The Consent Model Under the Data Protection Act; Introducing Complimentary Provisions to Enhance Protection.

By;

Munir Abdikadir Hussein Mohamed

90351

Strathmore University Law School.

Dissertation Submitted in Partial Fulfillment of the Requirements of the Bachelor of Laws Degree, Strathmore University Law School

SLS 4141 & SLS 4257

Prepared Under the Guidance and Supervision Of

Dr. Isaac Rutenberg

Word Count (9,839)

Declaration;

I, Munir Abdikadir Hussein, 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 and/or diploma. Other works cited or referred to herein are accordingly acknowledged.

Signed: _____

Date: _____

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

Signed: _____

Date: _____

Dr. Isaac Rutenberg

Acknowledgment;

Firstly, I would like to express my gratitude to my supervisor, Dr. Ruternberg. I greatly appreciate all the professional support and academic guidance provided by him during dissertation.

Secondly, I would also like to acknowledge and thank my father for taking keen interest in my topic and willing to engage me in conversation around the topic.

Thirdly, I would like to thank my mother for always being supportive during me my dissertation and throughout my degree.

Most importantly, I praise and thank Allah SWT for His greatness and for giving me the strength and courage to complete this dissertation.

List of Abbreviations

Commission Nationale De L'informatique Et Des Libertés	CNIL
Data Protection Act	DPA
European Union	EU
General Data Protection Regulation	GDPR
National Integrated Identity Management System	NIIMS
Personal Data Protection Bill	PDP
United Nations Economic and Social Council ECOSOC	UN
United States	US

List of Legal Instruments

- Kenyan Constitution 2010
- Data Protection Act 2019
- General Data Protection Rules, 2018
- Personal Data Protection Bill, 2019
- Charter of Fundamental Rights of the European Union
- Universal Declaration of Human Rights

List of Cases

- *Robert K. Ayisi v Kenya Revenue Authority & another* [2018] eKLR
- *Kenya Human Rights Commission v Communications Authority of Kenya & 4 others* [2018] eKLR
- *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties)* [2020] eKLR
- *Google Inc. v Commission nationale de l'informatique et des libertés* (CNIL)

Table of Contents

Abstract

Individual data is a valuable commodity. 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 emphasizes 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. The concept of consent has been included in various jurisdictions to place control over data in the data subjects' hands and it is an effective tool in avoiding exploitation. European data protection laws are often considered the hallmark of robust and efficient safeguards for data. Legislation in Europe, specifically the GDPR, has influenced laws around the globe. In Kenya, the recent Data Protection Act 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.

However, the same standards of consent required for European citizens (the main target of the GDPR) has been drafted into the Kenyan DPA. In light of this, the study dissects the requirements of consent under the DPA aiming to highlight the difficulty in *solely* relying on this consent model. The study finds that the consent model is falling short of properly protecting data subjects in Kenya. This is because exclusively relying on the consent model while failing to take into account the cultural and educational differences between the EU and Kenya greatly affects the effectiveness of the model. To remedy this, the study proposes a look at two solutions being employed in India that serve to compliment the model. Namely, the appointment of learned & certified data intermediaries that bridge the knowledge gap between the data subject and the data collector in addition to the introduction of a fiduciary duty (akin to that imposed on bankers and doctors) into the law

CHAPTER 1; Introduction to The Study

1.1 Introduction;

Privacy and protection go hand in hand, privacy is a right enshrined in multiple spheres of legislation (the constitution provides for the right to privacy) and as such is to be protected by governments.[1] The free flow of personal data as a tradable commodity has become an important part of the global economy. With Kenya's growing exposure and increased interaction with the world at large, it is critical to safeguard the citizen's personal data.[2] International frameworks in conjunction with strong domestic legislation are crucial stepping stones for a further reaching a protection scheme that will aid Kenya now and in years to come. Especially with the increased interest in the country as an entry point into the African market.[3] The Data Protection Act (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 General Data Protection Regulation (GDPR), the question is whether the data protection act (DPA) is sufficient or must it undergo further specialization and importantly, localization?

The DPA has come into force in order to provide centralized legislation regarding data protection in Kenya. It has established the office of the data commissioner who is tasked with overseeing the implementation of the act as well as exercising an oversight role regarding the processing of data.[4] ? Personal data is a topic that cuts through multiple spheres from human rights concerns to property rights to cybercrime. With the ongoing COVID-19 pandemic, potential breaches in data rights by governments seeking to encroach on privacy behind the shield of "public safety" are more and more likely.[5] Safe guarding it would not only be in the

[1] Article 31, Constitution of Kenya 2010.

[2] Walters, Trakman, and Zeller, *Data Protection Law A Comparative Analysis of Asia-Pacific and European Approaches*. Preface; vii *Accessed on 18th March 2020.*

[3] "Amazon Rollout of Cloud Computing Unit in Nairobi Set to Spur East African Market - Business Daily." https://www.businessdailyafrica.com/corporate/tech/Nairobi--Amazon-Web-Services/4258474-5348692-ll5ejz/index.html

[4] Section 8, The Data Protection Act 2019

[5] "Privacy, Data Protection and the Coronavirus - Mugambi Laibuta." https://www.laibuta.com/human-rights/privacy-data-protection-and-the-coronavirus/

best commercial and socio-political interests of the government but would be a practice in line with the spirit of the constitution.

1.2 Statement of Problem;

As highlighted earlier, data is precious. In its nature, it is the subject matter for privacy, ergo the necessity protection. It can be argued that Kenya was very late in implementing an act of parliament relating to individual data. This is especially alarming owing to the fact that there had already been multiple illustrations globally on how individual data can and is exploited and abused by governments, companies and individuals alike. Ideally, a data subject should be aware of who has their data, how it was collected and what it's being used for. However, whether or not that is the reality is a different question. An example would be the texts people receive from fast food chains or even the government or even the NIIMS system being rolled out in our country unbeknownst to many as well as its safeguards.[6] Internationally the best example would be Edward Snowden's exposé on the United States violation of data privacy in the early 2010s.[7]

The gap between the ideal and the reality is not as wide, having been shortened with the coming into force of The Data Protection Act. However, we must strive to close the gap totally. The Act has taken many crucially steps, owing to it being heavily inspired by the EU's General Data Protection Regulation (arguably the most comprehensive and well-developed piece of legislation in the field of data protection). Steps still need to be taken in order to domesticate the Act and facilitate for its effectiveness in Kenya. Revisiting the standards as well as provisions relating to consent will further enhance protection.

