E-COMMERCE IN KENYA: THE CASE FOR PROTECTION OF PERSONAL INFORMATION IN E-COMMERCE TRANSACTIONS

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

By:
NICOLE MWANGO OSORO
094312

Prepared under the supervision of:
MS. SARAH OCHWADA

MARCH 2019
Word Count: 15026

Table of Contents

Acknowledgements

I would like to thank the Almighty God for the gift of life, health and most importantly the strength to carry out this research.

A special thanks to my father, Mr. Alphaxard Osoro and my mother, Mrs. Rose Osoro, for their advice and support were of great motivation throughout my research. My supervisor Ms. Sarah Ochwada whose patience and grace allowed me to complete this research.

Declaration

I, NICOLE MWANGO OSORO, 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: .....

Dated: .....

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

Signed: .....

MS. SARAH OCHWADA

Abstract

The nature of electronic commerce requires purchasing individuals to reveal their personal information in certain circumstances, so as to enable the execution of e-commerce transactions. E-commerce websites are also designed to gather internet user's personal information in order to personalize services and strategize relationships with their consumers. This has brought forth privacy and security concerns in relation to the collection, storage and use of individual's personal information by these entities. This study will therefore, address the nature of e-commerce highlighting the structures of contracts under e-commerce as they are the various modes of completing an e-commerce transaction. It will then discuss the type of information that is gathered by e-commerce entities while an individual is transacting online and call attention to the potential harm to privacy when this information is not protected. The study will then look into the laws that seek to protect personal information in Kenya whilst establishing the shortfalls of these laws in ensuring that personal information belonging to individuals is protected. It will then propose recommendations that are geared towards an effective data protection regime and consequently the promotion of the right to privacy, a fundamental right under Article 31 of the Constitution of Kenya.

List of legal instruments

1. Access to Information Act No. 31 of 2016 Laws of Kenya
2. Age of Majority Act Cap 33 Laws of Kenya
3. Code of Conduct and Ethics for Advocates, 2016
4. Constitution of Kenya 2010
5. Consumer Protection Act No 46 of 2012 Laws of Kenya
6. Credit and Reference Bureau Regulation, Laws of Kenya 2013
7. Data Protection Act No. 24 of 2019
8. Evidence Act Cap 80 Laws of Kenya
9. General Data Protection Regulation 2016/769
10. HIV and AIDS Prevention and Control Act No. 14 of 2016 Laws of Kenya
11. International Covenant on Civil and Political Rights, 1976
12. Kenya Information and Communication Act No 2 of 1998 Laws of Kenya
13. Kenya Information and Communication Act, Cap 411A, Laws of Kenya, 2015
14. Kenya National Patient's Charter 2013
15. Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data on September 1980
16. Private Security Regulation Act No. 13 of 2016 Laws of Kenya
17. Sale of Goods Act Cap 31 Laws of Kenya
18. Universal Declaration of Human Rights, 1948

List of Cases

B v France ECHR 40 1992

Entorres v Miles Far East [1955] 2 QB 327 Court of Appeal

Esso Petroleum v Customs & Excise [1976] 1 WLR 1 House of Lords

Fisher v Bell [1961] 1 QB 394

Godfrey v. Demon Internet Limited EWHC QB 240 23rd April, 1999

Hague v Williams 37 N.J 328, 181 A 2d 345 (1962)

Hoffman v. Supplements Togo Management, LLC 18 A.3d 210 (2011)

Hotmail Corporation v. Van Money Pie Inc., et al. C98-20064, 1998 WL 388389

Klocek v. Gateway - 104 F. Supp. 2d 1332, 2000

Masterpiece Cakeshop v Colorado Civil Rights Commission 584 U.S. ___ (2018)

McCormick v England 494 S.E.2d 431

ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1996

R v Department of H Health, ex p Source Informatics Ltd [2000] 2 WLR 940

Remsburg v Docusearch Inc 816 A.2d 1001, 1005-06 (N.H. 2003)

Richard Lloyd v Google LLC EWCA Civ 1599 2019

United States Department of Justice v Reporters Committee for Freedom of the Press 498 US 749 (1989)

Vault Corporation v. Quaid Software Limited., 847 F. 2d 255, Court of Appeals

Whelan v Roe, 429 U.S 589, 1977

Abbreviations

E-Commerce	Electronic Commerce
B2B	Business to Business
B2C	Business to Consumer
B2G	Business to Government
C2B	Consumer to Business
C2C	Consumer to Consumer
GDPR	General Data Protection Regulation
OECD	Organisation for Economic Co-operation and Development
UNCTD	United Nations Conference on Trade and Development

1.0. CHAPTER 1: INTRODUCTION

1.1. Background

In Kenya, upon the inception of the internet in the early 1990s to 2009, there was minimal internet usage as the country at the time relied on expensive satellite making connectivity to the internet an expensive affair.[1] However, in the year 2012, Kenya experienced an increase in internet penetration due to the switch from expensive internet satellite to submarine internet cables making it more affordable for individuals to access the internet.[2] The use of the internet has had a great impact on the manner in which businesses are carried out. The Traditional "brick and mortar" retail marketing has become unpopular and more businesses are opting into e-commerce for it requires low operational costs.[3] It also permits commercial transaction across cultural and national boundaries making it convenient and cost effective in expanding a business's market.[4]

The nature of e-commerce connotes that it handles a great deal of data such as payment details, user profiles and their private accounts.[5] This type of data is considered as personal information. Personal information is defined as information that can be used to identify an individual either directly or indirectly in their physical, mental, psychological, cultural, genetic, economic or social aspect.[6] Information in e-commerce is collected directly when an individual discloses their information through filing in a prerequisite form or subscribing to a website. This information is crucial for the execution of a transaction such as, identifying the individual the goods will be addressed to once dispatched, the location where the goods will be delivered, conveyance of invoices and receipts as evidence of purchase and details that facilitate payment

[1] Souter D, Kerretts M, *Internet Governance in Kenya: An Assessment for the Internet Society*, Information Communication Technology Development Associates Ltd, Kenya. 2012, 5-7
[2] African Centre for Open Governance, *African Center for Open Governance Forum on Governance and Submarine fiber-optic cable initiatives in Kenya*, 21 July 2010, Nairobi, 9
[3] Niranjanamurthy M, Kavyashree N, Dr Dharmendra C, *Analysis of E-commerce and M-commerce: Advantages, Limitations and Security issues*, International Journal of Advanced Research in Computer and Communication Engineering, Vol 2, Issue 6, June 2013, 2362
[4] Laudon C, Traver C, *E-commerce 2009: Business Technology and Society*, 5ed, Prentice Hall, 2009, 20-56
[5] Smith R, Shao J, *Privacy and E-commerce: A Consumer- Centric Perspective*, 7 Electronic Commerce Research, (2002), 89-93
[6] Article 4, General Data Protection Regulation 2016, 2016/679

such as credit card details or contact number derived from the use of mobile services such as Mpesa. Mpesa is currently the most preferred method of payment in Kenya.

Information is also collected indirectly by way of cookies,[7] that gather data as the user browses through the web. The cookies then feed this data onto the entity's web server. This is usually beneficial as it stores the user's data and prevents the user from having to re-enter their credentials.[8] They also enable online shopping carts, used by various applications like Jumia and Kilimall, to attain a similar functionality as the conventional shopping cart. Jumia and Kilimall are online shopping applications that function in a similar manner as a mall. There have a variety of goods ranging from home appliances, clothes, shoes, electronic devices among others from different sellers with different prices thereby giving an individual an option to pick goods according to their preference, pay for them and have them delivered to their preferred location. One can also opt to pay goods on delivery depending on where the goods are being purchased. Goods that are purchased from a local seller in most occasions have the option of payment on delivery while international goods strictly require payment of goods so as to enable them to be dispatched. This is to say that it allows individuals to add products to the online shopping cart as they proceed to browse in search of other items. Once an individual is content, they are able to pay for all selected goods at once. However, some individuals and organisations use third party cookies in order to obtain information from users on web pages that are not of their own and further redirecting these users to their website through personalised advertisements. There is also another method of collecting a user's information which is by use of web bugs. Web bugs are graphic images that are one pixel wide and one-pixel high which is so small that it is invisible to the naked human eye. It is placed in websites and emails for the purpose of monitoring the user, thereby gathering information of the user's behaviour.[9]

[7] A cookie is a small text file that is created by a website that is stored in a user's computer temporarily for a specified session or permanently on the hard disk. They make it possible for the website to recognize the user and keep track of their preferences.
[8] Gertjan F, *Who Left Open the Cookie Jar? A Comprehensive Evaluation of Third-Party Cookie Policies.* SEC' 18 Proceedings of the 27th USENIX Conference on Security Symposium, Baltimore Maryland, 2018, 151-153
[9] https://cyber.harvard.edu/olds/ecommerce/privacytext.html#ftc1back on 23 August 2019

1.2 Statement of Problem

E-commerce businesses are exposed to a wide variety of personal information that belongs to their consumers. This information is collected when consumers engage in e-commerce transactions. There are laws that have been enacted in a bid to regulate and protect personal information in Kenya. However, these laws are inadequate in regulating the processing of personal information in e-commerce as they are specific to what the different Acts seek to protect. An example of this is the Kenya Information and Communication Act of Kenya that is specific to the protection of personal information that is intercepted by telecommunication facilities. Another example is the Banking Act of Kenya that is specific to the protection of personal information that is disclosed to financial institutions. The lack of expansive laws specific to the regulation and protection of personal information being processed in e-commerce poses numerous challenges; It creates a purview where these entities collect consumer's personal information without their knowledge or consent. There are also circumstances where these entities fail to disclose in a clear and precise manner how they will store and use their consumer's personal information or the involvement of third parties. Personal information can more often than not be subjected to purposes other than those which they were collected for such as being sold to target market companies. [10]

This constitutes a violation of an individual's right to privacy, accorded to all citizens of Kenya under Article 31 of the Constitution of Kenya. This owes to the fact that, a consumer's right to control their personal information in relation to determining what information will be collected, how it will be used and the limitation of who will come into contact with this information is undermined.

1.3 Statement Objectives

The objectives of this study is;

a) To determine the type of personal information required to complete e-commerce transactions.

[10] Goel R, *E-commerce*, New Age International Publishers Limited, 2007, 117

b) To determine whether there are existing laws that seek to regulate and protect the processing of this personal information.

c) To assess whether existing data protection laws are comprehensive enough to adequately protect personal information specifically in e-commerce.

1.4 Hypothesis

The following are the hypothesis made in this study:

a) E-commerce entities collect, store and process personal information belonging to their consumers as they require this information for the actuation of e-commerce transactions. The unregulated processing of personal data by these entities brings about privacy and security concerns due to the possibility of abuse of personal information by these entities

b) There are no expansive laws that regulate how information in e-commerce is collected, processed and distributed in Kenya. This then makes it easy for entities to collect consumer's personal information without their consent and further failing to inform them in a clear and precise manner how their personal information will be processed and or distributed. This consequently constitutes a violation of the consumer's right to privacy.

1.5. Research Questions

a) Does e-commerce require its consumers' personal information to complete a transaction?

b) Does the unregulated processing of personal information by e-commerce business entities pose privacy and security concerns?

c) Do the existing laws adequately provide a comprehensive regulatory framework that sufficiently protects personal data?

1.6. Theoretical Framework

This Study is based on the Protection Motivation Theory. Rogers in this theory seeks to clarify the cognitive processes that conciliates behaviour when an individual is faced with fear. It posits that when an individual is faced with a threatening event they conduct themselves in an appraisal process. As per the theory there exists two appraisal modes, one focused on the risk hence, the threat appraisal and the second appraisal is focused on an individual's capacity to act against the risk, thus the coping appraisal. This in turn influences their intent to take up a precautionary approach in relation to the threat resulting to an adaptive or maladaptive behaviour.[11]

In a situation where e-commerce operates in a spectrum that offers no comprehensive data protection laws, specific to the nature of e-commerce, individuals who engage in e-commerce transactions are faced with the risk of having their privacy violated. Applying this theory to such a situation, an individual before transacting online will assess the risks of engaging in e-commerce and the unfavourable consequences that comes with it. The individual is at risk of having their privacy violated once they disclose their personal information to an online business. This gives the online business an opportunity to exploit said information to their own benefit. This could be through the collection of the individual's personal information without their knowledge and consent or using this information for purposes it was not originally obtained for, such as selling this information to target market companies at a profit. This infringes an individual right to control their information or consent to the use of their information for purposes it was not originally obtained for. An individual can deny or avoid the risk and proceed to transact online. The individual is therefore said to have adopted a maladaptive behaviour that prompts the individual to avoid taking up an action to eliminate the risk.[12]

[11]Rogers R, *A Protection Motivation Theory of Fear Appeals and Attitude Change1*, 91 Journal of Psychology, (1975), 93-114

[12] Witte K, Allen M, *A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns*, 27 Health Education and Behaviour: The Official Publication of the Society for Public Health Education, (2000), 596-610

An individual can however, contemplate the risks and begin to explore various ways of limiting or eliminating the risk while taking into account the cost of such an action.[13] There are numerous ways in which an individual can secure their personal information online, namely, by use of encryptions or anonymous search engines.[14] However, such measures are limited in e-commerce transactions because, the nature of e-commerce requires the disclosure of information that is crucial for its execution, such as the name of the individual for identification purposes, payment details and delivery locations. In a bid to eliminate the risk completely, an individual will opt out from transacting online so as not to have their privacy violated.

