into specifics as EU law does. This leaves room for exploitation by organisations and even the government. In an attempt to copy the GDPR, the lawmakers forgot to localise the law in a way that catered for the specifics of this country. Especially as a third world country. Therefore, regulators and the telecommunication sector in Kenya, need to work together to understand security concerns and maintain the integrity of customer data, just like in Europe. In both, the telecommunication sectors have developed various systems to protect customer privacy with Europe doing a better job then Kenya. This however doesn't eliminate the need to have the DPA amended as such a law will bring with it the much needed clarity on who is responsible if data associated with the telecommunication sector falls into the wrong-hands.

Chapter 5

Conclusion and Recommendations

5.1 Introduction

The world of today places great importance on the information derived from persons all over the globe. That data is one with the individual and thus should be accorded the proper rights as well as rigid protection required. Privacy plays a major role as data can be used to identify and as well as exploit individuals and therefore further emphasises the need for legislation that greatly protects the data subject. However, data is still necessary for an increasing number of activities and finding a balance is an ongoing struggle in many parts of the world.

We would be hard-pressed to find another industry with as much easy access to a wealth of user data as telecom. Traffic, user behaviour, location, and more are easily attainable for the provider. With this information, providers can analyse which services their users use, how long they use them and when.

The findings in this study sought majorly to answer the question of regulation of personal information in the telecommunications industry. This question mostly arose due to the nature of telecommunications. Telecommunication requires personal information so as to enable the execution of its transactions. It is therefore apparent that there is a need for regulations on how this information is collected, used and distributed by these entities in a manner so as to ensure that consumers' right to privacy is not violated.

This chapter will proceed to propose recommendations that seek to enhance the regulation of the processing of personal information by telecommunication entities

5.2 Summary findings

The focal point of chapter one was to explore the evolving landscape of the collection of personal data within the telecommunication sector in Kenya and the implications it has on privacy rights. The growth of technology has affected the rise in the collection of personal data with the

telecommunications industry being one of the leaders. The main inquiry being whether the Data Protection Act should be refined to provide more clarity on the category of interests, especially concerning the right to privacy.

Chapter two unveils a theoretical framework rooted in Surveillance Capitalism, Communication Privacy Management, and Westin's Theory of Privacy. These theories provide important insights into the complexities of personal data collection, highlighting power imbalances,the data subject's claim to control information dissemination, and dynamic privacy boundaries.

Chapter three scrutinises indirect personal data collection in the telecommunications sector, revealing its delicate nature and the profound impact of technical advancements on privacy rights. It delves into metadata, location tracking, user behaviour analysis, and third-party data sharing, illuminating ethical issues. Emphasis is placed on metadata's sensitivity, its role in user profiling, and the rise of behavioural analytics, acknowledging benefits and privacy concerns. The conclusion underscores the delicate balance between technical progress and safeguarding individual privacy rights in the digital realm.

Chapter four highlights a comparative analysis of the European Union laws and the Kenyan laws. The main aim was to see the different things that the Kenyan laws can borrow from the GDPR. The main conclusion shows that the GDPR gives a more specific rationale for the collection of personal data. The chapter emphasises the significance of collaboration between the regulators and telecommunications sector to ensure the security and privacy of consumer data as well as the importance of localising the act.

5.3 Conclusion

The premise that the telecommunications sector handles a large amount of personal information and hence requires regulation of personal information in this regard has been demonstrated multiple times. The nature of telecommunications relies on personal information to carry out operations and boost efficiency. However, if the processing of personal information is not regulated, consumers risk having their privacy invaded.

The idea that there are no broad laws governing the handling of personal information is incorrect. This is because the DPA of 2019 was established and it intends to govern the processing of personal information by companies that are exposed to this information. One of the areas the Act regulates due to its nature is telecommunications.