1.3 Justification/Rationale;

The reason this particular study should be carried out is illustrated through these two (2) overlapping categories:

[6] Article19, Kenya: Digital identity regulations must satisfy constitutional requirements https://www.article19.org/resources/kenya-digital-identity-regulations-must-satisfy-constitutional requirements/
[7] "Edward Snowden: Leaks That Exposed US Spy Programme - BBC News." https://www.bbc.com/news/world-us-canada-23123964

- **Privacy**; Data protection is used as a tool to also protect privacy.[8] Individual data (which may be anonymized) can be identified with or without consent and thus can infringe on the individual's right to privacy as it leads to identification of the individual. By having stringent and strong mechanisms in place to protect data, it becomes possible to secure the individual's right to privacy. If not addressed, the individual's privacy is threatened and can be overpowered by loopholes in the system. Identification of these problems is the first step to their resolution. Privacy is a fundamental right both domestically and internationally, meaning that it should be priceless (no monetary or other such compromise should be made in order to protect it) and is inalienable; meaning that even if an individual wishes to waiver such rights, it should not be allowed.[9]
- **Exploitation**; The Chinese, already accustomed to massive privacy infringements in China, are setting up bases of operation in Kenya as is the case with other international technology firms that are seeking to capitalize on new markets.[10] If any structural weaknesses are present in our protection mechanisms, then they shall be exploited by any incoming parties. The Kenyan government has previously reported that internal corruption can pose a threat to the sanctity of dealings in the country and it can be argued that data can similarly be exploited.[11] Bringing such problems to light is a crucial first step in addressing and solving them.

1.4 Significance of Study;

The study seeks to root out the shortcomings of the proposed data protection mechanisms specifically focusing on the standards of consent; the actualization of the concept of consent in the law and determine its ability to protect. This particular gap in the legislative framework needs to be addressed because it can be magnified by the simple fact that the legislative integrity of Kenya isn't on the same level of our European and Western counterparts. To that

[8] De Hert p, Gutwirth S, (2006) Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power, in Claes E, Duff A, Gutwirth S, Privacy and the Criminal Law, Antwerp-Oxford, Intersentia, pp. 61–104.

[9] Bergkamp, "EU Data Protection Policy. The privacy fallacy: adverse effects of Europe's data protection policy in an information-driven economy 2002. https://www.huntonak.com/images/content/3/2/v3/3292/Privacy-fallacy.pdf

[10] "Amazon Rollout of Cloud Computing Unit in Nairobi Set to Spur East African Market - Business Daily." https://www.businessdailyafrica.com/corporate/tech/Nairobi--Amazon-Web-Services/4258474-5348692-ll5ejz/index.html

[11] Ethics and Anti-corruption commission, EACC Research Report No. 6, Nairobi, 2018.

effect, understanding the problems will not only help the common citizen understand what's at risk for them but help policy makers and enforcers protect the citizens from exploitation. This will serve to uphold the constitutional rights of individuals and avoid instances of abuse of power by governmental bodies and officials as in the case *Robert K. Ayisi v Kenya Revenue Authority & another*.[12] The results of research should aid policy makers in addressing any apparent shortfall and help them re-address consent under the DPA as well as serve as a reminder for the common citizen as to how precious their data is.

1.5 Aims and Objectives:

Aims;

The study aims to assess the potential effects of the current standard of consent as well as aiming to provide appropriate and applicable solutions to resolve any problems uncovered regarding consent.

Objectives;

The study aims to identify shortcomings of the act as a whole. Secondly, to review the requirements and the standard of consent. Thirdly, to deeply analyze whether or not the standard can be considered to be substantially fair as well as adequately guaranteeing privacy and data rights. Finally, find and suggest appropriate solutions to the raised concerns.

1.6 Research Questions;

1. How adequate is the Data Protection Act safeguarding the right to privacy? Specifically referring to concept of consent as a means of securing privacy rights.
2. Do certain conditions for consent under the DPA hinder individual data protection?
3. Does the law adhere to the right to privacy enshrined in the constitution?
4. Have other external factors such as education and culture affected personal agency regarding individual data?

1.7 Conceptual Framework

The concept of privacy was for a long time thought to only entail situations encompassing the physical or mental environment of an individual. Data protection was seemingly a consequence

[12] [2018] eKLR PETITION NO. 412 OF 2016

of privacy protection. Meaning that that protection of an individual's data was already catered for in the grand scheme of privacy thus requiring no separation of the two concepts. However, it is necessary that a distinction be made between the concept of privacy and data protection; Data protection is specifically related to the legal rules that regulate to which extent and under which conditions information related to individual physical persons may be used.[13] In understanding the distinction and similarly accepting their inter-relation, it would allow for policy on data protection to be tailor made to tackling issues of individual data protection without being hindered by the generality of protecting privacy as a whole, the devil is in the detail.

To further the point, the concept of privacy is one present in all jurisdictions around the world and respected/catered for in a majority of them, privacy is well established but data protection as an individual area of law is not yet as fleshed out and developed. In an age where the use of the internet and digital technologies have brought about social and economic benefits, to societies and individuals alike, it would be in our best interest to give due respect to the protection of individual data that drives such benefits.[14] Following the distinction and acceptance of their inter-relation, proper legislation can be utilized to its greatest extent.

1.8 Hypothesis;

The research is based on the following hypothesis: *"The Data Protection Act of 2019 has failed to compensate for the differences between Kenya and the EU and therefore is not as water tight regarding the concept of consent"*

1.9 Research Methodology:

This research paper will predominantly use doctrinal "black letter law" legal research. It will specifically aim to understand the present law and search for practical solutions. A review of primary and secondary sources that include; statutes, existing legislation, law reviews, research papers, journals, online legal blogs, legal publication and news articles.

[13] "Blume - Data Protection and Privacy – Basic Concepts in" pp. 153
[14] Global Partners Digital (GPD), "Travelguidetodataprotection.Pdf." https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf

1.10 Literature Review

Privacy especially relating to individual data has been a topic discussed in many forums particularly from the turn of the 21st century. The sudden influx of valuable individual data has taken the world by storm, the McKinsey Global Institute (MGI) publishes reports highlighting major benefits to businesses from such an influx. [15] Stating in one such report that smart and effective use of consumer data can have phenomenon positive impacts on the economy at large and benefit the world as a whole. However idealistic that may be, the flip side to that has been massive exploitation of said consumer data. Governments, the same ones entrusted to create policies to protect us, ironically (or in Kenya's case expectedly) have been some of the largest abusers of privacy when it comes to individual data. Reports published by various groups including a UN ECOSOC Consultative Member in a report to the High Commissioner for Human Rights highlighted the violations of privacy by governments including profiling, censorship and biometric dangers.[16] Clearly there must be attention paid to the key dangers posed by inadequate protection of individual data as it relates to privacy concerns.

Secondly, as stated earlier, our Data Protection Act was influenced by the EU's General Data Protection Regulation. This particular legislation has been scrutinized and analyzed with regards to its impact after its coming into force; former Executive Vice President-Designate of the European Commission, Frans Timmermans, stated in a report to the European Commission that more concise powers and boosted resources should be accorded to data protection authorities that in turn should allow them to carry out their functions effectively without much hinderance. [17] Similarly, in a blog post on the IT-governance.eu website, it was highlighted that mandatory compliance from the data controller's perspective with the GDPR principles

[15] McKinsey Global Institute (MGI), "MGI-The-Age-of-Analytics-Full-Report.Pdf." https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/The%20age%20of%20analytics%20Competing%20in%20a%20data%20driven%20world/MGI-The-Age-of-Analytics-Full-report.ashx

[16] United Nations Human Rights; Officer of The Hight Commissioner, "PiratePartiesInternational.Pdf." https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf

[17] European Commission Press Release, "GDPR Shows Results, but Work Needs to Continue." https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449

(including integrity, purpose limitation and data minimization) is needed for effective protection. [18]