One of the shortcomings of this theory is the chasm between an individual's intention to act and their behaviour.[15] This denotes that, despite the fact that an individual has the intention to secure their privacy, does not necessarily mean that their intention will deter them from transacting online and run the risk of having their privacy infringed. Although upon review of evidence one can deduce that behaviour ensues intention more often than not.[16] This can be derived from a study that came to a conclusion that out of three online shoppers there were seven others who were more concerned with the privacy and security of their information and would only indulge in online shopping if the website being used assures them that there will be no privacy violations.[17]

It is important for regulators to understand why consumers act the way they do as in turn they are able to come up with adequate laws that are geared towards protecting consumers.[18] Hart states that, the law is not simply a set of commands backed up with sanctions but instead a set of guidelines for behaviour, where these guidelines are offered to steer private relations such

[13] Rogers R, *A Protection Motivation Theory of Fear Appeals and Attitude Change1*, 91 Journal of Psychology, (1975), 93-114
[14] Head M, Yuan Y, *Privacy Protection in Electric Commerce- A Theoretical Framework*, 20 Human System Management, (2001), 10
[15] P. Sheeran, Webb T, *The Intention-Behavior Gap,* 10 Social and Personality Psychology Compass, (2016), 510
[16] P. Sheeran, *Intention-Behavior Relations: A Conceptual and Empirical Review*, 20 European Review of Social Psychology, (2002), 25
[17] Harris Interactive, *Privacy Survey finds Consumers Demanding Companies do more to Protect Privacy; Public wants Company Policies to be Independently Verified*, http://www.harrisinteractive.com/news/%20allnewsbydate.asp?NewsID=429 on 20 August 2019
[18] Kenny M, Devenney J, *European Consumer Protection: Theory and Practice*, Cambridge, Cambridge University Press, 2012, 438

as contracts[19] and as such there is need for laws that regulate how online business entities process personal data belonging to their consumers.

1.7. Literature Review

E-commerce has no definite definition. Vladimir's definition of e-commerce is the sharing of business data, maintenance of business connections and the execution of business transactions by means of telecommunication networks.[20] On the other hand Kinuthia defines e-commerce as the execution of commercial ventures by use of electronic media, the internet being the most common means.[21] In the case of ***Godfrey v Deman Internet Limited,*** Justice Morland. categorized internet technology as either email, UseNet [22]or the world wide web[23]. A report by United Nations Conference on Trade and Development (UNCTD 2000) identified six channels used in e-commerce which are; electronic payment, telephone, money transfer systems such as Mpesa in Kenya, the Internet, fax and Electronic Data Interchange. [24]

Mukhopadhyay explains that e-commerce minimizes operational costs such as business start-up and travel costs, making it more appealing to businesses.[25] The benefit of shopping online is a captivating attraction to purchasers who appreciate how efficient it is to purchase some services and goods online. As Emmelhainz says, e-commerce speeds up transactions[26] and also saves up on time; this could be derived from a study done in Europe that revealed that 50% of cyber-consumers preferred e-commerce so as to save time.[27] This is quite beneficial as one need not move from one location to the next in order to get goods that they would have

[19] Hart A, *The Concept of Law*, Oxford University Press, 1961, 112-130
[20]Vladimir Z, *Electronic Commerce: structure and issues*, 1 International Journal of Electronic Commerce Research., (1996), 3-23
[21] Kinuthia J, Akinnusi D, *The Magnitude of Barriers Facing E-Commerce Businesses in Kenya*, 4 Journal of Internet and Information Systems, (2014), 12–27.
[22] UseNet is worldwide distributed discussion system that consists of a collection of online discussions that are categorized into newsgroups. Users can upload their own articles to spur up a discussion or can contribute to an already existing discussion.
[23] Godfrey v. Demon Internet Limited EWHC QB 240 23rd April, 1999
[24] United Nations Conference on Trade and Development, *United Nations Conference on Trade and Development, E-commerce and Development Report*, New York, 2002
[25] Mukhopadhyay T, Kekre S, Kalathur S, *Business Value of Information Technology: A Study of Electronic Data Interchange*, 9 Management Information Systems Research Center, University of Minnesota, (1995), 137-156
[26] Emmelhainz M, *Electronic Data Interchange: Does it Change Purchasing Process*, 23 Journal of Purchasing and Materials Management, Winter, (1987) 2-8
[27] Civic Consulting, *Consumer Market Study on the Functioning of E-commerce and the Internet Marketing and Selling Techniques in the Retail of Goods*, European Union Publications, 2015, 27

otherwise purchased online. The study also revealed that 66% of online shoppers preferred e-commerce because of lower prices.[28]

E-commerce has various models such as B2B which according to Randall, is the most frequently used[29]and it entails e-commerce transactions between businesses. The second model is the B2C that involves retail transactions between an organizations and individual shopper an example would be the Jumia application in Kenya. The third model is the C2C that operates in a similar manner as an auction where the consumers interact directly with each other in a person to person model, an example of this would be the OLX application in Kenya. The fourth model is the C2B model where the consumer determines the price of goods or services and the focus of the transactions shifts from the business selling to consumer buying an example would be fiverr.com. The fifth model is the B2G, where the government interacts directly with its citizens through availing goods and services over an electronic system an example of such a model in Kenya is e-Citizen.[30] One unique characteristic that cuts across all these models is information. Smith brings out that online businesses handle a great amount of information like payments, consumer profiles, their personal records which are ordinarily stocked directly on the business's server.[31]

A report from the USA Federal Trade Commission revealed that data is collected through direct and indirect means. Information is directly gathered when an individual knowingly subscribes to online commercial sites or purchases goods online. Such information that is gathered is the name of the individual, their email address, location and credit card details among others. Information is gathered indirectly without user's knowledge through the use of cookies which keeps track of the internet surf of users in a particular website. The report further reveals that because websites gather so much information they are capable of coming up with a complete data picture of an individual.[32]This could give rise to loss of confidentiality over personal

[28] Civic Consulting, *Consumer Market Study on the Functioning of E-commerce and the Internet Marketing and Selling Techniques in the Retail of Goods*, 27
[29] Randall H, *B2B E-Commerce: Business Models and Revenue Generating Activities*, 2000, 3
[30] Ritendra G, *E-commerce*, New Age Publishers, 2007, 8-33
[31] Smith R, Shao S, *Privacy and E-commerce: A Consumer-Centric Perspective*, 7 Electronic Commerce Research, (2007), 90-97
[32] United States Federal Trade Commission, *Privacy Online: A Report to Congress*, 1998, 3, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf on August 22 2019

information, it can also lead to discrimination is some circumstances, it makes it easy for anyone to steal the identity of the individual or commit fraud by impersonating the individual, it can also lead to damaged reputation or financial losses.[33]

The amount of personal information gathered while individuals engage in e-commerce creates uncertainty because as Bart says, revealing personal information online is considered risky due to information risk[34] . Nowak and Phelps define information risk as the uncertainty in regards to the manner in which personal data is managed by online entities that have access to it.[35] Diven brings out that consumers are vulnerable as they have little control over information collected by e-marketers beyond the purpose in which the information was initially collected.[36] An example of this is by using such information to personalise advertisements, that it deny consumers an opportunity to explore various goods by limiting them to a specified array of goods. As a result of this, the need for information privacy becomes important. Grandinetti defines information privacy as the right of an individual or organisation to control how, when and to what particular degree data in regards to them is to be transmitted to others.[37] White states that the issue in information privacy is not information disclosure this is because information is necessary for e-commerce but it is the degree of control that a consumer has over information collection and its use by other individuals engaging in e-commerce.[38] Lee proposes that when such information is collected and misused there is risk of loss of anonymity, identity theft or even fraud. Phelps and Nowak explain that such fear consequently leads to motivation among potential consumers to avoid threats associated with disclosing personal information to e-marketers. [39]

---

[33] Recital 75, *European Union General Data Protection Regulation*, 2016/679

[34] Bart, Fareena Sultan, and Urban G, *Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study*, 69 Journal of Marketing, (2005) 140–152.

[35] Nowak G and Phelps J, *Understanding Privacy Concerns: An Assessment of Consumers' Information-Related Knowledge and Beliefs*. 6 Journal of Direct Marketing, (1992), 28–39

[36] Dinev T and Hart P, *Internet Privacy Concerns and their Antecedents: Measurement Validity and a Regression Model*, 23 Behavior and Information Technology, (2004), 413–423.

[37] Grandinetti, M, *Establishing and maintaining security on the Internet*, 13 Sacramento Business Journal, (1996), 22

[38] White T, *Consumer Disclosure and Disclosure Avoidance: A Motivational Framework*, 14 Journal of Consumer Psychology, (2004), 41–51.

[39] Albarran A, and Goff D, *In Understanding the Web: Social, Political, and Economic Dimensions of the Internet*, Wiley Blackwell, 2000 135–164

As Smith states, the growth of e-commerce is dependent on security and privacy policies of a State.[40] It is therefore important to come up with a regulatory framework that regulates the manner in which information is collected, processed, used and distributed in order to create certainty in e-commerce

1.8. SCOPE AND LIMITATION

The study is aimed at determining whether regulation of personal information processed by e-commerce will positively attribute to the promotion and protection of the right to privacy. It will consist of desktop research on academic literature such as books, journals, dissertations, Statutes, case law and reports relating to the study. This study will therefore be limited to desktop research due to time constraints. There is also limited legal study done on this topic in Kenya that may affect evaluation of documented material.

1.9. CHAPTER BREAKDOWN

Chapter 1

An introduction into study and the purpose of the study. It gives the background of the study, its objectives and answers it seeks to achieve, a hypothesis and the limitations of this study. The chapter shall also include a theoretical framework and literature review that seeks to justify the need for protection of privacy in e-commerce.

Chapter 2

This chapter shall discuss e-contracts which are used in the actuation of e-commerce transactions. It will also discuss how effective they are in relation to their enforceability and validity.

Chapter 3

This chapter shall consist of a discussion on what information is collected online thereby determining that personal information is more often than not processed by online businesses.

[40] Smith R, Shao S, *Privacy and E-commerce: A Consumer-Centric Perspective*, 7 Electronic Commerce Research, 2002, 89-116

It will further define what personal information is and highlight the effects of not regulating and protecting personal information.

Chapter 4

This chapter shall consist of a discussion on the laws that have sought to protect the processing of personal information. It will highlight that the laws that are in place are not sufficient in regulating personal data.

Chapter 5

This Chapter shall give a conclusion and recommendation in relation to the protection of personal information in e-commerce.

CHAPTER 2: A COMPREHENSIVE STUDY OF CONTRACTS USED IN E-COMMERCE TRANSACTIONS.

2.0. Introduction

The previous chapter laid a foundation of this study highlighting that e-commerce entities process huge amounts of personal information that they collect directly or indirectly from individuals. It also highlighted that these entities are not being regulated and this gives rise to privacy and security concerns amongst many individuals. It also called attention to the inevitable need to have these entities regulated so as to protect individual's right to privacy.

This chapter will define e-contracts. It will look into the elements of an e-contract and the formation of e-contract. It will then involve a discussion of the types of e-contracts in relation to their validity and enforceability. This discussion is important because e-contracts are the cornerstone of e-commerce. They are used to communicate the responsibilities and duties of the contracting parties thereby facilitating e-commerce transactions in an efficient manner.