5.4 Recommendations

In order for Kenya to adequately regulate the processing of personal information, it ought to reform its Data Protection legislations;

a. The amendment of section 28 (2)(e) of the DPA that provides that entities that process personal data can indirectly access a data subject's personal data as long as the collection would not prejudice the data subject's interests. This allows for abuse and is troublesome because it makes personal data widely available, and a defence against entities would be a lack of specificity. Instead, the act should say "vital interests" to ensure that this is only done when absolutely essential.

b. The modification of section 28 (2)(f)(iii) of the DPA, which states that organizations that handle personal data may obtain a data subject's information indirectly if the information is gathered to safeguard the interests of the data subject or another individual. The lack of clarity as to what interests are being protected leaves room for abuse. Instead, it should read "vital interests" to ensure it only occurs when necessary.

c. The addition of the data subjects' right to recompense and an effective remedy under Section 26 of the DPA. This ensures that data subjects receive compensation for any breaches of personal data by organizations who process their information.

d. The inclusion of a specific penalty for indirectly collecting personal data in instances other than the ones provided. This will ensure that data subjects are protected from a violation of their right to privacy.

e. The amendment of section 6(3) of the Data Protection (General) Regulations that provides that entities that collect personal data indirectly should notify the data subject within fourteen days. This time frame is too long for a data subject to not be informed that their personal data has been collected. Instead, the data subject should be notified immediately to ensure that the data subject is in control of their personal data.

f. The deletion of the DPA's section 28(2)(a), which allowed companies processing personal data to get indirect access to a data subject's personal information that was in a public record. This implies that a data subject has automatically consented to the ongoing processing of their personal information, which is held in public records. This provision is problematic because it makes personal data widely accessible to companies who may take advantage of the possibility to collect and aggregate a data subject's personal information in order to create an individual profile.

g. The modification of the DPA's section 28(2)(b), which states that organizations processing personal data may have indirect access to a data subject's personal information that they knowingly made public. This is because the term 'deliberately' should not be used as a justification for collecting data subjects' personal information. This provision should take a more restrictive approach and compel businesses to notify data subjects that their data is being processed.

Bibliography

1. Books

Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019.

Westin A, *Privacy and Freedom*, Atheneum, New York, 1967.

Petronio S, Caughlin JP, *Communication Privacy Management Theory*, Sage Publications, Mahwah, 2006.

Button M and Cross C, *Cyber Frauds, Scams, and Their Victims*, 1 ed, Routledge, London, 2017.

2. Chapter in Book

Tzanou M, 'Data Protection as a Fundamental Right Next to Privacy? "Reconstructing" a Not SoNewRight' in Binder C (eds) *Elgar Encyclopedia of Human Rights*, Elgar Encyclopedia, UK, 2022.

Dunnage J,' Policing and surveillance',in Corner P and Lim J (eds) *The Palgrave Handbook of Mass Dictatorship*, Palgrave Macmillian, Ohio, 2016.

3. Hard Copy Journals

Harris A, Goodman S & Traynor P, 'Privacy and Security Concerns Associated with Mobile Money Applications in Africa', 8 *Washington Journal of Law, Technology & Art* 3, 2013.

Mbogo M, 'The Impact of Mobile Payments on the Success and Growth of Micro-Business: The Case of M-Pesa in Kenya' 2 *The Journal of Language, Technology & Entrepreneurship in Africa* 1, 2010.

Feldstein S, 'The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression' 30 *Journal of Democracy* 1, 2019.

Tsohou A and Kosta E,'Enabling valid informed consent for location tracking through privacy awareness of users: A process theory' 33 *Computer Law & Security Review* 4, 2017.

Königs P, 'Government Surveillance, Privacy, and Legitimacy' 35 *Philosophy and Technology* 8, 2022.

4. Online Journals

Hoven, Jeroen, Blaauw M, Pieters W, and Warnier M, 'Privacy and Information Technology', The Stanford Encyclopedia of Philosophy, 2020, https://plato.stanford.edu/entries/it-privacy/

5. Self-Published Articles

Austin L, 'Rereading Westin' Theoretical Inquiries in Law, Forthcoming, 2018.