The EU GDPR has been the best example of the best developed and implemented data protection regime in the world and other countries have followed suit, comparative studies have been carried out between the EU and other countries such as Asian countries, with the outcome being that the different regions face different developmental and cultural barriers to the full execution and as such those other countries have formulated their own localized solutions to certain limitations. Such as in Singapore where privacy hasn't been a major concern for individuals which allows the government encroach on that privacy which in turn leads to effective exposure of data privacy crimes leading to a large number of decisions and fines issued by the commissioner. [19]

In Kenya, some studies focused on The Data Protection Act have already been carried out, such as Privacy International's (in conjunction with Dr. Robert Muthuri[20]) analysis on the Act highlighted some of the general issues throughout the Act. The report is an overview of the whole Act and it paints a good picture of the current state of data privacy but does not narrow down and explore specific fixes to said problems.[21]

To conclude, there has been research done on the importance of data protection around the globe and its inter-relation with privacy as a fundamental right. There has also been extensive research done on the different modes of achieving data protection that are specific to a country's needs. Kenya itself has also taken steps to ensure data protection relating to data privacy with the coming into force of the Data Protection Act but what this research specifically

[18] Irwin, "The GDPR; Understanding the 6 data protection principles." https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles
[19] Walters, Trakman, and Zeller, *Data Protection Law A Comparative Analysis of Asia-Pacific and European Approaches*.
[20] *A Legal Knowledge Engineering Consultant. He holds a PhD in Legal Informatics, an LLM in Innovation Technology & the Law, and is an Advocate to the High Court of Kenya.*
[21] Privacy International "Analysis of Kenya Data Protection Act, 2019_Jan2020.Pdf." https://privacyinternational.org/sites/default/files/2020 02/Analysis%20of%20Kenya%20Data%20Protection%20Act%2C%202019_Jan2020.pdf

aims to tackle specific limitations in the act and explore fixes that are complimentary to the country's unique nature.

1.11 Limitations and Delimitations;

Limitations:

- Availability of governmental resources
- Relative novelty of data protection in Kenya
- Unique cultural and educational status of Kenya hindering direct copy-and-pasting of solutions
- The small amount of existing literature, at the time of the study, that addresses the new DPA

Delimitations;

- Focus on one or two other jurisdictions outside of the EU for solutions, likely India.
- Focus on 2 or 3 major subsets of consent in the act.

1.12 Chapter Breakdown:

Chapter 1; Introduction to the study.

Chapter 2; Conceptual framework

Chapter 3; Consent requirements and their faults.

Chapter 4; Recommendations for Complimentary Solutions

Chapter 5; Conclusions.

CHAPTER 2; Conceptual Framework:

2.1 Introduction:

This chapter seeks to identify the various linked concepts that will guide the study as they relate directly to the problem at the heart of the study. Attempting to suggest solutions to the problem at hand requires an understanding of the philosophical underpinnings that inform law and policy makers. Individual data, albeit in a newer form, still form part of an individual private information and thus special attention should be paid in regards to the importance of its protection.

Data protection is the encompassing theme of the study and it refers to the formulation and structuring of the laws relating to data, those which are aimed at safeguarding said data from manipulation and exploitation. It is heavily reliant on the right to privacy in our constitution.[22] The DPA seemingly sets out to correct the power imbalance and allow the data subject to regain significant control of their own data. The following theories seek to provide justification for the protection:

2.2 Concept of Privacy as a human right;

Certain rights are inherent meaning that by virtue of an individual simply being human they are born with these rights. Article one of the universal declarations of human rights, which can be categorized as the central legislation regarding international human rights, echoes that ideal.[23] There are a handful of certain rights that can be described as being fundamental to preserving the human dignity. As such accommodation and legislation must be prepared in order to allow for full enjoyment of these rights.[24] The concept of privacy and its protection is well established in Kenya, as the High Court in a case regarding the right to privacy went ahead to confirm that "*Privacy is a fundamental human right, enshrined in numerous international human rights instruments. It is central to the protection of human dignity and forms the basis*

[22] Article 31, Constitution of Kenya 2010
[23] Article 1, UDHR: "*All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood*"
[24] Weston, B.H., *"Human Rights and Nation-Building in Cross-Cultural Settings.*

of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information, and association".[25]

Privacy is a well-established concept as it is present in various legislations, cultures and religions. A precise definition of the term eludes law makers, it is described as being "so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings" that finding a common definition across all jurisdictions would be nearly impossible.[26] There is, however, a distinction between privacy as a concept and the right to privacy. Interestingly, privacy as *a concept* must be defined to an extent because that very definition is what allows for *the right to* privacy to be *protected.* This is because a set definition (not a universal definition but one that is localized to a specific jurisdiction) is indeed required to aid in the development legislative framework. A number of scholars agree that this right to privacy is an important and necessary requirement in a modern and democratic society.[27] Recognition of the right to privacy is an already present and developed norm, it is the move from simple recognition to effective protection that is yet to be attained. In a functioning democratic society, privacy is understood to be the right to left along, otherwise interpreted as keeping others away from the private sphere or private information.[28]

2.3 Concept of Consent:

Consent can simply be defined as granting permission or agreement.[29] It indicates that an individual who consents to something freely agrees to it and accepts the parameters of the agreement. Consent is a key factor of the law as in a functioning democratic society, members consent to being governed by their chosen leaders. These leaders then facilitate for the laws that will in turn govern the members of the society. As a safeguard, consent works very well as it implies that an individual is aware of the situation and giving consent can be used as evidence in the event that a dispute arises.

Likewise, in data protection, the concept plays a central role. It features prominently in multiple

[25] Kenya Human Rights Commission v Communications Authority of Kenya & 4 others [2018] eKLR
[26] Post, C "*Three Concepts of Privacy*"- https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1184&context=fss_papers
[27] Westin, A. F., Privacy and Freedom, The Bodley Head Ltd, London, 1970, 330–364
[28] "Blume - Data Protection and Privacy – Basic Concepts in" pp. 158
[29] Definition of consent: Cambridge English dictionary.

pieces of legislation as well as influences greatly the research, regulation and public debates around data protection. Owing to that importance, it would be in a state's best interest to formulate legislation that supports itself on the foundation of consent. The problem this might raise is whether or not the simple "accept or do not" approach to gaining consent properly secures one rights to privacy as again the consent may not be properly given.

2.4 Inter-relation of Concepts in Data protection:

These two concepts are complimentary. Data originates from the data subject; it is part of their personal information. Therefore, the individual's data should be subject to privacy and as such be governed by the right to privacy. This right to privacy then brings in the need for consent. Consent acts as a shield to the private data of citizens and therefore, a well-established & organized form of gaining consent becomes a powerful tool in protecting data. If there was lack of recognition of ones right to privacy regarding their data, then there would be no need for consent at all. On the other hand, if there is already a recognition of ones right to privacy but a poorly constructed form of consent, it would similarly take power away from the data subject.

2.5 Conclusion;

Both above mentioned concepts are pillars of data protection, they assist law makers in developing legislation. Similar to other rights that are currently accorded to citizens, privacy should likewise become a top priority as the world is progressing towards a data-oriented model. Additionally, the model of consent used in different legislative pieces should be one based on the essence of the concept, that is to secure the power that an individual has in whatever transaction is going on.