2.1. E-Contracts

A contract arises when two or more parties agree to be legally bound. It sets out tasks to be carried out by the contracting parties in a bid to satisfy a set of terms and conditions laid out in the agreement.[41] A contract has three main stages which are a) contract preparation which constitutes of specification for the fulfilment of the contract, b) Negotiation of a contractual agreement that aids in establishing a mutual plan on payment, expectations and achievements and, c) fulfilment of a contractual agreement which involves the real execution of the contractual agreement and the specified undertakings.[42]

An electronic contract, also known as an e-contract, is the computerized facilitation of a contract in a cross organisational business progression. It governs and facilitates electronic

[41] Krishna P, *From Contracts to E-Contracts: Modeling and Enactment,* 6 Information Technology and Management, (2005), 364
[42] Krishna P, *From Contracts to E-Contracts: Modeling and Enactment*, 364

trading relationships between business organisations.[43] It is modelled, specified, executed, enacted, controlled, monitored and deployed by a software system.[44]

2.2. Elements of E-contracts

The elements of an e-contract are akin to those of the conventional contract.[45] This implies that in e-contract there exists an offer which is prompted by a consumer's act of surfing through a seller's website and selecting goods and services they wish to purchase.[46] This offer is in relation to the sellers invitation to treat which is the act of displaying the sellers products as decided in the case of ***Fisher v Bell***.[47] Acceptance ought to be communicated to the individual who makes the offer as decided in the case of ***Entorres v Miles Far East***[48]**.** Acceptance is usually communicated to the consumer through emails or displaying of a requisite form on the seller's website that the consumer ought to fill in, so as to avail the goods and services to the consumer.[49] The consumer then pays for the product via the available payment methods such as the use of credit or debit cards or mobile services such as Mpesa. This is usually treated as a consideration.[50] In relation to intention to be legally bound by the contract, In ***Esso Petroleum v Customs & Excise*** the courts held that contractual agreements created in a commercial set up are presumed to be agreements that have an intent to create a legal relationship.[51] E-commerce operates in a commercial context and therefore there is a rebuttable presumption that the parties have an intent to be legally bound. However, some elements of a valid contract are difficult to ascertain due to the complexity of the internet. For one, the internet's anonymity is one of its defining characteristics, and for this reason it is quite difficult for sellers to identify who they are dealing with, consequently making it difficult to determine if the individuals have a capacity to contract.[52] This presents a challenge in circumstances where children who are below the age

---

[43] Singh R, *Law Relating to Electronic Contracts*, 2ed LexisNexis, 2015, 82
[44] Krishna P, *From Contracts to E-Contracts*: *Modeling and Enactment*, 364
[45] Singh R, *Law Relating to Electronic Contracts*, 84
[46] Pragadeeswaran M, Rajan A, *Critical Study on Different Types of E-Contract with Special Reference to the Remedies Available on Breach*, 119 International Journal of Pure and Applied Mathematics, (2018), 1731
[47] *Fisher v Bell* [1961] 1 QB 394
[48]*Entorres v Miles Far East* [1955] 2 QB 327 Court of Appeal
[49] Pragadeeswaran M, Rajan A, *Critical Study on Different Types of E-Contract with Special Reference to the Remedies Available on Breach*, 1732
[50] Section 3, *Sale of Goods Act*, Cap 31 Laws of Kenya
[51] *Esso Petroleum v Customs & Excise* [1976] 1 WLR 1 House of Lords
[52] Mann C, *The Unacknowledged Legislators of the Digital World*, Atlantic Unbound, 1999, http://www.theatlantic.com/unbound/digicult/dc991215.htm on 15 September 2019

of majority, which is the age of 18,[53] are able to purchase goods and services that are specific to adults such as alcohol and sexually related goods and services. This consequently calls for the recognition of e-contracts as a separate form of contract that is regulated on its own merits taking into consideration its shortcomings.

2.2. Formation of E-Contracts

The development of the internet facilitated a means to make electronic contracts. The Kenya Information and Communication Act recognises the formation of contracts by defining electronic signatures as "*data in electronic form affixed to or logically associated with other electronic data which may be used to identify the signatory in relation to data message and to indicate the signatory's approval of the information contained in the data message*." [54]

E-contracts are created in two ways. The first is through the use of e-mails which is common and popular among many individuals. The second way is through the use of the world wide web.[55]

2.2.1. Emails

Electronic mail is perhaps one of the principal uses of the internet and the most well-known. It is a service that facilitates the sending and receiving of messages rapidly and securely by use of electronic and computer channels. In computing, email is a system administration that enables at least two users to converse with one another by way of sending and receiving messages via a computer or comparative device.[56] Electronic mail is a significant aspect of e-commerce. This is because it enables transmitting of information, text files, advanced photographs, sound and video files over the internet. It is a quick, flexible and reliable method of correspondence. An email message comprises of two components, the message header and the message body. A party with an intention to convey business particulars via email is required to register with a Web Access Provider commonly known as Internet Service Providers (ISPs). ISPs run a mail server that is easily accessible to interested parties. Registration is done through

[53] Section 2, *Age of Majority Act*, Cap 33 Laws of Kenya
[54] Section 2, *Kenya Information and Communication Act*, Cap 411A, Laws of Kenya, 2015
[55] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, Unpublished Degree of Doctor in Philosophy in Law Thesis, Gulbarga University, 2014, 50
[56] https://www.poplarbluff.org/classes/eml_pkt.pdf on 25 September 2019

filling out a form that is readily available electronically. Upon filling out the form an electronic mail box, commonly known as an inbox, and an address specific to the user is assigned to them. The party that purpose to send an offer to a desired party, will type out the offer in their email or attach the offer to their email and then address it to the desired party who is regarded to as the recipient. In order for the email to be sent, the sender has to click the send button.[57] This actuates the transmission of the offer electronically. It is first sent to the sender's ISP who then redirects the email with the offer attached, to the recipient's ISP who then enables it to be displayed on the recipient's inbox. The recipient cannot automatically know what the email entails until they open up the email. The sender on the other hand has no way of knowing whether the recipient has received and read the email unless they get a response from the recipient. [58]

An email agreement is read by each contracting party rather than processed by a data system[59]. It can also assume any structure which the parties decide upon.[60] It is therefore the simplest form of contracting online. Moreover, an e-contract finalized through the exchange of emails is not essentially different from the traditional form of commercial contracts that relied on the exchange of letters. As a matter of fact the legal issues that surround the use of letters in contracting via the conventional way are similar to those of using emails as a method of contracting.[61]

2.2.2. Contracting through the Website

The rapid growth of e-commerce over the recent years indicates that a significant extent of transactions takes place over the internet.[62] Ordinarily, a seller would give a presentation of items on his or her site and the price of each item. A client can browse through the seller's website with the intent of knowing what products are up for sale. The client then taps on a product they find intriguing or one they purpose to purchase. If satisfied with the details and

[57] Shashikant P, *Advantages Of E-Contracts Over Traditional Contracts; E-Contracts And E-Commerce In India*, Unpublished LLM Thesis, Bharati Vidyapeeth Deemed University new Law College,2014-2015, 34
[58] Shashikant P, *Advantages of E-Contracts Over Traditional Contracts; E-Contracts and E-Commerce in India*, 34
[59] Farooq A, *Cyber Law in India: Law on Internet*, Pioneer Books, 2001, 12
[60] Shashikant P, *Advantages of E-Contracts Over Traditional Contracts; E-Contracts and E-Commerce in India*, 2015, 33
[61] Hill J, *Cross-Border Consume Contracts*, Oxford University Press, 2008, 53
[62] Burrows A, Peel E, *Contract Formation and Parties*, Oxford University Press, 2010, 4

the client is willing to purchase the goods or services, they then proceed to make an order by filling in a requisite form or clicking on the, 'I Agree' or 'I Accept' button that submits the clients desire to purchase the goods or services.[63] This is one of the commonly utilised form of e-contract used by numerous websites that offer goods and services online. In recent years the utilisation of social media platforms such as Instagram, Facebook and WhatsApp by entrepreneurs has been on the rise and is seemingly catching up to previously used contracting mechanisms. The different types of e-contracts contracted through the world wide web are shrink wrap, click wrap and browse wrap and the most current, online shopping agreements.

2.2.2.1 Shrink Wrap

Shrink wrap contracts are licence agreements or may consist of terms and condition that are of a contractual nature. In this kind of an agreements an individual is only capable of reading and accepting the terms and conditions after opening the product.[64] Consequently, a purchaser is said to have accepted the terms and conditions by using the purchased product. This is because a licenced software comes packed with a note attached at the cover of the package. The cover contains the terms and conditions for the use of the purchased software and upon opening the package, it is deemed that the purchaser has read the terms and accepted the said terms and therefore bound by those terms.[65] That being the case, it is evident that the term shrink wrap describes the plastic wrapper that is used to cover software packages. Shrink wraps are commonly used in the software industry but this is not to say that it is limited to this industry as other industries are free to utilize it.[66]

This contract is a preceding contract that is imposed upon a purchaser when they purchase a software.[67] It is normally placed on the software in a manner that the buyer of the software should notice. They are able to then read the terms and are consequently made aware that

[63] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 50
[64] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 51
[65] Shashikant P, *Advantages of E-Contracts Over Traditional Contracts; E-Contracts and E-Commerce in India,* 34
[66] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 52
[67] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 53

breaking or tearing up the package bounds them to the licence agreement of the manufacturer of the purchased software.[68]

Shrink wraps are preferred by many computer software companies.[69] This is because it enables the manufacturer of the software to retain the rights over the copy of the software by licencing the software instead of selling it to the purchaser.[70] The main clauses of shrink wraps are to prohibit the purchaser from making unauthorized copies of the software, renting the software to third parties and reverse engineering the software or modifying the software. It also limits the use of the software to one central processing unit, provides for disclaiming warranties and limits liability.[71]

The enforceability of shrink wraps is unclear in the legal arena.[72] ***Vault corp v. Quaid Software ltd***[73] was the first to legally address the enforceability of shrink warps and in this case the courts held that shrink wraps were unenforceable. In ***ProCD v Zeidenberg*** [74] the courts reconsidered and gave software companies a bit of a relief by holding that shrink wrap contracts are enforceable. Nevertheless, in ***Klocek v. Gateway*** a case that was decided on a later date, held that shrink wrap contracts are not enforceable,[75] consequently leading to the uncertainty on the enforceability of shrink wrap contracts.

2.2.2.2. Click Wraps

Click wrap contracts are on many occasions found as a component of the installation procedure of programming packages.[76] Click wraps can either be clickthrough agreement or a click wrap license agreement. The name click wrap originated from the usage of shrink wrap contracts.[77]

---

[68] Shashikant P, *Advantages of E-Contracts Over Traditional Contracts; E-Contracts and E-Commerce in India*, 34
[69] Shashikant P, *Advantages of E-Contracts Over Traditional Contracts; E-Contracts and E-Commerce in India*, 34
[70] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*,54
[71] Shashikant P, *Advantages of E-Contracts Over Traditional Contracts; E-Contracts and E-Commerce in India*, 35
[72] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 54
[73] *Vault Corporation v. Quaid Software Limited*., 847 F. 2d 255, Court of Appeals
[74] *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1996
[75] *Klocek v. Gateway* - 104 F. Supp. 2d 1332, 2000
[76] Pragadeeswaran M, Rajan A, *Critical Study on Different Types of E-Contract with Special Reference to the Remedies Available on Breach*, International Journal of Pure and Applied Mathematics, Vol 119, No 17 2018, 1737
[77] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 51

In a click wrap agreement, the user reads through the terms and conditions that are availed on the website and the user is required to express their consent by way of clicking on the 'I Agree' 'I Accept' icon or declining the purchase of a product by picking 'I Disagree'.[78] Click wraps are broadly utilized over the internet for approving access to websites, enable a user to download a software or trading a product. Click wraps require the action of the purchaser to assent to the terms and conditions of the click wrap contract.[79]

There are two types of click wraps, the first is the type and click where the individual is required to type specific words that express consent on a dialogue box that is displayed on the screen. The user then submits their consent by selecting the submit icon. This communicates that the user has accepted the terms and conditions of the contract. A user can only proceed to further engage in the website such as downloading of software or viewing sort after information once they follow this procedure.[80] The second type is the icon clicking. This is where an individual ought to express their consent by clicking 'OK', 'I Agree' or 'I Accept' interface that is displayed on the screen. An individual can express their rejection by selecting the 'Cancel' interface or by closing the window.[81]

Software developers rely on click wraps licence agreements as a means to protect software from unauthorized use, modification or copying of the software. The click wrap licence agreement grants a license to the purchaser to use the purchased software as opposed to selling the software. This enables the software developer to retain control over his or her product.[82] Most click wraps are non-exclusive licences which mean that the licensor reserves the right to license the same software to others.[83]