Belsie L, 'Impacts of the European Union's Data Protection Regulations', National Bureau of Economic Research, 2022.

Meier K, 'A new Era for Data Protection in Switzerland – Are you ready?',EY Switzerland, 2023.

Kanji C and Njenga R, 'The Data Protection Act 2019 Kenya', A.B. Patel & Patel LLP, 2021.

Mweu N, 'Kenya - Data Protection Overview', OneTrust DataGuidance, 2023.

Data protection is the process of safeguarding important information from corruption, disruption and/or loss. Juneh H, 'Data Protection and Data Security', Academia Edu, 2018.

Dutt D, ' Behavioral Analytics: A Privacy-First Approach', Forbes, 2020.

Grischina A, 'Data Analytics in the Telecom Industry: Use Cases, Challenges, and Trends', Softteco, 2023.

Akindele L, ' Commercialisation of data in the telecommunications sector', PwC, 2020.

Minch R, ' Privacy Issues in Location-Aware Mobile Devices', Hawaii International Conference on System Sciences, Hawaii, 2004.

Jarameel K and Kibet B, 'Defining Data Protection in Kenya: Challenges, Perspectives and Opportunities', SSRN, 2022.

Satter R, 'U.S. court: Mass surveillance program exposed by Snowden was illegal', Reuters, 2020.

Danao M and Aditham K, 'What Is A Data Breach? Definition, Examples & Prevention', Forbes Advisor, 2023.

Belsie L, 'Impacts of the European Union's Data Protection Regulations', National Bureau of Economic Research, 2022.

6. Legislations

General Data Protection Regulation.

Data Protection Act of the United Kingdom, 2018.

General Data Protection Regulation, 2016/679.

Constitution of Kenya (2010).

Data Protection (General) Regulations, 2021(Legal Notice No 263).

Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021 (Legal Notice No 265).

The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021 (Legal Notice No 264).

Data Protection Act (No 24 of 2019).

Safaricom Data Privacy Statement, 2019.

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

Data Protection Directive 95/46/EC.

Revised Federal Data Protection Act of Switzerland, 2023.

7. Cases

Order Police Department of the Riga Region Administration of the State Police v Riga municipality SIA 'Rīgas satiksme' (2017), Supreme Court, Administrative Division, Latvia.

Safaricom PLC v Simon Billy Kinuthia & 2 others (2021) eKLR.

Joshua Kiprop Kisorio v Safaricom Plc & 4 others; Abdinajib Adan Muhumed (Interested Party) (2021) eKLR.

Olmstead v United States (1938), The Supreme Court of the United States.

Roe v Wade (1973), The Supreme Court of the United States.

Riley v California (2014), The Supreme Court of the United States.

8. Dissertations and Theses

Gichaga EW, ‘Right to privacy in the wake of mobile money transfers in Kenya: Is the data protection bill a step in the right direction?’ Unpublished, Strathmore University, Nairobi, 2018.

Munir A, ‘The Consent Model Under the Data Protection Act; Introducing Complimentary Provisions to Enhance Protection’, Published LLB Dissertation, Strathmore University Law School, 2021.

Kinyanjui AW, ‘Data protection as a human right: Balancing the right to privacy and national security in Kenya’ Unpublished, University of Nairobi, Nairobi, 2017.

Abdulrauf L, 'The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa', Unpublished, University Of Pretoria, Pretoria, 2015.

Sissing S, 'A criminological exploration of cyber stalking in South Africa', Unpublished, University of South Africa, Pretoria, 2013.

Nyemba C, 'Right to Data Privacy in the Digital Era Critical Assessment of Malawi's Data Privacy Protection Regime', Published, University of Pretoria, Pretoria, 2018/2019.

9. Newspapers

Muiruri K, 'Over 11 million SIM cards Set For Deactivation on Registration Deadline', Citizen Digital, 14 October 2022 -<https://www.citizen.digital/business/over-11-million-sim-cards-set-for-deactivation-on-registration-deadline-n307433>- on 2 January 2023.