As both of these concepts are at the forefront of data protection, they should be used as a standard to analyze data legislation. The effectiveness of the DPA shall be criticized in view of these key concepts.

CHAPTER 3; Consent Requirements and their Faults

3.1 Misunderstanding the importance of data privacy

Privacy as a right has been dominated by "versions of privacy" that touch on maters in the material-plane, specifically laws governing a variety of sectors from information relating to property to financial records and peer-to-peer communication. These categories have been at the forefront of privacy legislation due to them being present throughout a good majority of our history thus their solidity through long term development. Technology on the other hand is a relatively new concept and as such the legislation around the concept is also relatively new. As such, it would be in our best interest to shift perception and bring to attention the importance of safeguarding individual data privacy.

To do that, it is important to first deconstruct the current view of privacy. One common approach to tie privacy and data is highlighted by Daniel J. Solove[30] as the "I've got nothing to hide" concept. It states that individuals who believe they have nothing to hide have little to no problem with their data being collected by corporations and the government. That the intentions of those bodies collecting their data are entirely in their best interests. The effect of this is that privacy of personal data is stationed down the hierarchy of types of privacy, taking a back seat when it comes to legislation and importance. The unfortunate reality about data privacy however, is that it not only intertwined with all the other forms of privacy but in today's digital age can be considered to be the most important of all.

For example, in Kenya, during the period before the DPA, money lending and fintech applications were disrespecting individual privacy. These applications would provide quick access loans to individuals often with very high interest rates and at the cost of personal data. When registering, they would often require disclosure of personal data defined in the DPA as information relating to an identified natural person including full names, financial details and access to contact details[31]. Most of those applications justify their requirement of such data by stating that it will be used to generate a "credit score' of sorts. The score then determines how much one can borrow and how long the repayment schedule will be. The applications then used

[30] Associate Professor, George Washington University Law School; J.D., Yale Law School.
[31] Section 2, Data Protection Act 2019

the information for other, often non disclosed, reasons and would even access details on one's contact lists without requesting access from the user[32]. Most of the citizens unfortunately involved often don't understand the importance of keeping their data private thus opening them to exploitation. The first problem to tackle is reshaping the perception of data privacy as a right.

3.2 The Need for protection.

The need for legislation is either realized by the government or the governed. Well established areas of law such as civil matters, property rights, constitutional implementation are the foundations of a society. These areas are keenly watched by the government and as such they are accorded the proper time and understanding when it comes to legislation. They often require minimal demand from the public in order for the government to enact legislation. The second way in which proper legislation often comes about is through individually lead causes from the "governed". Such was the case regarding LGBTQ[33] rights or the rights of women in early 1900. These areas required a push from the public in order for legislation to be passed.

For data protection, legislation can originate from both sides of the divide. For example, in the 1960s, an academic researcher at Columbia University called Dr Alan Westin wrote a book known as "privacy and freedom" which he defined privacy as: *an individual's right "to control, edit, manage, and delete information about them[selves] and decide when, how, and to what extent information is communicated to others*[34]. His works had prompted enacting of legislation in the United States regarding privacy in the 1990s. Globally, a lot of countries had followed suit in their recognition of privacy rights. Alternatively, governments and other legislative bodies can take initiative, such as when the European commission tasked themselves with modernizing the data protection legislation in 2012 in order to prepare Europe for the looming digital age[35].

[32] HILLARY KEVERENGE, *Home News O-Kash, OPesa Loan Apps Will Text Or Call Your Contacts If You Default – And It's Well DocumentedNEWSO-Kash, OPesa Loan Apps Will Text Or Call Your Contacts If You Default-* https://androidkenya.com/2019/04/o-kash-opesa-quick-loan-apps/
[33] LGBTQ is an acronym for lesbian, gay, bisexual, transgender and queer or questioning.
[34] Alan F. Westin, *Privacy and Freedom*
https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr
[35] Data Protection in the EU: https://ec.europa.eu/info/law/law-topic/data-protection_en

In Kenya, up until November 2019, there was no dedicated act dealing with data protection. In 2018 there was the Kenya Data Protection Policy but the DPA of 2019 was the first data protection law in the country's history. The DPA borrows for the EUs GDPR and is indeed a big step in the right direction. It comes with a host of benefits including developing a regulatory framework for processing of personal data, establishing the office of the data commissioner and introducing fines and penalties as deterrents and punishments. However, the act still faces challenges, specifically when it comes to consent.

3.3 Consent as a pillar

Consent is one of the fundamental pillars in data protection, as it is in other areas of the law. Consent in contract law means that both parties are aware of and agree to the same terms, consent obtained by the bank when agreeing on a loan indicates that the bank and individual are aware of and agree to the same terms. Thus, it should be the same case when data is being collected or processed, that the subject and the controller/processor are both aware of the same terms and are in agreement.

Under the GDPR, consent is one of the key legal requirements for processing of data.[36] This does not mean that it is a simple requirement, as pointed out in a case involving technology giant Google, in which French data protection authorities argued that the consent obtained by Google was neither "specific" nor "unambiguous"[37]. The requirements for consent under the GDPR are very detailed and it starts with the definition provided by the rules for consent; "*Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*"[38]. That definition provides some insight into the requirements laid down, touching on the concepts that are to be delved into, namely "freely given", "specific", "informed and "unambiguous".

[36] Article 6, GDPR
[37] The Local FR; "*Why France hit Google with a whopping €50 million fine"*- https://www.thelocal.fr/20190121/why-france-fined-google-50-million
[38] Article 4(11), GDPR.

3.4 Consent under the DPA 2019:

The DPA was inspired by the GDPR and a majority of the provisions in the act are similar. This is to the benefit of the Kenyan citizens as the GDPR is often described as the most developed legislation regarding data protection. There are some differences such as the definition of consent, where the Kenyan DPA includes "express" and "unequivocal" as additional requirements for consent but doesn't include "unambiguous". These requirements should then take a central seat when data collectors are seeking consent from data subjects. In practice, this should be the case but it can be argued that consent collected in Kenya does not strictly follow the requirements. To elaborate this further, it is necessary to review these specific requirements for consent and whether they were they are correctly adhered to. The study will mainly focus on 3 of the requirements of consent under section 2 of the act, namely that consent has to be "informed, specific and freely given". This is because these particular conditions are problematic as they fail in their endeavor to gain concrete consent, further elaborated below:

1. **Informed:** Black's law dictionary defines informed consent as "*A person's agreement to allow something to happen, made with full knowledge of the risks involved and the alternatives*".[39] This means that beyond giving consent for an activity, a person must be fully aware of what he/she is consenting to, in what form and the repercussions of giving consent (the implications on the individual brought about by their consent). This concept protects the consenting individuals from exploitation because it is that very knowledge that allows said individuals to understand the consequences of their consent better. Thus, helping them make a more informed decision and steer clear of avoidable negative consequences down the line.