Click wrap agreements have various provisional clauses. There is a notice of agreement clause that states that the use of the product automatically generates consent, hence a user is regarded

[78] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 51
[79] Pragadeeswaran M, Rajan A, *Critical Study on Different Types of E-Contract with Special Reference to the Remedies Available on Breach*, 1737
[80] [80] Pragadeeswaran M, Rajan A, *Critical Study on Different Types of E-Contract with Special Reference to the Remedies Available on Breach*, 1737
[81] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 51
[82]Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 51

[83] Pragadeeswaran M, Rajan A, *Critical Study on Different Types of E-Contract with Special Reference to the Remedies Available on Breach*, 1737

as having accepted to be legally bound by the terms and condition of the program or product purchased. The retention of title clause that provides that the user of a product is in mere possession and not the owner of the product. An exclusive use clause. This clause prevents the purchaser from generating an unapproved duplicate of the product. An anti-refusal clause that stipulates that the user has no right to lend, rent or transfer a product to a third party. A clause specified to limit the usage of a program to one specific computer. An ant-reverse engineering clause that prohibits an individual from restructuring a software from the purchased software. A copyright protection clause aimed at securing protection over the design. A clause limiting liability. This clause limits the liability of the seller and confers the right to reject to a purchaser through sending back of the purchased product. Lastly click wraps provide miscellaneous clauses for instance a governing law clause, a jurisdiction clause and a force majeure clause.[84]

Click wraps are mostly preferred to shrink wraps. This is because a consumer has an ample time to go through the terms and conditions before accepting to contract and a simple act of a click of a button concludes the contract.[85] There is also some uncertainty as to whether click wrap contracts are enforceable, but most individuals are of the opinion that the nature of click wraps make them more enforceable than shrink wrap agreements.[86] In ***Hotmail Corporation v Van Money Pie***, the court held that click wraps are enforceable and for that reason the defendants herein were bound by the terms of service that were availed on the website. This was because the defendants had clicked the 'I Agree' button.[87]

2.2.2.3. Browse Wrap

In a browse wrap agreement users are not obliged to accept or reject the terms and conditions of the agreement before proceeding to use the products.[88] The terms and conditions of the use of a website or other downloadable products in a browse wrap agreement are posted on the website.[89] However, they appear as a hyperlink which can be accessed by clicking the link and

[84] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 52
[85] Shashikant P, Advantages of E-Contracts Over Traditional Contracts; E-Contracts and E-Commerce in India, 40
[86] Shashikant P, *Advantages of E-Contracts Over Traditional Contracts; E-Contracts and E-Commerce in India*, 121
[87] *Hotmail Corporation v. Van Money Pie Inc*., et al. C98-20064, 1998 WL 388389
[88] Shashikant P, *Advantages of E-Contracts Over Traditional Contracts; E-Contracts and E-Commerce in India*, 124
[89] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 55

such an action is optional.[90] In comparison to a click wrap, an express manifestation of assent by the user is not a necessary requirement, rather, use of product is sufficient enough to deduce consent on the part of the user. The use of products could be through entering the website or downloading a software.[91]

There is uncertainty as to the enforceability of browse wrap agreements just like shrink wraps.[92] The nature of browse wraps presents issues such as the irresolution as to whether a user has agreed to the terms and conditions of the agreement.[93] Therefore, courts have held that the legitimacy of browse wrap agreements depends principally on the user's undeniable or constrictive notification of the terms and conditions of the product prior to the use of the product.[94] This was similarly held in ***Hoffman v. Supplements Togo Management,*** the court held that it is difficult to come up with a conclusion that the plaintiff viewed and expressed consent to the term of use if there is lack of direct evidence that demonstrates their consent.[95]

2.3.2.4. Online Shopping Agreement

This contract facilitates the purchase of goods, home appliances, clothes, shoes among other goods available online. This type of contacts has gained and continues to gain more popularity than the other types of e-contracts. It is commonly preferred and used by many established online applications in Kenya such as Jumia, Kilimall, Masoko among others. It is commonly used in a B2C type of business structure. It involves information sharing, order, payment channels, performance of order and lastly support and services.[96]

Information sharing involves the use of application by the business to share business particulars with its potential customers. The particulars could be in the form of the company's website, online inventories, email alarms, internet publicizing, announcement sheets, message board

[90] Shashikant P, *Advantages of E-Contracts Over Traditional Contracts; E-Contracts and E-Commerce in India*, 124
[91]Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 55
[92] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 57
[93] Shashikant P, *Advantages Of E-Contracts Over Traditional Contracts; E-Contracts And E-Commerce In India*, 125
[94] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 57
[95] *Hoffman v. Supplements Togo Management*, LLC 18 A.3d 210 (2011)
[96]Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 55

frameworks, news and dialogue groups.[97] An example of this would be email alerts sent by Samsung to its users whenever a new Samsung phone has been launched.

This type of agreement also encompasses entrepreneurs that have taken advantage of social media platforms such as Instagram, Facebook and WhatsApp, which is continuously gaining popularity especially amongst the youth. Entrepreneurs on Instagram and Facebook post their products on their social page for consumers to see while those who use WhatsApp have to post their goods on their status every day as statuses have a 24-hour expiry date. This is done until the goods are sold.

Once a consumer has familiarised themselves with the product they wish to purchase they will then use the available website to order for the good. Upon placing an order online, the user then has a variety of options in which he or she will use to pay for the goods or the selected forms of payment the website requires. The most common modes of payment are through the use of credit and debit card, cash on delivery, cheques and[98] mobile services such as Mpesa which is commonly used by numerous citizens. Performance of the order is dependent on the nature of the transaction and direction provided by the consumer. The mode of fulfilment will also depend on how the e-business handles its operations as they can outsource this function to third parties.[99] Outsourcing is mostly used by individuals who operate on social media platforms mostly Facebook and Instagram. Examples of applications that are outsourced for delivery purposes are uber or safeboda. This contract has gained recognition and is enforceable.

2.3. Conclusion

E-contracts are the cornerstone of e-commerce. They are used to actuate e-commerce transactions and therefore its validity and enforceability is important in e-commerce. It is used to lay down the responsibilities and duties of each parties and also seeks to safeguard the interest of contracting parties. Taking shrink wraps and click wraps as examples, they have been commonly used by software engineers to safeguard their interest over the software they develop by prohibiting purchasing individuals from tampering with their software or availing it to third parties who have not purchased it. It also helps them to maintain control over their

[97]Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 55
[98] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 55
[99] Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, 55

software by licencing of the software instead of transferring property in their product by way of a sale. Online shopping agreement contracts have widened the scope of e-contracts by including other forms of products that could be purchased online unlike shrink wraps and click wraps that are in themselves limiting to the software industry. These contracts require one to disclose their personal information especially when physical goods are the subject matter of the contract. This is because the information is necessary in ensuring that the goods are delivered to the consumer. This suggest that there is need to come up with mechanisms that regulate the processing of information that is gathered.

CHAPTER 3: PERSONAL INFORMATION AND PRIVACY IN E-COMMERCE

3.1. Introduction

The previous chapter looked into e-contract. It attempted to define e-contracts and highlighted the elements that constitutes a valid e-contract. It then entailed a detail discussion on the formation of e-contracts and how effective these contracts are in relation to their enforceability.

This chapter will first identify the type of information that is gathered when an individual is transacting online. It will then define personal information in an attempt to illustrate that the information that these entities are exposed to are more often than not personal information. The chapter will then look into the possible dangers that arise when processing of personal information is not regulated. This chapter is important as it demonstrates the need for regulation of personal information in e-commerce.

3.2. Information Collected in E-commerce.

E-commerce businesses deal with a lot of information.[100] Information is gathered directly and indirectly. Information is collected directly where a user knowingly discloses their information such as when contacting online to purchase a good or service or when they subscribe to a commercial site. This information includes the name, email address, location and credit card details et cetera.[101] The name of the individual is necessary to identify the user for purposes of record keeping and also to identify the individual that the goods will be addressed to. Emails are of importance as it enables the business to send their electronic receipts to the user upon payment of the goods. Location is also essential for the delivery of physical goods as vendors are able to locate the drop off location. Credit card details are essential for payment of goods. Mobile phone numbers can also be used in an instance where one uses mobile services to pay for the goods such as Mpesa. Information is gathered indirectly when the user does not directly disclose this information. This information is gathered through the use of a cookie which

[100] Smith R, Shao S, *Privacy and E-commerce: A Consumer-Centric Perspective*, 7 Electronic Commerce Research, 89-116

[101] United States Federal Trade Commission, *Privacy Online*: A Report to Congress, 1998, 3, https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf on 5 November 2019,

collects information surfed by the user as the user casually browses through the website and further updates this information to the web server.[102] This is helpful to a user as they do not have to re-enter their credentials again as their information is already stored in the website's server.[103] There are third party cookies that are used by individuals and businesses to obtain information from users on websites that are not their own. They use information gathered to redirect these users to their website by using personalized advertisements. When it comes to the use of cookies, some websites disclose this to their users and also informs them of third party cookies so as to afford them the opportunity to consent while others omit this which poses a challenge, as this information is collected without the knowledge and consent of the user. Entities have also taken advantage of web bugs which are also used to collect information about users and are usually small in size and visibly invisible to the naked eye.[104]

Information that is collected is classified into, sensitive information, identification information, personal data and anonymous information. Sensitive information is that which reveals information about a person's race or ethnical background, religious beliefs, philosophical ideologies and individual beliefs, political inclinations and opinions and also information that discloses an individual's health status and history.[105] Identification information directly identifies an individual. This information is not limited to the name, address and contact number of an individual but also their DNA, identification card number and credit card details.[106] Personal data refers to data that is capable of being used to identify a specific individual. Examples of personal data includes, name of the individual, address of the individual, telephone number of the individual.[107] Anonymous information is data that cannot be directly associated to an identifiable living individual. Such information is mostly general and not specific to a certain individual in question. An example is gender of an individual or a type of disease.[108]

---

[102] Gertjan F, *Who Left Open the Cookie Jar? A Comprehensive Evaluation of Third-Party Cookie Policies,* 151-153
[103] Gertjan F, *Who Left Open the Cookie Jar? A Comprehensive Evaluation of Third-Party Cookie Policies*,151-153
[104] https://cyber.harvard.edu/olds/ecommerce/privacytext.html#ftc1back on 10 November 2019
[105] Ghani N, *Personal Information Privacy Protection in E-commerce*, 9 World Scientific and Engineering Academy and Society Transactions on Information Science and applications, (2009), 29
[106] Ghani N, *Personal Information Privacy Protection in E-commerce*, 29
[107] Ghani N, *Personal Information Privacy Protection in E-commerce*, 29
[108] Ghani N, *Personal Information Privacy Protection in E-commerce*, 29

The first three pose a risk or harm upon disclosure of such information as they are identifiable to a specific individual and therefore require protection.[109]

3.2. Personal Information

Personal information is defined as any documented data that can essentially be processed completely or in part by any programmed method. This data directly or indirectly relates to an individual. The individual is distinguishable and recognisable from that data or from any additional data in the possession of the data controller or processor who is also referred to as a data user. This includes any declaration of an individual's viewpoint in any matter and any sign relating to the intent of a data user in regard to the individual.[110] Personal information therefore encompasses information and opinions that can be used to identify an individual and the procession of that data manually or electrically.[111] Personal information is the subject of data protection. This therefore mean that the first three classifications of data which are sensitive information, identification information and personal data, that are collected in e-commerce automatically form part of subject matter of data protection. Anonymous information does not automatically fall under subject matter of data protection as it is not particularly identifiable to an individual as decided in ***R. v Department of Health, Ex Parte Source Informatics***. However, anonymity still requires duty of confidentiality.[112]

3.3. Importance of Protection of Personal Information.

The protection of personal information falls under the right to privacy which is a fundamental right accorded to all citizens of Kenya under the Bill of Rights in the Constitution of Kenya.[113] Privacy has many a time been interpreted as the right to have the ability to protect one's secrets

[109] Ghani N, *Personal Information Privacy Protection in E-commerce*, 30
[110] Section 2, Data Protection Act, United Kingdom.
[111] Madeiha I, *E-commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill*, International Review of Law Computers & Technology, 2002, 2
[112] R v Department of H Health, ex p Source Informatics Ltd [2000] 2 WLR 940
[113] Article 31, The Constitution of Kenya 2010

and also to prevent others from invading personal space.[114] With the nature of e-commerce such a definition does not encompass the protection of personal data that is disclosed as it is required and essential for completion of a transaction. A more elaborate definition of privacy would be the capability of an individual to control collection, retention and distribution of their information.[115] In order to understand the need of information privacy outside the traditional understanding of what privacy is, Solove uses the taxonomy of privacy to show the different issues that arise when personal information is concerned.[116]

3.5. Taxonomy of Privacy

The taxonomy of privacy contains four general categories. These categories involve information collection, information processing, information dissemination and invasion.