'Mobile Money in Africa: Press 1 for Modernity',The Economist, 28 April 2012 http://www.economist.com/node/21553510

10. Internet Sources

Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Global ICT developments https://www.itu.int/ITU-D/ict/statistics/ict/

GDPR Countries 2024 https://www.gdpradvisor.co.uk/gdpr-countries

The Thin Line Between User Behavioral Analytics and Privacy Violation https://www.tripwire.com/state-of-security/thin-line-between-user-behavioral-analytics-and-privacy-violation

The European Union (EU) General Data Protection Regulation (GDPR) https://www.hrpo.pitt.edu/european-union-eu-general-data-protection-regulation-gdpr

Data Privacy Laws by Country 2024 https://worldpopulationreview.com/country-rankings/data-privacy-laws-by-country

Vital interests, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/vital-interests/#:~:text=another%20legal%20basis%E2%80%A6%E2%80%9D-,What%20are%20'vital%20interests'%3F,matters%20of%20life%20and%20death

Public task, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/public-task/#:~:text=What%20is%20the%20'public%20task'%20basis%3F,-Article%206(1&text=This%20can%20apply%20if%20you,is%20laid%20down%20by%20law

'The importance of data security for enterprises', Africa Telecom Review, 10 March 2022 -<https://www.telecomreviewafrica.com/en/articles/features/2701-the-importance-of-data-security-for-enterprises>-

'What is Metadata?', GSMA Association, https://www.gsma.com/publicpolicy/metadata

'Is metadata personal data?', Atlaw, 30 November 2022, https://www.altlaw.co.uk/blog/is-metadata-personal-data

'Metadata and Privacy: A Technical and Legal Overview', Office of the Privacy Commissioner of Canada, October 2014, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/

Breaker- Rolfe J, 'The Thin Line Between User Behavioral Analytics and Privacy Violation', Fortra, 10 July 2023, https://www.tripwire.com/state-of-security/thin-line-between-user-behavioral-analytics-and-privacy-violation

'Understanding Privacy Violations through Metadata Analysis in Communication', Utilities One, 22 November 2023, https://utilitiesone.com/understanding-privacy-violations-through-metadata-analysis-in-communication

Privacy issues in Location-Aware Mobile Devices https://ics.uci.edu/~ics215/papers/privacy-issues.pdf

Understanding Privacy Violations through Metadata Analysis in Communication', Utilities One, 22 November 2023, https://utilitiesone.com/understanding-privacy-violations-through-metadata-analysis-in-communication

'Mobile Privacy and Big Data Analytics',
https://www.gsma.com/publicpolicy/resources/mobile-privacy-big-data-analytics

https://www.aclu.org/issues/privacy-technology

https://rainmaker.co.in/blog/view/a6bf5b46-ab33-47c2-bc07-2ed66c006892/the-price-of-personalization-how-targeted-advertising-breaches-data-privacy-and-challenges-the-gdprs-shield

Hill M, " The biggest data breach fines, penalties, and settlements so far', CSO, 18 Septemeber 2023 https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html

Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Global ICT developments https://www.itu.int/ITU-D/ict/statistics/ict/

The European Union (EU) General Data Protection Regulation (GDPR) https://www.hrpo.pitt.edu/european-union-eu-general-data-protection-regulation-gdpr

The Thin Line Between User Behavioral Analytics and Privacy Violation https://www.tripwire.com/state-of-security/thin-line-between-user-behavioral-analytics-and-privacy-violation

GDPR Countries 2024 https://www.gdpradvisor.co.uk/gdpr-countries

Data Privacy Laws by Country 2024 https://worldpopulationreview.com/country-rankings/data-privacy-laws-by-country

What is the legitimate interests basis?, Information Commissioner's Office, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/what-is-the-legitimate-interests-basis/#:~:text=Legitimate%20interests%20is%20different%20to,the%20individual%20has%20specifically%20agreed