   In data protection, informed consent means that the data subject is aware of the full identity of the data collector, what types of data/information is being collected, where it is being stored and what it is going to be used for[40]. This is a basic requirement under general data protection legislation, the EU GDPR similarly states that informed consent requires that those consenting to the data processing should fully understand what they

[39] *Informed Consent*, Black's Law Dictionary (10th ed. 2014)
[40] GDPR;EU, *Consent requirements*: https://gdpr.eu/gdpr-consent-requirements/?cn-reloaded=1

are consenting to. This was used by CNIL when imposing the fine on Google, stating that "the *users' consent is not sufficiently informed. The information on processing operations for the ads personalization is diluted in several documents and does not enable the user to be aware of their extent. For example, in the section "Ads Personalization", it is not possible to be aware of the plurality of services, websites and applications involved in these processing operations (Google search, You tube, Google home, Google maps, Play store, Google pictures…) and therefore of the amount of data processed and combined*[41].

In Kenya, the DPA states that the data subject has the right to know what their personal data is going to be used for[42] and even allows for the collection of said personal data indirectly (from another source) if the data subject consents to it[43]. Knowledge of the use of one's data therefore, is a valid requirement for gaining consent under the act. While it is true that in theory this system can safeguard the rights of the individual, in practice there are key concerns regarding its viability.

Firstly, the concept of informed consent currently found in the DPA can be traced to the EUs GDPR, this in of itself is not a criticism of the consent but it is important to understand the origin. It was correct for legislators in Kenya to look towards arguably the most developed data protection law as a reference regarding the requirements of consent and how to incorporate them into the national law. However simply uprooting a successful concept and planting it elsewhere in hopes that it will be equally as effective is farfetched. Akin to taking a perfectly acclimatized strain of tomato in the Amazon basin and planting it in the Nubian desert believing it would succeed. The question then arises, has the concept been adapted/localized for use in Kenya? The jurisdiction of the GDPR covers processing of data within the European region. The laws thus mainly affects European citizens, it can then be argued that those citizens are aware of the importance of personal data. This is a result of the increased importance and awareness requirements the continent has been placing on individual data protection; from recognition of data protection as a right under the EU Charter of

[41] CNIL; *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC.* https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
[42] Section 26 (a), The Data Protection Act 2019
[43] Section 28 (2) (c) , The Data Protection Act 2019

Fundamental Rights[44] to the legal vetting of countries outside the EU on the level of their data protection (the adequacy of such protection) when engaging in activities with those countries that may affect the data protection of their citizens.[45] Similarly, there have been a number of scandals relating to data privacy concerns within the region (such as the google ruling discussed above and the illegal collecting of Facebook data tied to the Cambridge Analytica debacle[46]) and this "increased awareness" allows for the assumption that the importance of data privacy in the area is clear. Unfortunately, it can also be argued that the same value and understanding of individual data is not held by most Kenyans. In Kenya, there was lack of a centralized data protection act before 2019, unlike Europe which had privacy laws dating back to the 1980s[47]. The NIIMS system is a clear example of such, the narrative pushed was that the system would be a convenient method of collecting one's documents and details into one integrated system. The problem with this is that the information mostly stops there, data collectors under the DPA are only required to present basic level information when collecting the data. The law does not take into account that the average Kenyan citizen does not know the true value of their data and its implications. The positives are often focused on more, such as the availability of all governmental resources and identifications (National ID, drivers license, etc) in one card. To reiterate, there is no provision under the DPA that requires data controllers/collectors to inform the subject about any alternatives to processing or a requirement to explain to the data subject in a language or terms that they can fully understand. This can then lead to individuals consenting without fully understanding what it is they are consenting to effectively the "informed" requirement of consent. The idea of consent being a safeguard therefore is weakened because even though data collectors are required to follow the law (regardless of whether or not the data subject understand the law), the nature of consent requires understanding the subject matter. It is that lack of understanding that therefore does not allow for consent to be considered "informed" effectively reducing the strength of the consent given.

[44] Article 8, EU Charter of Fundamental Rights
[45] Article 45, General Data Protection Rules 2018
[46] Politico; *2.7M Europeans affected by Facebook, Cambridge Analytica scanda*l https://www.politico.eu/article/facebook-cambridge-analytica-jourova-2-7-million-data-protection-privacy/
[47] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

2. **Specific;** The consent given by a data subject must be for a specific purpose, the DPA as well as the GDPR both require the intended use of the data collected to be specified. The collector should ensure that the specific data types being processed are individually known and the data subject consents to those data types/sets specifically. There should not be instances where a subject is consenting without being aware of the extent of their consent, how many datasets they are allowing to be collected and processed, in what manner and what safeguards are in place[48]. The last requirement has seemingly been omitted from the collection process of the NIIMS project, not only is that inconsistent with the DPA but it may set a dangerous precedent. It will lead to exploitation in the future as security measures may continue being omitted. To elaborate, a large number of citizens assumed that the data being collected was going to be shared with commercial banks or financial institutions, which then prompted a response from then director of the National Registration Bureau Ruben Kimotho explaining that "data shall be protected by the law and not shared, regardless of which institution acquires such data" at a forum meant for public participation on proposed regulations.[49] This clearly highlights the vague nature of data use after its collection, such concerns should have been addressed when collection was happening at individual level by instructing the data collectors to fully inform the citizens on the specific collection requirements.

3. **Freely Given:** Consent must be given willingly and freely, there must be no coercion or other such factors placed on the individual consenting. kin to the law of contract concept of "vitiating elements" such as undue influence or duress. In data protection, it is not as clear cut due to the ideas of "duress or undue influence" may manifest themselves differently. Alternative methods are used in order to convince an individual to consent in a manner that may seem free but not exactly "freely given". The best example of this is when the subject seemingly has no alternatives (or believing they have none), leading them to believe they must consent to get a vital service. Alternatively, the subject may have other indirect factors (such as stigma or peer pressure) affecting them and thus consents. These tactics are often used by websites

[48] Section 29 (f), Data Protection Act 2019
[49] "Huduma Namba Jitters" https://www.youtube.com/watch?v=T-lw10Er-Yw&list=PLbV-Gqi6cvAm64WXQ8gMm_HSVNLfi6bLK&index=266&ab_channel=SwitchTVNews

online when collecting data, the website will not allow access to anyone who does not consent to/accept their cookie requests[50]. When it comes to collection of data *en masse* from the government, tactics like those mentioned above are worse because not only is it happening at scale but the power dynamic accentuates the negatives.

The power dynamic is the main factor. For websites, the majority of the time there shall be alternatives to the services provided, Google has duck-duck-go, Spotify has Pandora, Hulu has Netflix. The data subject needs to be able to refuse consent, to be fully aware that alternatives (if present) are available and that not consenting will be substantially detrimental. In Kenya, the NIIMS system was/still is intended to be used by the citizens to store a variety of their documents and data in one easy to access location, the government also stated that access to vital governmental services such as renewing driving license or processing of passports shall be done using the system. Insinuating that for one to access those services, that person must be in the system and thus have consented to their data being collected in the first place. Essentially, it would seem that regardless of whether or not the individual actually wants to give consent, out of fear of being denied services they consented (even though a 3 Judge bench on April 1st 2019 ruled that the registration must not be mandatory and that services shall not be denied based on lack of registration[51]). The initial wave of fear was a strong enough factor in the decision of individuals to consent. The fact that there were individuals who held the opinion/belief that they would be left out of services if they failed to register is inconsistent with the duty of data controllers to notify the data subjects on the correct consequences of refusing to provide the necessary data.[52] The NIIMS registration controversy shows that consent was given but it cannot necessarily be deemed to be "free" because the government initially intended to provide services only to those that registered which goes against the concept entirely. Seeing as the GDPR was an influence, it would be necessary to refer to Recital 42 which states that "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is

[50] HTTP cookies are essential to the modern Internet but a vulnerability to your privacy. As a necessary part of web browsing, HTTP cookies help web developers give you more personal, convenient website visits" https://www.kaspersky.com/resource-center/definitions/cookies
[51] Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR
[52] Section 29 (h), The Data Protection Act 2019

unable to refuse or withdraw consent without detriment".[53] This further emphasizes the fact that without proper knowledge and no requirement to make sure the data subject understands the subject matter entirely, consent cannot be considered to be freely given.