3.5.1. Information Collection

This stage involves the process of gathering data about individuals. Solove identifies two problematic ways in which information is gathered which are surveillance and interrogation. Interrogation,[117] is whereby personal information is gathered through coercion.[118] Information is gathered by means of coercion in e-commerce where entities gather more information than they ought to. Consumers feel obligated to divulge more information than they ought to in fear of not having their purchased goods delivered. This is problematic as it results to intrusion of the consumer's personal life. This also opens a purview where collected information is subjected to purposes other than that which it was said to be obtained for.[119] Surveillance,[120] is the monitoring of an individual's behaviour, their activities or information.[121] The use of cookies by businesses without notifying the user can be equated to that of surveillance. Cookies collect information as a user surfs the web and then feeds the gathered information to the web

[114] Anderson R, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wilea Computer Publishing, 2001, 612
[115] Goldberg I, Wagner D, Brewer E, *Privacy-Enhancing Technologies of the Internet*, Institute of Electrical and Electronics Engineers Compcon '97, 1997, 103-109
[116] Solove D, *A Taxonomy of Privacy*, 154 University of Pennsylvania Law Review, (2006), 478
[117] Solove D, A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol 154, 2006, 499
[118] https://wiki.openrightsgroup.org/wiki/A_Taxonomy_of_Privacy#Information_collection on 1 November 2019
[119] https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf on 2 November 2019
[120] Solove D, *A Taxonomy of Privacy*, 491
[121] https://thelawdictionary.org/surveillance/ on 1 November 2019

servers. This is beneficial to the user as they need not have to re-enter their credentials when revisiting the site. It is also beneficial for the website in offering some services such as online shopping carts. In as much as this is beneficial, some entities use these cookies without informing and seeking consent from the consumers. There is also the use of third party cookies placed by organisations or businesses on website that are not of their own in order to redirect the user to their website using personalized advertisements targeted at the user. These individuals and businesses also use web bugs which are almost invisible to the naked eye that gather information about the user by monitoring their behaviour.[122] The use of cookies without informing or seeking consent from an individual violates their right to privacy in relation to the individual's right to control their personal information.

3.5.2. Information Processing

This stage involves the storing, analyzing and manipulation of personal data. Solove identifies five ways of processing information that are problematic.[123] The first problematic way is Aggregation which is the gathering of information about an individual.[124] An example would be an application like Jumia collecting information about a consumer's recent purchase and using that information to display relevant products on its home page. In as much as this is in a positive light in ***United States Department of Justice v Reporters Committee for Freedom of the Press***, the courts held that aggregation is a violation of privacy.[125] This is because aggregation facilitates the accumulation of personal data that enables entities to come up with a user's profile. A personal profile can be used by fraudulent individuals to impersonate the individual. They can also use such a profile to damage the reputation of the individual or cause financial losses in instances where they use the individual's details to acquire property.

Identification is the second form which entails the linking of personal information about an individual to that individual.[126] Identification limits one's ability to change through self-development by tying them down to their past consequently leaving them no room to escape.[127] This was illustrated in the case of ***B v France*** that involved an application of a transgender

[122] https://cyber.harvard.edu/olds/ecommerce/privacytext.html#ftc1back on 9 November 2019
[123]Solove D, *A Taxonomy of Privacy*, 504
[124] Solove D, *A Taxonomy of Privacy*, 505
[125] United States Department of Justice v Reporters Committee for Freedom of the Press 498 US 749 (1989)
[126] Solove D, *A Taxonomy of Privacy*, 510
[127] Solove D, *A Taxonomy of Privacy*, 512

individual who had transitioned from a male to a female and wanted to change her documents to indicate that she was now female as opposed to them indicating that she was male.[128] Identification also deprives an individual their ability to remain anonymous. Anonymity protects individuals from biases and enables them to interact with others more freely.[129] The case of ***Masterpiece Cakeshop v Colorado Civil Rights Commission*** shows how biases limit how individuals interact freely, where two gay couples were denied a wedding cake because of the baker's religious bias against same sex marriage.[130]

The other way is that of insecurity.[131] In ***Whelan v Roe*** the courts held that the right to privacy also extended to an individual's interest to avoid divulging personal information.[132] Insecurity therefore, is the increase of an individual's vulnerability to the potential abuse of their personal data by entities revealing such information to third parties without the consent of the individual or the selling of such information to target market companies.[133]

The fourth problematic way is that of secondary use. This is the use of personal data for a purpose other than that which was agreed upon.[134] It pauses a harm as the user does not consent to the secondary use of their information and that there is a high possibility that the secondary use may be one that the user finds undesirable. Solove illustrates this through a case where United States military recruits' fingerprints were taken so as to facilitate the screening of their backgrounds. Their fingerprints were sent to the FBI and then incorporated the fingerprints into the FBI's criminal fingerprint records. The incorporation of their fingerprints into the criminal records was not the primary reason as to why the fingerprints were taken and any human being would not consent to having their fingerprints incorporated in a criminal database in an instance where they have not committed any crime.[135] An example of secondary use of information in e-commerce is where a vendor acquires personal data from an e-consumer which was necessary

---

[128] B v France ECHR 40 1992
[129] https://wiki.openrightsgroup.org/wiki/A_Taxonomy_of_Privacy#Information_collection on 1 November 2019
[130] Masterpiece Cakeshop v Colorado Civil Rights Commission 584 U.S. ___ (2018)
[131] Solove D, *A Taxonomy of Privacy*, 515
[132] Whelan v Roe, 429 U.S 589, 1977
[133] Solove D, *I've Got Nothing to Hid and other Misunderstandings of Privacy*, 745 San Diego Law Review, (2007), 758
[134] Solove D, *A Taxonomy of Privacy* , 520
[135] Sankar P, *DNA Typing: Galton's Eugenic Dream Realized*, in Caplan J, Torpey C, *Documenting Individual Identity: The Development of State Practice in the Modern World*, Princeton University Press 2002, 278-279

and primarily acquired for the completion of the transaction, who then decides to sell such information to target market companies.

The last problematic way is exclusion, whereby the owner of the personal information is not given notice thereby depriving them of their ability to access their information and also to have a say in how their information is used.[136]

3.5.3. Information Dissemination

This stage involves ways in which personal information is revealed, transferred or threatened to be transferred to others. Solove identifies seven problematic ways in which information is disseminated.[137] The first is breach of confidentiality. In ***McCormick v England*** the courts held that unauthorized disclosure of confidential information constitutes a breach of confidentiality.[138] The second way is disclosure that constitutes revealing of personal information.[139] The difference between breach of confidentiality and disclosure is that in breach of confidentiality one violates trust and is more so prevalent in patient doctor relationships as seen in the case of ***McCormick v England*** whereas in disclosure the harm caused is usually that of one's reputation.[140] One situation could be where an individual whose past online activities, such as those considered repugnant like acquiring the services of call girls, are disclosed to the public. Despite changed behaviour their reputation is damaged due to the disclosure of past mistakes making individuals prisoners of their past.[141] Disclosure can also pose a threat to an individual's personal security. The case of ***Remsburg v Docusearch Inc***, illustrates this, where a man acquired the employment address and social security number of a lady by the name Lynn on the database of the defendant. The man stalked and killed the lady.[142]

The third way is exposure which constitutes the revelation of certain physical and emotional characteristics about a person. Such information is considered by the owner of said information to be that of an embarrassing or humiliating nature.[143] This could be through the revelation of

---

[136] Solove D, *A Taxonomy of Privacy*, 521
[137] Solove D, *A Taxonomy of Privacy*, 523
[138] McCormick v England 494 S.E.2d 431
[139] Solove D, *A Taxonomy of Privacy*, 528
[140] https://wiki.openrightsgroup.org/wiki/A_Taxonomy_of_Privacy#Information_collection on 1 November 2019
[141] Solove D, *A Taxonomy of Privacy*, 531
[142] Remsburg v Docusearch Inc 816 A.2d 1001, 1005-06 (N.H. 2003)
[143] Solove D, *A Taxonomy of Privacy*, 533

certain information in relation to the purchasing of certain goods and services that implies that an individual is in a certain situation. These situation as Solove brings out are, but not limited to, strong display of emotions, nudity, bodily functions and injury. They goods are thereby considered to be that of a sensitive nature such as antiretroviral drugs that suggests that the person is HIV positive. An individual could be humiliated when information relating to the purchasing of an online book or service that helps them deal with certain traumas is exposed to the public. This is due to social constructs that encourage the concealment of such information as a way of preserving human dignity. Divulgence of this information that is considered humiliating or embarrassing by e-commerce entities make it hard for individuals to integrate into society once they feel that they have been exposed. [144]

The fourth way is increased accessibility. Increased accessibility does not involve direct disclosure of information but makes information that was already in the public sphere more accessible thereby such information can be easily exploited for purposes other than that which it was made public for.[145] The courts recognised the harm of making information easily accessible in the case of ***United States Department of Justice v Reporters Committee for Freedom of Press*** where it distinguished the difference between scattered information found in courthouse records and a summary of aggregated information posted online.[146]

The fifth way is that of blackmail. Blackmail is where an individual threatens to reveal personal information about an individual if they do not accede to their demands in which many a time was through payment of a lot of money. The sixth way is through appropriation which is similar to identity theft where one uses personal information they gathered to take up the consumer's identity and likeness for own purpose or goals in order to fit into society. The seventh way is distortion. Distortion involves the manipulation of the way a person is regarded to by others. Distortion usually involves false information about an individual and is normally covered under defamation cases.[147]

[144] Solove D, *A Taxonomy of Privacy*, 534
[145] Solove D, *A Taxonomy of Privacy*, 537
[146] United States Department of Justice v Reporters Committee for Freedom of the Press 498 US 749 (1989)
[147] Solove D, *A Taxonomy of Privacy* , 539-543

3.5.6. Invasion

This stage constitutes of intrusion and decisional interference. This stage is as a result of the other stages. Invasion is the direct disruption of an individual's life through intrusion which is directly interfering with one's personal space on a day to day basis. This could be through the disclosure of personal information that is gathered in an e-commerce transaction. It can also arise when entities opt not to use least intrusive measures in gathering information thereby collecting more information than they ought to in an e-commerce transaction. Decisional interference is where one uses information about another person to regulate their life and make important decisions on their behalf.[148] Search engines is an example of a mechanism that more often than not is used to gather information about a user's surfs and stores them. They will always remind a user of sites they frequent. This does not deny the individual the opportunity to discover other sites with more affordable items that are of better quality, but it limits the consumers to specific sites.

Each and every stage of the taxonomy brings out the possible harms that an individual may face when their personal information is at play. This information is subject to be exploited unless there are laws and policies put in place that protect exploitation of personal information by holding businesses accountable for any violation. This will in turn protect an individual's right to privacy.

3.7. Conclusion

E-commerce transaction is reliant on the divulgence of a lot of personal information from its consumers. This information is necessary for completion of transactions such as credit card details for payment of goods and services online. E-businesses collect a lot of personal information and lack of data protection laws and policies open up doors for exploitation of consumer personal information.[149] Every individual has a right to privacy that allows them to have control over how their information is collected and used.[150] This right is a necessary condition for an individual's autonomy which is important for individuals so that they are able

[148] Solove D, *I've Got Nothing to Hid and other Misunderstandings of Privacy*, 759
[149] Guo M, *A Comparative Study on Consumer Right to Privacy in E-commerce*, 3 Modern Economy (2012), 403
[150] Goldberg I, Wagner D, Brewer E, *Privacy-Enhancing Technologies of the Internet*, 103-109

to develop their personality without fear of judgment from other individuals.[151] Moreover, protection of personal information by online businesses creates trust among consumers who become more willing to transact online and as a result economic development of a country.

[151] Blume P, *Data Protection and Privacy- Basic Concept in a Changing World,* Scandinavian Studies in Law, (2010), 153

CHAPTER FOUR: LEGAL FRAMEWORK OF DATA PROTECTION IN KENYA

4.1. Introduction

The previous chapter looked into the type of information that is collected in e-commerce and identified that personal information was one of the information that entities that engage in e-commerce are exposed to. The chapter also discussed the possible harms that one could be exposed to when personal information is not protected through the use of the taxonomy of privacy.

This chapter provides a comprehensive legal framework on data protection in Kenya. It is important to note that at the commencement of this study the Data Protection Act of 2019 had not been enacted. However, there were laws in place that sought to protect personal information. This chapter shall therefore, identify the different legislations that have attempted to protect personal information in Kenya, before the enactment of the Data Protection Act of 2019. It will then look into the provisions of the Data Protection Act identifying the positive and negative attributes of the Act in relation to the protection of personal information in e-commerce. This chapter is important in identifying whether the laws are adequate in guaranteeing that personal information of Kenya Citizens are protected and regulated.

4.2. Data Protection Laws in Kenya before The Data Protection Act 2019

In Kenya, before the Data Protection Act of 2019 was signed into law, there were no elaborate laws that guaranteed data protection. However, there were laws put in place to protect personal information. These laws were not adequate in protecting personal information in e-commerce. This is because the provisions were specific to what the various Acts sought to regulate such as the telecommunication industry. In as much as the Constitution recognizes this right, there ought to be mechanisms put in place so as to ensure that it is implemented.

4.2.1. The Constitution of Kenya 2010

The Constitution of Kenya is the supreme law of the land.[152] Article 31 provides for the right to privacy for every Kenyan citizen in relation to not having information about "their person, their home, property, possession, information relating to their family or personal affairs required or revealed and lastly not to have the privacy of their communication infringed." Moreover, the Constitution under Article 2 facilitates for the application of general rules of international Law in Kenya. [153] Additionally, international conventions or treaties ratified by Kenya, are to be considered as part of Kenya's law.[154] Kenya has signed the Universal Declaration of Human Rights that advocates for the right of privacy.[155] Similarly, Kenya has ratified the International Covenant on Civil and Political Rights that in like manner advocates for the right to privacy. [156]

4.2.2. The Kenya Information and Communications Act

The Kenya Information and Communication Act was established to facilitate the development of the information and communication sector in Kenya.[157] Section 31of The Act penalises the unlawful interception of a message sent and the disclosure of the contents of a message intercepted through a licensed telecommunication.[158] A telecommunication license is a document that authorizes an entity to provide telecommunication services and enables the management telecommunication establishments. The document contains terms and conditions relating to the license and rights and duties of telecommunication operators. [159]The act further inflicts a penalty on unauthorized access to, and interception of computer services.[160]

4.2.3. The Access to Information Act

The Access to information Act was enacted in pursuit of Article 35 of the Constitution of Kenya that states that every citizen of Kenya has a right to access information held by the State or that

[152] Article 2(1), *The Constitution of Kenya*, 2010
[153] Article 2(5), *The Constitution of Kenya*, 20102
[154]Article 2(6), *The Constitution of Kenya*, 2010
[155] Article 12, *Universal Declaration of Human Rights*, 1948
[156] Article 17, *International Covenant on Civil and Political Rights*, 1976
[157] *Kenya Information and Communication Act*, Cap 411A, Laws of Kenya, 2015
[158] Section 31, *Kenya Information and Communication Act*, Cap 411A of 1998
[159] Intven H, Tetrault M, *Telecommunication Regulation Handbook, Licensing Telecommunication Services*, https://www.itu.int/ITU-D/treg/Documentation/Infodev_handbook/2_Licensing.pdf on 5 January 2020
[160] Section 83W, *Kenya Information and Communication* Act, Cap 411A of 1998

which is held by another individual that is necessary for one to achieve their fundamental rights and freedoms. It also provides for the right to access information for the purpose of correction or deletion of inaccurate information that affects the person.[161] The Act therefore, provides a legal framework for both public and private entities to disclose information in line with the constitution for the purpose of accountability and transparency. [162]

4.2.4. Consumer Protection Act

The Act was enacted with an objective of realizing Article 46 of the Constitution of Kenya that provides for consumer protection.[163] Section 86 of the Act states that information that is gathered while administering the Act should not be revealed unless an individual consents to it or otherwise as provided for in the Act.[164] Licensee should not monitor, disclose or allow any person to monitor or disclose the content or any information of any subscriber transmitted through licensed systems of interception or surveillance of communications and related data[165]

4.2.5. Private Security Regulation Act

The Act was enacted to regulate the private security industry and to also provide a framework for cooperation of private security industries with the National Security organs in Kenya. Section 42 of the Act provides for access to information and places an obligation on the Private Security Regulatory Authority to publish information in a manner that respects and upholds human rights and fundamental freedoms such as that of the right to privacy.[166] The Act also provides that information collected during the entry of an individual into a building ought to be used for the purpose of identification and not for any other purpose. [167]

4.2.6. HIV and AIDS Prevention and Control Act

This Act provides for confidentiality measures in relation to HIV and AIDS prevention, control and management under part V of the Act. Section 19 provides that the Minister in charge of Health ought to prescribe privacy policies for the collection, recording, storage and security of

[161] Article 35, *Constitution of Kenya* 2010
[162] Section 3, *Access to Information* Act No. 31 of 2016
[163] Article 46, *Constitution of Kenya*, 2010
[164] Section 86, *Consumer Protection Act* No. 46 of 2012
[165] Section 15, *Consumer Protection Act* No. 46 of 2012.
[166] Section 42, *Private Security Regulation Act* No. 13 of 2016
[167] Section 48, *Private Security Regulation Act* No 13 of 2016

information records or forms that are used in the testing of HIV or any other related medical assessments and that any individual related with this should conduct themselves in accordance with the privacy policies.[168] The Act further provides that no one has the right to disclose any information relating to an individual's HIV test result unless the individual consents to it or otherwise as provided under Section 22 of the Act[169]. Disclosure of this information results to an offence.[170]

4.2.7. Financial Acts

The Banking Act of Kenya, as per Section 31, prohibits publishing of information that reveals the financial affairs of an individual unless the individual through a written consent permits such a publication.[171]

The Credit Reference Bureau Regulations, gives the Central Bank of Kenya the mandate to revoke of licenses granted to Bureaus when it consistently fails to protect the confidentiality of information collected.[172] It also places an obligation to Bureaus to maintain a duty of confidentiality with regards to the information that is disclosed to them.[173] The Bureaus also protect confidentiality of their customers and can only report or reveal such information to the customer, Central Bank of Kenya, a requesting subscriber, a third party authorized by the customer and as required by law.[174]

4.2.8. Professional codes of ethics

Professional codes of ethics have also been used in protection of personal information. Rule 7 of the Code of Conduct and Ethics for Advocates provides for Advocate Client privilege. This places an obligation on advocates not to reveal information that is communicated to them by the client. This is necessary for the advancement of justice and ensuring that a client can fully confide in their advocate.[175] The basis of this rule is based on Section 134 of the Evidence Act that prohibits the disclosure of information communicated to an advocate by their client unless

[168] Section 20, *HIV and AIDS Prevention and Control Act* No. 14 of 2016
[169] Section 22, *HIV and AIDS Prevention and Control Act* No. 14 of 2016
[170] Section 22, *HIV and AIDS Prevention and Control Act* No. 14 of 2016
[171] Section 31, *Banking Act* Cap 488, No 4 of 2012
[172] Section 12, *Credit and Reference Bureau Regulation*, 2013
[173] Section 27, *Credit and Reference Bureau Regulation*, 2013
[174] Section 26, *Credit and Reference Bureau Regulation*, 2013
[175] Rule 7, *Code of Conduct and Ethics for Advocates*, 2016

the client expressly permits the disclosure. This privilege does not cease when an advocate retires but it does not protect communication made in furtherance of a crime.[176]

We also have the Doctor Patient Privilege that is essential to patients seeking medical attention so as not to have individuals worry that their condition will be disclosed to others. This is also a right provided to patients as per the Kenya National Patients' Charter.[177] In the case of ***Hague v Williams*** the courts held that a patient should be given the opportunity to disclose his or her symptoms without fear that the information disclosed will be let out to the public.[178]

4.3. Data Protection Act 2019.

In May 2018, the Information, Communication and Technology Cabinet Secretary Joe Mucheru shaped a taskforce to build up a Policy and Regulatory Framework for Privacy and Data Protection in Kenya. This taskforce was mandated to take reasonable measures through research and audits to ensure that they come up with a data protection framework suitable to protect personal information of the citizens of Kenya.[179] The taskforce also involved public participation a right granted to all Kenyan citizens under the constitution of Kenya,[180] where interested parties were given an opportunity to comment on the proposed Data Protection Bill by suggesting various areas that needed amendments.[181] A final and revised data protection bill namely the Data Protection Bill of 2019, was presented before parliament and published in The Kenya gazette on the 5th of July 2019.[182] The Bill was then signed into law by the President, Honourable Uhuru Kenyatta on the 8th of November 2019 and is to commence on the 25th of November 2019. [183]

---

[176] Section 134, *Evidence Act* Cap 80 Laws of Kenya

[177] Ministry of Health, Kenya National Patient's Charter, http://medicalboard.co.ke/resources/PATIENTS_CHARTER_2013.pdf on 20 November 2019

[178] *Hague v Williams* 37 N.J 328, 181 A 2d 345 (1962)

[179] Authority of the Republic of Kenya, *Kenya Gazette,* Nairobi, May 11 2018 file:///C:/Users/Hp/Downloads/Vol.CXX-No_.56_.pdf on 20 November 2019

[180] Article 2(1)(2), Constitution of Kenya 2010

[181] https://ca.go.ke/wp-content/uploads/2018/09/Public-Notice-On-Data-Protection-Bill.pdf on 20 November 2019

[182] Authority of the Republic of Kenya, *Kenya Gazette*, Nairobi, July 5 2019 file:///C:/Users/Hp/Downloads/Vol.CXXI-No_._85_.pdf on 20 November 2019

[183]Authority of the Republic of Kenya, *Kenya Gazette*, Nairobi, November 15 2019 file:///C:/Users/Hp/Downloads/Vol.CXXI-No_.156_.pdf on 20 November 2019

4.4. Importance of The Data Protection Act 2019 to E-Commerce

The enactment of the Act was a step in the right direction. The Act seeks to promote and protect the privacy of Kenyans [184]as it sets to implement Article 31 (c) and (d) of The Constitution of Kenya that confers the right not to have one's information regarding their family or personal affairs unnecessarily called for or disclosed. The Act also establishes the office of the Data Protection Commissioner under Part Two of the Act, which is of the status of a body corporate.[185] The Act also sets out the functions of the office of the Data Commissioner[186] and Data Commissioner, [187]as being those which ensure that personal data will be protected in accordance with the provisions provided for in The Act. The Act also seeks to set out the rights and duties of data subjects and data controllers in relation to data processing and other surrounding issues.[188]

4.5. Positive Attributes of The Act to E-Commerce

The Act defines personal data as information that belongs to a data subject. It involves information that can be used to identify the data subject such as "*a name, identification number, location details, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural, social or social identity."*[189] This definition is essential in establishing what constitutes personal information as per The Act. It is therefore without bias to conclude that from this definition, the nature of information e-commerce is exposed to, more often than not, is personal information and as such, subject to protection from possible exploitation. However, information collected is necessary in facilitating that e-commerce businesses survive and thrive as personal information in this digital age has become a crucial resource as was oil in the past.[190] Taking this into account the Act's approach in protection of personal information is not in relation to the exclusion of personal information in e-commerce but the regulation of personal information that is processed through the;

[184] Section 3, *Data Protection Act* No. 24 of 2019
[185] Section 5, *Data Protection Act* No. 24 of 2019
[186] Section 8, *Data Protection Act* No. 24 of 2019
[187] Section 9, *Data Protection Act* No. 24 of 2019
[188] Section 3, *Data Protection Act* No. 24 of 2019
[189] Section 2, *Data Protection Act* No. 24 of 2019
[190] http://www.ict.go.ke/wp-content/uploads/2018/08/Kenya-Data-Protection-Policy-2018-15-8-2018.pdf on 3 December 2019

"Collection, recording, organization, structuring; Storage, adaption or alteration; Retrieval. Consultation or use; Disclosure by transmission, dissemination, or otherwise making available; Alignment or combination, restriction, erasure or destruction."[191] by data controllers and processors who the Act recognizes as "*natural or legal persons, public authorities, agencies or other bodies that operate alone or jointly with others"* that are in contact with personal information. The difference between the two as brought out by the Act is that controllers determine the reason why personal data is to be processed and the manner in which it will be processed while processors process information on behalf of data controllers.[192]

The Act provides principles under Section 25 that data controllers and processors ought to abide by while processing personal information belonging to data subjects. These principles are:

a) *"processed in accordance with the right to privacy of the data subject;*
b) *processed lawfully, fairly and in a transparent manner in relation to any data subject;*
c) *collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;*
d) *adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;*
e) *collected only where a valid explanation is provided whenever information relating to family or private affairs is required;*
f) *accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;*
g) *kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and*
h) *not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject."*[193]

[191] Section 2, *Data Protection Act* No. 24 of 2019
[192] Section 2, *Data Protection Act* No. 24 of 2019
[193] Section 25, *Data Protection Act* No. 24 of 2019

These principles comply with the European General Data Protection Regulation that came into force on May 2018[194] and the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data that came into force on 23rd September 1980.[195] These principles are important as they bestow duties that data controllers and processors ought to abide by in order for them to process personal data belonging to a data subject without violating their right to privacy and other rights in relation to data protection.

a) Principle of lawfulness, fairness and transparency

This principle places an obligation on data controllers and processors to process data in accordance to the rule of law while upholding the virtues of fairness and transparency.[196] Firstly, the data controller or processor ought to inform the data subject in detail on how their personal data will be processed and who will be carrying out this act. This further imparts a responsibility to communicate to the data subject the existence of third parties that will be involved or will be in contact with, the data subject's personal information.[197] This ensures that personal data is processed in a fair and transparent manner. Secondly, personal data is processed in a lawful manner when the data controller and processor seeks consent from the data subject before proceeding to process their personal information.[198] Consent is not absolute in all cases as data subjects have a right to determine that only part of their personal data can be processed.[199]

b) Principle of purpose limitation.