3.5 Conclusion:

In conclusion, it is firstly important to outline that the conditions for consent under the DPA are well established and effective conditions in Europe. However, of equal importance is understanding that Europe and Kenya are substantially different, specifically relating to cultural relativity and educational levels. It is because of these differences that the conditions for consent discussed above struggle when attempting to wholly and fully obtaining consent. Not because the conditions themselves are poorly constructed or that different requirements are needed, but because of the differences between the regions that does not allow for the conditions to effectively work. This then leads to instances where the threshold for consent is set very low and is barely achieved and not effectively achieved.

It can be argued that Kenyans can not be seen to be as informed (regarding data) to fully understand the consequences of their consent but it can be argued that they are informed *enough* to satisfy the requirement. Similarly, many of them don't know the full extent of the data that is being collected but are aware of enough to consent to specifics. Finally, many of them simply consented not because they were confident in the data collection but simply because they did so because a number of their colleagues and families consented and thus *barely* satisfied the freely given factor of consent. All these requirements are fulfilled because the threshold is very low, leading to a "just enough" mentality. Therefore, to reiterate, the conditions for consent are good standards however by themselves do not properly secure data rights in Kenya. There must be steps or solutions introduced that complement these requirements and allow them to be fully utilized. These solutions must be feasible and facilitate for consent to be properly attained.

[53] Burden of proof and requirements for consent; Recital 42- GDPR; https://gdpr.eu/Recital-42-Burden-of-proof-and-requirements-for-consent/

Chapter 4: Recommendations for Complimentary Solutions

4.1 Introduction;

As discussed above, the model of consent is well established. The current form and conditions of consent under the DPA is heavily influenced by the GDPR and thus is already of high quality. However, it can be further enhanced and become even more effective in practice if certain additions are incorporated into the legislating framework that would seek to compliment these conditions.

4.2 Fiduciary Duty:

Power is dangerous if not used properly. The DPA accords a lot of rights to data subjects when their data is being processed especially for consent. It places burden of proof for establishing consent on the data controller[54] and for data allows them to revoke the consent[55]. Even with this, it would be a stretch to require the common citizen to fully utilize this power as data rights and its importance are fairly new concepts in the country. Therefore, we must strive to make data work for these individuals.[56] One way would be to legally impose a fiduciary duty on the data controllers. Professor Jonathan Zittrain[57] describes fiduciaries essentially as a loyalty clause imposed on people with power. Just as lawyers and financial advisors have access to important and exploitable information, data controllers have access to very sensitive data and as such should be required to act in the best interest of the data subjects.

A suggestion would then be to add a requirement under section 32 of the DPA that would establish a fiduciary duty on the data controllers, essentially protecting the data subjects in Kenya and allowing them to enjoy their rights. The idea of developing a fiduciary duty on data collectors has be implemented in other countries, specifically India. Introduction of a fiduciary relationship into privacy jurisprudence has already happened in India through the designating

[54] Section 31(1), The Data Protection Act 2019
[55] Section 31 (2). The Data Protection Act 2019
[56] CGAP, *HOW TO MAKE DATA WORK FOR THE POOR*, *https://www.cgap.org/sites/default/files/publications/2020_01_Focus_Note_Making_Data_Work_for_Poor_0.pdf*
[57] A professor of international law at Harvard Law School and the Harvard Kennedy School of Government. https://cyber.harvard.edu/people/jzittrain

of data processing entities as "data fiduciaries".[58] Similar to the Kenyan DPA, "There is no general requirement in the PDP Bill for the data collectors to act in the user's interests, for their benefit or to avoid acting in a manner detrimental to the user"[59], under the DPA, the only section that states that processing should be done in the best interest of an individual is when that individual is a child.[60] This can be considered a result of a lower standard or a less complex standard of protection stemming from an attempt to not discombobulate the average citizen. John H. Langbein suggests that the lower standard is often used in cases where it is easier in helping overcome certain information asymmetries as well as situations where a higher standard would be difficult to implement (social or educational conditions).[61] Indian legislators intend to close any loopholes that would allow exploitation by not allow data to be used in a way that would benefit collectors and processors over data subjects. The same approach can be used here in Kenya.

Regarding feasibility, Kenyan citizens are more akin to Indian citizen regarding levels of development and standards of education. Therefore, the idea would be implementable on the same level when it comes to determining reception of the concept. The fact that it would also not require mass amendments to the act coupled with the fact that data collectors would then have to act in the interest of the subject regardless of the subjects understanding would further enhance data protection.

4.3 Representation;

Another concept that would further aid citizens when it comes to properly understanding the consequences of consent would be to have a representative present or mediating or advising when consenting to data collection. Data collectors are mandated by law to prove that they established and received consent from the individuals under section 32 (1). However, except

[58] Rishab Bailey, *Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2019*, https://blog.theleapjournal.org/2020/01/fiduciary-relationships-as-means-to.html
[59] Rishab Bailey and Trishee Goyal, *Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2018*. https://datagovernance.org/files/research/NIPFP_Rishab_Trishee_fiduciaries_-_Paper_4.pdf
[60] Section 33 (1) (b), The Data Protection Act 2019
[61] John H Langbein, *Questioning the Trust Law Duty of Loyalty: Sole Interest or Best Interest?, Yale Law Journal, Vole. 114, Issue 1, 2005*.

where the consent was given to receive a service [62], the law implies that consent once received can be greatly relied upon and only come into question if the data subject realizes and/or raises cause for concern. The average citizen cannot be, and should not, be expected to realize that they have either mis-understood or not fully understood the consequences of their consent. Therefore, like legal representation, there should be an intermediary between the data subject and the data collector especially for mass collection or complex transactions.

The idea of representatives that help data subjects navigate the murky waters of consent is heavily influenced by the work of Rahul Mattan. He proposed the idea of "learned intermediaries" in early 2017, stating that these learned intermediaries would be an additional layer of supervision added to the already existing consent framework, these individuals would be trained personnel that would not only help the subject fully understand the consequences of consent but would also be "legitimate auditors of data controllers".[63] These individuals would then strive to make sure that the relationship between the collectors and subjects are fair, akin to a physician acting as an intermediary between patients and pharmaceutical companies, advising patents on whether or not to take the medicine and the impacts of the medicine.