This principle bestows a responsibility on data controllers and processors to, clearly define and explain to the data subject the purpose of processing their personal data. It further obliges them to, eschew processing personal data in a manner that is inconsistent with the purpose it was initially obtained for.[200] This principle does not explicitly bar data controllers and processors

[194] General Data Protection Regulation 2016/679 on May 2018
[195] Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* on September 1980
[196] Section 25, *Data Protection Act* No. 24 of 2019
[197] Section 29, *Data Protection Act* No. 24 of 2019
[198] Section 30, *Data Protection Act* No. 24 of 2019
[199] Section 29, *Data Protection Act* No. 24 of 2019
[200] Section 25 *Data Protection Act* No. 24 of 2019

from exercising secondary use of personal data. Moreover, there are two acceptable instances where personal data can be subject to secondary use. One instance is where data controllers or processors seek consent from a data subject so as to further utilize their information for purposes other than those initially procured for.[201] The other instance is when the secondary use of personal data is required by the authority of the law in occasions of national security, public interest, requirement by written law or a court order.[202]

c) Principle of minimalism

This principle requires data controllers and processors to ensure that, personal data collected is sufficient, relevant and specific to the purpose in which it is being obtained for.[203] This connotes that data controllers and processors ought to employ the least intrusive mechanisms while collecting personal data. This is important as it precludes online business owners from gathering additional data that may in turn be used for purposes other than that which it was acquired.[204]

d) Principle of Accuracy

Data controllers and processors have a responsibility to ensure that personal data that is being processed is accurate, complete and kept up to date.[205] This principle reaffirms the rights conferred to data subjects that grants them access to their personal data for the purpose of correcting or deleting erroneous information.[206] This principle not only ensures that no harm befalls a data subject due to inaccurate data but also increases the efficiency of an online business. In an occasion where a consumer relocates, they are able to update this information and this enables the business to deliver the goods to the correct location.

e) Principle of storage limitation

[201] Section 30, *Data Protection Act* No. 24 of 2019
[202] Section 51, *Data Protection Act* No. 24 of 2019
[203] Section 25, *Data Protection Act* No. 24 of 2019
[204] https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf on 20 November 2019
[205] Section 25, *Data Protection Act* No. 24 of 2019
[206] Section 29, *Data Protection Act* No. 24 of 2019

This principle requires data controllers and processors to only store personal data for a period of time that it is required for the data to be processed for the purpose it was acquired for.[207] This ensures that data controllers and processors delete personal data once this purpose is realized. This precludes them form using this personal data for purposes it was not obtained for.

f) Principle of integrity and confidentiality

This principle is not provided for under Section 25 as the other principles of processing personal information however it is provided under Section 41 and 42 of the Act. This principle ensures that personal information belonging to a data subject is protected by security procedures that ensure that the data is not accessed by unauthorized entities, used, disclosed, lost or damaged.[208] These security measures could be in the form of physical means such as the use of identification cards, organisational means such as the use of access controls, information means like enciphering which is the conversion of texts to codes, technical means like encryptions and anonymisation.[209] In an instance where there is a breach, the Act provides for the communication of this breach to the data subject as soon as possible. [210]

These principles ensure that entities that process personal data in e-commerce; notify the individual, use the information for the specific purpose that the consumer consents to and once that purpose is achieved the entities ought to dispose of this information. This affords consumers the right to be in control of the collection of their data and how it is used.

4.6. Negative Attributes of the Data Protection Act to E-Commerce

The Office of the Data Protection Commissioner under part two of the Act is established as a body corporate.[211] This status denies the office the financial and personal independence it requires to execute its mandate. Financial independence ensures that the office acquires sufficient funds that will enable them to employ their functions without any difficulty. Personal

[207] Section 25, *Data Protection Act* No. 24 of 2019
[208] Section 41 *Data Protection Act* No. 24 of 2019

[209] https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf on 21 November 2019
[210] Section 43, *Data Protection Act* No. 24 of 2019
[211] Section 5, *Data Protection Act* No. 24 of 2019

independence ensures that they are able to elect individuals on their own accord thereby minimizing manipulation from various sectors of the state. This ensures that the office is not subject to any control by any entities or persons in authority and is able to execute its mandate efficiently without major financial drawbacks.[212]

Section 25 of The Act provides for principles of data protection that complies with the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the European GDPR however, it fails to recognize the principle of accountability. The principle of accountability as per the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data states that *"A data controller should be accountable for complying with measures which give effect to the principles."*[213] This principle ensures that data controllers demonstrate their compliance with their obligations to process personal information belonging to a data subject, in accordance with the other principles. They ought to be able to account for in detail, backed up with proof that they respected the data subject's privacy while processing their personal information. This principle plays a crucial role in the investigation of breaches and ensures that entities that violate data protection laws are held accountable for their actions.

Section 26 of the Act provides for the rights of data subjects that include the *"a) right to be informed of the use to which their personal data is to be put; b) to access their personal data in the custody of data controller or data processor; c) to object to the processing of all or part of their personal data; d) to correction of false or misleading data; e) to deletion of false or misleading data about them."* [214] This section neglects to provide for the right to effective remedy and the right to compensation. The right to an effective remedy is by itself a secondary right and ensues a violation of a human right.[215] Article 2 of the ICCPR states that individuals whose human rights have been violated are entitled to an effective remedy.[216] The right to privacy is a fundamental human right that is provided in the Constitution of Kenya. It is also

[212] Omollo J, *Fourth Arm of the Government? Commissions and Independent Offices in Kenya*, 2014 https://www.academia.edu/7932670/THE_FOURTH_ARM_OF_GOVERNMENT_COMMISSIONS_AND_INDEPENDENT_OFFICES_IN_KENYA on November 25 2019
[213] Article 14, *Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* September 1890
[214] Section 26, *Data Protection Act* No. 24 of 2019
[215] Agbor A, *Pursuing the Right to an Effective Remedy for Human Rights Violation in Cameroon: The Need for Legislative Reform* http://dx.doi.org/10.17159/17273781/2017/v20i0a1764 on 30 November 2019
[216] Article 2, *International Convention on Civil and Political Rights*

provided under Article 17 of the ICCPR. This right places an obligation upon States to ensure that a remedy is enforced whenever a human right is violated.[217] This right therefore accords an individual the liberty to submit a complaint of a perceived breach of their rights by data controllers or processors to a relevant authority. The relevant authorities then ought to investigate the matter and sanction entities once there is evidence of a breach or violation of a data subject's rights.[218] The data subject ought to be compensated for damages that they suffered due to the violation. In the case of ***Richard Lloyd v Google LLC*** the court held that compensation for breaches of data protection legislation, that is resultant in a loss of control of personal data, sought through a representative action can be awarded without proof of distress or any material damage.[219]

Section 28 (2) of The Act provides for instances where a data controller or processor collects data indirectly. Subsection 2(a) and (b) provides that data can be collected indirectly when the data is in public record and when it is deliberately made public respectively. This provision is problematic as it makes information that is in public easily accessible to data controllers and processors. This opens a purview where data controllers need not seek consent to collect such information and places individuals at a position of possible abuse of their personal information. It also opens up a possibility where these entities can aggregate one's personal information thereby coming up with a profile based on what is available on public record.

Section 31 of The Act provides for Data Protection Impact Assessment for instances where data controllers and processors are processing information that has a high risk potential.[220] This is in a positive light however a data protection impact assessment should be conducted by every entity that processes personal information. This is to ensure that these entities comply with the provisions of the Act.

4.7. Conclusion

The laws that provided for the protection of personal information before the enactment of the Data Protection Act were specific to only limited areas in which the Acts regulated and were

[217] Article 17, *International Convention on Civil and Political Rights*
[218] United Nations Human Rights Committee, General comment no. 31 [80], *The nature of the general legal obligation imposed on States Parties to the Covenant*, 26 May 2004
[219] *Richard Lloyd v Google* LLC EWCA Civ 1599 2019
[220] Section 31, *Data Protection Act* No. 24 of 2019

therefore not adequate in ensuring that personal information of individuals in e-commerce were protected. The Data Protection Act is therefore a step towards the right direction as it provides a more comprehensive framework for the protection of personal information. However, the Act has its shortfalls such as the status of the office of the Data Protection Commissioner that denies the office the level of independence it requires in order for it to sufficiently execute its functions. There are also some provisions that ought to have been included in the Act that were omitted. An efficient data protection regime operates on a spectrum that enables data subjects to report violations of their rights and the ability to hold these entities accountable for this breach. As the right to privacy is a fundamental right and it ought to be safeguarded as any other right that is provided under the Constitution of Kenya

CHAPTER FIVE: CONCLUSION AND RECOMMENDATION

5.1. Introduction

The advent of the internet saw to the development of e-commerce. E-commerce has gained popularity amongst many entrepreneurs due to its low operational costs and the ability to expands one's business across cultural and geographical boundaries. Consumers are also attracted to e-commerce due to its convenience as they need not move from one location to another in order for them to purchase a good. The nature of e-commerce connotes that it handles a great deal of personal information that belongs to their consumers.

The findings in this study sought majorly to answer the question of regulation of personal information in e-commerce. This question mostly arose due to the nature of e-commerce. E-commerce transactions require information so as to enable the execution of its transactions. It is therefore apparent that there is a need of regulations on how this information is collected used and distributed by these entities in a manner that 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 e-commerce entities.

5.2 SUMMARY FINDINGS

The focal point of chapter one brought out that in spite of the benefits e-commerce has to offer it handles a great deal of personal information. This information is not regulated by any laws or policies and therefore there exists a possibility of exploitation of personal information by entities that conduct e-commerce and this is a challenge both in the development of e-commerce that relies on the trust of its consumers and to the privacy of unsuspecting consumers.

Chapter two looked into the nature of contracts in e-commerce, highlighting the elements and the difficulty in ascertaining some of the elements. The chapter also looked into the available e-contracts that are used in e-commerce transactions and how effective they are in e-commerce transactions. This study revealed one major drawback when it comes to e-contracts which is the uncertainty when it comes to the enforcement of e-contracts. This chapter was important because e-contracts facilitate e-commerce transactions.

Chapter three investigated the type of information that is collected in e-commerce. It reaffirmed that e-commerce transactions handle a great deal of personal information that is gathered directly and indirectly. It used the taxonomy of privacy to demonstrate that the lack of regulations in relation to personal information poses a danger on the privacy of an individual.

Chapter four undertook to look into the laws that seek to protect personal information from exploitation. This study commenced when the Data Protection Act 2019 had not been enacted and therefore it looked into the laws that regulated personal information before the Act which were not sufficient as they involved provisions specific to the sector they were implemented to regulate. However, the chapter also looked into the Data Protection Act of 2019 highlighting its positive attributes and negative attributes that pose a challenge in safeguarding personal information belonging to data subjects.

5.3. Conclusion

The hypothesis that e-commerce handles a great deal of personal information and therefore there is need for regulation of personal information in this regard had been proven. The nature of e-commerce is reliant on personal information for execution of its transactions and also to increase its efficiency. However, if the processing of personal information is not regulated, consumers are faced with the possibility of having their privacy violated.

The hypothesis that there are no expansive laws that regulate the processing of personal information is not true. This is because the Data Protection Act of 2019 was recently enacted and it seeks to regulate the processing of personal information by entities that are exposed to this information, e-commerce being one of the areas the Act will regulate due to its nature.

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 recognition of e-contracts in Kenya so at to enable individuals to use these contracts to transact online. This recognition is essential in that it will be specific to the nature of e-commerce taking into account the unique nature of e-commerce and the difficulties in ascertaining some essential elements of the conventional contract.

b) The office of the Data Protection Commissioner should be established under chapter 15 of the Constitution of Kenya that establishes Commissions and Independent offices. This will enable the office to receive the financial and institutional independence it requires to execute its functions without influence from state parties.

c) The inclusion of the right to effective remedy and compensation of data subjects under Section 26 of the Data Protection Act. This ensures that data subjects are compensated for violation of breach of personal data by entities that process their data

d) The removal of section 28 (2)(a) of the Data Protection Act that provides that entities that process personal data can indirectly access a data subject's personal data that is in public record. This implies that a data subjects has automatically consented to the further processing of their personal information that is stored in public records. This provision is problematic in that it makes personal data easily accessible to entities who may exploit this opportunity and accumulate a data subject's personal information, aggregate it in order to come up with a profile on the individual.

e) The amendment of section 28 (2)(b) of the Data Protection Act that provides that entities that process personal data can indirectly access a data subject's personal data which they deliberately made public. This is because the term deliberately should not be used as a justifiable reason to collect data subject's personal information. This provision should include a more limiting approach and require that entities inform data subjects that their data is being processed.

f) An amalgamation of a self-regulatory approach and governmental approach in that entities that process data ought to adopt privacy policies in their businesses that entail; Notice and awareness, Consent that involves an Opt in or Opt out, Access and Accuracy, Data Security and Integrity, Redress and enforcement. This affords consumers the right to report perceived violations to the businesses so as to try and seek redress before they opt to seek redress from other authorities.

BIBLIOGRAPHY

Books

1. Albarran A, and Goff D, *In Understanding the Web: Social, Political, and Economic Dimensions of the Internet*, Wiley Blackwell, 2000
2. Anderson R, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wilea Computer Publishing, 2001
3. Burrows A, Peel E, Contract Formation and Parties, Oxford University Press, 2010, 4
4. Goel R, *E-commerce*, New Age International Publishers Limited, 2007
5. Hart L. A, *The Concept of Law*, Oxford University Press, 1961
6. Hill J, *Cross-Border Consume Contracts*, *Oxford University Press*, 2008, 53
7. Kafka F, *The Trial*, Knopf, 1956
8. Kenny M, Devenney J, *European Consumer Protection: Theory and Practice*, Cambridge, Cambridge University Press, 2012
9. Laudon C, Traver C, *E-commerce 2009: Business Technology and Society*, 5ed, Prentice Hall, 2009
10. Ritendra G, *E-commerce*. New Age Publishers, 2007
11. Singh R, *Law Relating to Electronic Contracts*, 2ed LexisNexis
12. Sankar P, *DNA Typing: Galton's Eugenic Dream Realized*, in Caplan J, Torpey C, *Documenting Individual Identity: The Development of State Practices in the Modern World*, Princeton University Press 2002

Journal Articles

1. Bart, Fareena Sultan, and Urban G, Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study, 69 Journal of Marketing, (2005)
2. Blume P, Data Protection and Privacy- Basic Concept in a Changing World, Scandinavian Studies in Law, (2010)
3. Dinev T and Hart P, Internet Privacy Concerns and their Antecedents: Measurement Validity and a Regression Model, 23 Behavior and Information Technology, (2004)

4. Emmelhainz M, Electronic Data Interchange: Does it Change Purchasing Process, 23 Journal of Purchasing and Materials Management, Winter, (1987)
5. Ghani N, Personal Information Privacy Protection in E-commerce, 9 World Scientific and Engineering Academy and Society Transactions on Information Science and applications, (2009)
6. Grandinetti, M, Establishing and maintaining security on the Internet, 13 Sacramento Business Journal,
7. Guo M, A Comparative Study on Consumer Right to Privacy in E-commerce, 3 Modern Economy (2012)
8. Head M, Yuan Y, Privacy Protection in Electric Commerce- A Theoretical Framework, 20 Human System Management, (2001)
9. Kinuthia J, Akinnusi D, The Magnitude of Barriers Facing E-Commerce Businesses in Kenya, 4 Journal of Internet and Information Systems, (2014)
10. Krishna P, From Contracts to E-Contracts: Modeling and Enactment, 6 Information Technology and Management, (2005)
11. Madeiha I, E-commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill, International Review of Law Computers & Technology, 2002.
12. Mukhopadhyay T, Kekre S, Kalathur S, Business Value of Information Technology: A Study of Electronic Data Interchange, 9 Management Information Systems Research Center, University of Minnesota, (1995), 137-156
13. Niranjanamurthy M, Kavyashree N, Dr Dharmendra C, Analysis of E-commerce and M-commerce: Advantages, Limitations and Security issues, International Journal of Advanced Research in Computer and Communication Engineering, Vol 2, Issue 6, June (2013)
14. Nowak G and Phelps J, Understanding Privacy Concerns: An Assessment of Consumers' Information-Related Knowledge and Beliefs. 6 Journal of Direct Marketing, (1992)
15. P. Sheeran, Intention-Behavior Relations: A Conceptual and Empirical Review, 20 European Review of Social Psychology, (2002)
16. P. Sheeran, Webb T, The Intention-Behavior Gap, 10 Social and Personality Psychology Compass, (2016)

17. Pragadeeswaran M, Rajan A, Critical Study on Different Types of E-Contract with Special Reference to the Remedies Available on Breach, 119 International Journal of Pure and Applied Mathematics, 2018
18. Randall H, B2B E-Commerce: Business Models and Revenue Generating Activities, 2000.
19. Rogers R, A Protection Motivation Theory of Fear Appeals and Attitude Change1, 91 Journal of Psychology, (1975)
20. Smith R, Shao J, Privacy and E-commerce: A Consumer- Centric Perspective, 7 Electronic Commerce Research, (2002)
21. Solove D, A Taxonomy of Privacy, 154 University of Pennsylvania Law Review, (2006)
22. Solove D, I've Got Nothing to Hid and other Misunderstandings of Privacy, 745 San Diego Law Review, (2007)
23. Vladimir Z, Electronic Commerce: structure and issues, 1 International Journal of Electronic Commerce Research., (1996)
24. Witte K, Allen M, A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns, 27 Health Education and Behaviour: The Official Publication of the Society for Public Health Education, (2000)
25. White T, Consumer Disclosure and Disclosure Avoidance: A Motivational Framework, 14Journal of Consumer Psychology, (2004)

Dissertations and Theses

1. Patil A, *Legal Regulation of E-contracts: An Indian Perspective*, Unpublished Degree of Doctor in Philosophy in Law Thesis, Gulbarga University, 2014
2. Shashikant P, Advantages of E-Contracts Over Traditional Contracts; E-Contracts and E-Commerce in India Unpublished LLM Thesis, Bharati Vidyapeeth Deemed University new Law College, 2015

Internet Sources

1. Agbor A, *Pursuing the Right to an Effective Remedy for Human Rights Violation in Cameroon: The Need for Legislative Reform* http://dx.doi.org/10.17159/17273781/2017/v20i0a1764 on 30 November 2019
2. Authority of the Republic of Kenya, Kenya Gazette, Nairobi, May 11 2018 file:///C:/Users/Hp/Downloads/Vol.CXX-No_.56_.pdf on 20 November 2019
3. https://ca.go.ke/wp-content/uploads/2018/09/Public-Notice-On-Data-Protection-Bill.pdf on 20 November 2019.
4. Authority of the Republic of Kenya, Kenya Gazette, Nairobi, July 5 2019. file:///C:/Users/Hp/Downloads/Vol.CXXI-No_._85_.pdf on 20 November 2019.
5. Authority of the Republic of Kenya, Kenya Gazette, Nairobi, November 15 2019. file:///C:/Users/Hp/Downloads/Vol.CXXI-No_.156_.pdf on 20 November 2019.
6. https://cyber.harvard.edu/olds/ecommerce/privacytext.html#ftc1back on 23 August 2019.
7. Harris Interactive, Privacy Survey finds Consumers Demanding Companies do More To Protect Privacy; Public Wants Company Privacy Policies to be Independently Verified, 2002, http://www.harrisinteractive.com/news/%20allnewsbydate.asp?NewsID=429 on 20 August 2019.
8. https://thelawdictionary.org/surveillance/ on 1 November 2019.
9. https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf on 20 November 2019
10. https://wiki.openrightsgroup.org/wiki/A_Taxonomy_of_Privacy#Information_collection on 1 November 2019.
11. http://www.ict.go.ke/wp-content/uploads/2018/08/Kenya-Data-Protection-Policy-2018-15-8-2018.pdf on 3 December 2019.
12. Intven H, Tetrault M, *Telecommunication Regulation Handbook, Licensing Telecommunication Services*, https://www.itu.int/ITU-D/treg/Documentation/Infodev_handbook/2_Licensing.pdf on 5 January 2020

13. Mann C, The Unacknowledged Legislators of the Digital World, Atlantic Unbound, 1999, http://www.theatlantic.com/unbound/digicult/dc991215.htm on 15 September 2019
14. Omollo J, *Fourth Arm of the Government? Commissions and Independent Offices in Kenya*, 2014https://www.academia.edu/7932670/THE_FOURTH_ARM_OF_GOVERNMENT_COMMISSIONS_AND_INDEPENDENT_OFFICES_IN_KENYA on November 25 2019

Legislations

Kenyan Legal Instruments

1. Access to Information Act No. 31 of 2016 Laws of Kenya
2. Age of Majority Act Cap 33 Laws of Kenya
3. Code of Conduct and Ethics for Advocates, 2016
4. Constitution of Kenya 2010
5. Consumer Protection Act No 46 of 2012 Laws of Kenya
6. Credit and Reference Bureau Regulation, Laws of Kenya 2013
7. Data Protection Act No. 24 of 2019
8. Evidence Act Cap 80 Laws of Kenya
9. HIV and AIDS Prevention and Control Act No. 14 of 2016 Laws of Kenya
10. Kenya Information and Communication Act No 2 of 1998 Laws of Kenya
11. Kenya Information and Communication Act, Cap 411A, Laws of Kenya, 2015
12. Kenya National Patient's Charter 2013
13. Private Security Regulation Act No. 13 of 2016 Laws of Kenya
14. Sale of Goods Act Cap 31 Laws of Kenya

European Union Legal Instrument

1. General Data Protection Regulation 2016/769

Treaties and international instruments

1. International Covenant on Civil and Political Rights, 1976

2. Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data on September 1980
3. Universal Declaration of Human Rights, 1948

Reports

1. African Centre for Open Governance, *African Center for Open Governance Forum on Governance and Submarine fiber-optic cable initiatives in Kenya*, 21 July 2010
2. Civic Consulting, *Consumer Market Study on the Functioning of E-commerce and the Internet Marketing and Selling Techniques in the Retail of Goods*, European Union Publications, 2015
3. Souter D, Kerretts M, *Internet Governance in Kenya: An Assessment for the Internet Society*, Information Communication Technology Development Associates Ltd, Kenya. 2012
4. United Nations Conference on Trade and Development, *United Nations Conference on Trade and Development, E-commerce and Development Report*, New York, 2002
5. United States Federal Trade Commission, Privacy Online: A Report to Congress, 1998, 3,https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf on August 22 2019

Conference Papers

1. Gertjan F, *Who Left Open the Cookie Jar? A Comprehensive Evaluation of Third-Party Cookie Policies*. SEC' 18 Proceedings of the 27th USENIX Conference on Security Symposium, Baltimore Maryland, 2018.
2. Goldberg I, Wagner D, Brewer E, *Privacy-Enhancing Technologies of the Internet*, Institute of Electrical and Electronics Engineers Compcon '97, 1997.