For the idea to be implemented successfully, there are two major requirements aside from training of the intermediaries (as said intermediaries would take it upon themselves to seek education). The first would be the issue of monetary compensation, on one hand they could derive their fees from customers (data subjects) following the model of physicians or financial advisors. The problem is that such a practice would not be inclusive, as a percentage of population that would not either be able to afford or would not see the importance of having such representation. Alternatively, they could be paid by the government which would then in turn allow for inclusivity of all financial backgrounds as well as creating employment, unfortunately this would require restructuring of national budget or setting aside funds which would difficult to implement or require funds to be transferred from other projects/sectors. The second requirement would be to create a system of accreditation or certification under the law

[62] Section 32 (4), The Data Protection Act.
[63] R MATTHAN, *Beyond Consent; A New Paradigm for Data Protection*, https://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf

that would allow these intermediaries to practice legally. All in all, creating these representatives would go a long way to assist the data subject.

4.4 Conclusion;

All in all, these two recommendations both address the problem of solely relying on the conditions of consent to properly safeguard the interests of the data subject. They both put the interests of the data subjects first as well as ensure that there is another layer of protection that compliments the safeguarding nature of consent. It must be highlighted that these two methods are not without dangers, finding a perfect solution is nearly impossible. Corruption can easily affect both solutions as it is a big problem in the country, however if managed properly, they may lower the deficiencies that the DPA currently has regarding consent as a whole.

Chapter 5; Conclusions and Inferences

Individual data protection should be a major concern in developing countries. History has shown that exploitation in general, ranging from natural resources to labor, is an ever-persistent threat. It is often stated that "data is the new oil" implying that it is a valuable commodity that shall eventually drive an entire economy[64] however data is not bound by the same shackles as oil. Firstly, oil in its crude form is not as valuable, it must be refined to be profitable. Secondly, oil is a finite resource. Data is an effectively unlimited resource that can be thoroughly exploited even in its raw form, making data more like nuclear power.[65]

The next step then would be to ensure that the source of data, the individual, is well protected from any form of exploitation. Legislation should then be enacted to that effect, which has been done in Kenya through the Data Protection Act 2019. The template used was the very successful European General Data Protection Rules (GDPR) that has been considered the golden standard for data protection across the world. Thus, towards the end of 2019 the DPA came into force and has been steadily implemented, such as the important office of the Data Commissioner being occupied in November 2020.

The legislation is a very good step at protection but it is not perfect, specifically referring to the standards of consent under the act. The standard is similar to that available under the GDPR and even though the standards are industry standard, in practice they fall short in effectively protecting the individuals' data rights. This is because the differences in culture and education between the two regions allows for the conditions of consent to stand freely and be effective. This incommensurability of values is detrimental to the Kenyan citizen as they will consent and face the consequences of consent without knowing any better.

[64] JOSHUA NEW, *Why Do People Still Think Data Is the new Oil;* https://datainnovation.org/2018/01/why-do-people-still-think-data-is-the-new-oil/#:~:text=When%20British%20data%20scientist%20Clive,commodity%20in%20the%20modern%20economy .

[65] JAMES BRIDLE, *Opinion; Data Isn't the New Oil- It's the new Nuclear Power*. https://ideas.ted.com/opinion-data-isnt-the-new-oil-its-the-new-nuclear-power/

To remedy this, we must look for complimentary solutions that would take advantage of the successful consent model in the DPA and make it successful in Kenya. A look at other jurisdictions found that there were different approaches to effectively utilize the concept consent, specifically in India. It can be argued that the average Kenyan is more in line with the average Indian regarding levels of education and cultural dispositions. In India they have attempted to include a fiduciary duty on those collecting the data that requires them to act in the best interest of the data subject, effectively addressing the power imbalance and restoring power into the hands of the data subject. Secondly, introduction of learned data intermediaries that act to represent the data subjects where consent is involved.

These solutions are arguable best suited to further secure individual data protection under the data protection act; however, implementation may not be as straight forward as presented. Data intermediates may still fall prey to corruption, as well as the problem of determining where their compensation would be derived from (the government? The data subjects? NGOs?). All in all, taking a single step is better than not taking a step at all. With the very relevant and real-world examples of how data is taking over the world, it would be in all our best interests to avoid repeating mistakes made elsewhere and protect each and every Kenyan.

Bibliography:

Journals/Articles/Books

- *2.7M Europeans affected by Facebook, Cambridge Analytica scandal* (2018) *POLITICO*. Available at: https://www.politico.eu/article/facebook-cambridge-analytica-jourova-2-7-million-data-protection-privacy/ (Accessed: 25 October 2020).
- *2020 is a crucial year to fight for data protection in Africa* (no date) *Privacy International*. Available at: http://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa (Accessed: 9 December 2020).
- '2020_01_Focus_Note_Making_Data_Work_for_Poor_0.pdf' (no date). Available at: https://www.cgap.org/sites/default/files/publications/2020_01_Focus_Note_Making_Data_Work_for_Poor_0.pdf (Accessed: 8 December 2020).
- *Amazon rollout of cloud computing unit in Nairobi set to spur East African market - Business Daily* (no date). Available at: https://www.businessdailyafrica.com/corporate/tech/Nairobi--Amazon-Web-Services/4258474-5348692-ll5ejz/index.html (Accessed: 24 March 2020).
- 'Analysis of Kenya Data Protection Act, 2019_Jan2020.pdf' (no date a). Available at: https://privacyinternational.org/sites/default/files/2020-02/Analysis%20of%20Kenya%20Data%20Protection%20Act%2C%202019_Jan2020.pdf (Accessed: 23 March 2020).
- 'Analysis of Kenya Data Protection Act, 2019_Jan2020.pdf' (no date b). Available at: https://privacyinternational.org/sites/default/files/2020-02/Analysis%20of%20Kenya%20Data%20Protection%20Act%2C%202019_Jan2020.pdf (Accessed: 26 March 2020).
- *Article 8 - Protection of personal data* (2015) *European Union Agency for Fundamental Rights*. Available at: https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data (Accessed: 25 October 2020).
- Bailey (no date) *Amazon rollout of cloud computing unit in Nairobi set to spur East African market - Business Daily*. Available at: https://www.businessdailyafrica.com/corporate/tech/Nairobi--Amazon-Web-Services/4258474-5348692-ll5ejz/index.html (Accessed: 23 March 2020).
- Bergemann, B. (2018) 'The Consent Paradox: Accounting for the Prominent Role of Consent in Data Protection', in Hansen, M. et al. (eds) *Privacy and Identity*

Management. The Smart Revolution. Cham: Springer International Publishing (IFIP Advances in Information and Communication Technology), pp. 111–131. doi: 10.1007/978-3-319-92925-5_8.

- Bergkamp, L. (2002) 'EU Data Protection Policy', *Computer Law & Security Review*, 18(1), pp. 31–47. doi: 10.1016/S0267-3649(02)00106-1.
- Blume, P. (no date a) 'Data Protection and Privacy – Basic Concepts in a Changing World', *Scandinavian Studies In Law*, p. 14.
- Blume, P. (no date b) 'Data Protection and Privacy – Basic Concepts in a Changing World', *Scandinavian Studies In Law*, p. 14.
- Businesses, F., The Federation of Small (no date) *Why is data protection so important?* Available at: https://www.fsb.org.uk/resources-page/why-is-data-protection-so-important.html (Accessed: 25 March 2020).
- Carey, P. and Carey, P. (2018) *Data protection: a practical guide to UK and EU law*. Fifth edition. Oxford, United Kingdom: Oxford University Press.
- Claes, E., Duff, A. and Gutwirth, S. (eds) (2006) *Privacy and the criminal law*. Antwerp: Intersentia.
- *Comparing privacy laws: GDPR v. POPIA* (2020) *DataGuidance*. Available at: https://www.dataguidance.com/resource/comparing-privacy-laws-gdpr-v-popia (Accessed: 8 December 2020).
- *Comparing privacy laws: GDPR v. Singapore's PDPA* (2020) *DataGuidance*. Available at: https://www.dataguidance.com/resource/comparing-privacy-laws-gdpr-v-singapores-pdpa (Accessed: 8 December 2020).
- Dahir, A. L. (no date) *Digital lending apps are coming under scrutiny in East Africa for predatory practices, Quartz Africa*. Available at: https://qz.com/africa/1712796/mobile-loans-apps-tala-branch-okash-face-scrutiny-in-kenya/ (Accessed: 10 October 2020).
- Dewan, R. K. and Dewan, C.-D. M. (no date) *Personal Data Protection Laws in India | Lexology*. Available at: https://www.lexology.com/library/detail.aspx?g=08197ebe-aeb4-41d6-a855-ce57a313ea6d (Accessed: 7 December 2020).
- 'DIGITAL_RIGHTS_IN_KENYA.pdf' (no date). Available at: https://info.mzalendo.com/media_root/file_archive/DIGITAL_RIGHTS_IN_KENYA.pdf (Accessed: 8 December 2020).

- *Edward Snowden: Leaks that exposed US spy programme - BBC News* (no date). Available at: https://www.bbc.com/news/world-us-canada-23123964 (Accessed: 24 March 2020).
- *Everything You Need to Know About Informed Consent* (2018) *Atlan | Humans of Data*. Available at: https://humansofdata.atlan.com/2018/04/informed-consent/ (Accessed: 21 October 2020).
- *GDPR shows results, but work needs to continue* (no date) *European Commission - European Commission*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449 (Accessed: 25 March 2020).
- 'gdpr_v._nigeria.pdf' (no date). Available at: https://www.dataguidance.com/sites/default/files/gdpr_v._nigeria.pdf (Accessed: 7 December 2020).
- 'Guidelines on DPOs ENG.pdf' (no date). Available at: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/300557324E87916AC2258260003751C4/$file/Guidelines%20on%20DPOs%20ENG.pdf (Accessed: 26 March 2020).
- Irwin, L. (2018) *The GDPR: Understanding the 6 data protection principles*, *IT Governance Blog En*. Available at: https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles (Accessed: 26 March 2020).
- Irwin, L. (2020) *The GDPR: What exactly is personal data?*, *IT Governance Blog En*. Available at: https://www.itgovernance.eu/blog/en/the-gdpr-what-exactly-is-personal-data (Accessed: 25 March 2020).
- *Kenya: Digital identity regulations must satisfy constitutional requirements* (no date) *ARTICLE 19*. Available at: https://www.article19.org/resources/kenya-digital-identity-regulations-must-satisfy-constitutional-requirements/ (Accessed: 24 March 2020).
- Lambert, P. (2018) *Understanding the new European data protection rules*. Boca Raton, FL: CRC Press.
- Langbein, J. H. (no date a) 'Questioning the Trust Law Duty of Loyalty: Sole Interest or Best Interest?', *The Yale Law Journal*, p. 62.
- Langbein, J. H. (no date b) 'Questioning the Trust Law Duty of Loyalty: Sole Interest or Best Interest?', *The Yale Law Journal*, p. 62.

- *Making data work for everyone* (no date). Available at: https://blogs.worldbank.org/opendata/making-data-work-everyone (Accessed: 14 December 2020).
- Matthan, R. (2017) 'DISCUSSION DOCUMENT 2017-03', p. 17.
- 'MGI-The-Age-of-Analytics-Full-report.pdf' (no date). Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/The%20age%20of%20analytics%20Competing%20in%20a%20data%20driven%20world/MGI-The-Age-of-Analytics-Full-report.ashx (Accessed: 25 March 2020).
- New, J. (2018) 'Why Do People Still Think Data Is the New Oil?', *Center for Data Innovation*, 16 January. Available at: https://datainnovation.org/2018/01/why-do-people-still-think-data-is-the-new-oil/ (Accessed: 30 December 2020).
- 'NIPFP_Rishab_Trishee_fiduciaries_-_Paper_4.pdf' (no date). Available at: https://datagovernance.org/files/research/NIPFP_Rishab_Trishee_fiduciaries_-_Paper_4.pdf (Accessed: 13 December 2020).
- 'Opinion: Data isn't the new oil — it's the new nuclear power' (2018) *ideas.ted.com*, 17 July. Available at: https://ideas.ted.com/opinion-data-isnt-the-new-oil-its-the-new-nuclear-power/ (Accessed: 30 December 2020).
- *Personal data protection | Fact Sheets on the European Union | European Parliament* (no date). Available at: https://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection (Accessed: 25 October 2020).
- 'PiratePartiesInternational.pdf' (no date). Available at: https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf (Accessed: 25 March 2020).
- Post, C. (no date) 'Three Concepts of Privacy', *THE GEORGETOWN LAW JOURNAL*, 89, p. 12.
- *Privacy, Data Protection and the CoronaVirus - Mugambi Laibuta* (no date). Available at: https://www.laibuta.com/human-rights/privacy-data-protection-and-the-coronavirus/ (Accessed: 23 March 2020).
- Rengel, A. (2014) 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace', *Groningen Journal of International Law*, 2(2), p. 33. doi: 10.21827/5a86a81e79532.

- Rishab, B. (no date) 'Fiduciary relationships as a means to protect privacy: Examining the use of the fiduciary concept in the draft Personal Data Protection Bill, 2019'. Available at: https://blog.theleapjournal.org/2020/01/fiduciary-relationships-as-means-to.html (Accessed: 13 December 2020).
- 'sea-risk-data-privacy-in-asean.pdf' (no date). Available at: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-data-privacy-in-asean.pdf (Accessed: 9 December 2020).
- *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC | CNIL* (no date). Available at: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (Accessed: 23 October 2020).
- 'The Data Protection Commissioner' (2020) *Mugambi Laibuta*, 20 January. Available at: https://www.laibuta.com/constitution/the-data-protection-commissioner/ (Accessed: 25 March 2020).
- 'travelguidetodataprotection.pdf' (no date). Available at: https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf (Accessed: 25 March 2020).
- Walters, R., Trakman, L. and Zeller, B. (2019) *Data Protection Law A Comparative Analysis of Asia-Pacific and European Approaches*. Singapore: Springer Singapore. Available at: https://doi.org/10.1007/978-981-13-8110-2 (Accessed: 23 March 2020).
- *What are Cookies?* (2020) *www.kaspersky.com*. Available at: https://www.kaspersky.com/resource-center/definitions/cookies (Accessed: 26 October 2020).
- *What are the GDPR consent requirements?* (2019) *GDPR.eu*. Available at: https://gdpr.eu/gdpr-consent-requirements/ (Accessed: 23 October 2020).
- *Why France hit Google with a whopping €50 million fine* (2019). Available at: https://www.thelocal.fr/20190121/why-france-fined-google-50-million (Accessed: 21 October 2020).
- 'za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf' (no date). Available at: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf (Accessed: 26 March 2020).