UNIVERSITY OF NAIROBI

SCHOOL OF LAW

MASTER OF LAWS PROGRAM 2018/2019

GOVERNANCE IN THE DATA AGE: THE APPLICATION OF CORPORATE GOVERNANCE TO ENSURE CONSUMER DATA PROTECTION IN KENYA

BY: MUGO EVALYNE WANJA

G62/12692/2018

SUPERVISOR: DR. PETER MUNYI

A RESEARCH PAPER SUBMITTED TO THE UNIVERSITY OF NAIROBI IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE DEGREE OF MASTER OF LAWS (LL.M) OF THE UNIVERSITY OF NAIROBI

DECLARATION

1. I understand what Plagiarism is and I am aware of the University's policy in this regard
2. I declare that this is my original work and has not been submitted elsewhere for examination, award of a degree or publication. Where other people's work or my own work has been used, this has properly been acknowledged and referenced in accordance with the University of Nairobi's requirements.
3. I have not sought or used the services of any professional agencies to produce this work
4. I have not allowed and shall not allow anyone to copy my work with the intention of passing it off as his/her own work.
5. I understand that any false claim in respect of this work shall result in disciplinary action, in accordance with University Plagiarism Policy.

NAME……

REG. NO……

SIGNATURE…….

DATE…….

This project has been submitted for my approval as the University of Nairobi Supervisor.

SIGNED:……. DATE:…….

DR. PETER MUNYI

DEDICATION

I dedicate this work to God and my family. Special thanks to my parents Jamleck Mugo and Agnes Mugo for the support and encouragement throughout this journey. I also thank my siblings Robert, Susan, Emma and Denis for their unwavering support.

ACKNOWLEDGEMENT

I wish to thank my supervisor Dr. Peter Munyi for his guidance and precious time as I worked on this project.

I also wish to express my sincere appreciation to my reader Dr. Kenneth Wyne Mutuma for the continuous support of my study and research.

ABSTRACT

Data privacy is a hot button issue that is being discussed by people all over the world. Vast amounts of personal data are being collected, transmitted and stored globally by ever growing computing and communication technologies. Hand in hand with this, large scale data breaches are also happening all over the world making consumers lose trust of the companies that they have entrusted their data with. Although there is no specific legislation on data protection in Kenya, corporate governance principles can be applied to ensure consumer data protection in Kenya. This can be done with the Board of directors recognizing that their duty of care also extends to ensuring that there is data privacy within the company.

TABLE OF ABBREVIATIONS

1. AU – African Union
2. CAPA - Canadian Access and Privacy Association
3. CBK - Central Bank of Kenya
4. CMA – Capital Markets Authority
5. EAC – East African Community
6. EFC - Electronic Frontier Canada
7. EU – European Union
8. IRA – Insurance Regulatory Authority
9. OECD - Organisation for Economic Co-operation and Development
10. OHCHR - Office of the United Nations High Commissioner for Human Rights
11. OPC - Office of the Privacy Commissioner
12. PIAC - Public Interest Advocacy Center
13. UN – United Nations
14. UNCTAD - United Nations Conference on Trade and Development
15. USA – United States of America

TABLE OF CASES

1. Bernard Murage v. Fineserve Africa Limited & 3 others (2015) eKLR
2. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González Case C-131/12
3. Kenya Human Rights Commission v. Communications Authority of Kenya & 4 others (2018) eKLR
4. Mark Madrack v. Yahoo Inc & Others Case 5:17-cv-00373
5. Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others (2018) eKLR
6. Palkon v. Holmes et al Civil Action No. 2:14-CV-01234 (SRC)
7. Re: Target Corporation Case 0:14-cv-00203-PAM-JJK
8. Re: The Home Depot, Inc. Shareholder Derivative Litigation Civil Action File No. 1:15-Cv-2999-Twt
9. Re: Yahoo! Inc. Shareholder Litigation., Case No. 17-CV-307054.
10. Rechnungshof v. Osterreichischer Rundfunk C-465/00 AND C-138/01 (2003)
11. Salomon v A Salomon and Co Ltd (1897) AC22
12. Skanska Industrial Solutions and Others Case C-724/17
13. United States v. Antoine Jones, 132 S. Ct. 945 (2012)

TABLE OF STATUTES

1. The Constitution of Kenya, 2010
2. Access to Information Act, No. 31 of 2016
3. Banking Act, Cap 488, Laws of Kenya
4. Capital Markets Act Cap 485A Laws of Kenya
5. Companies Act No. 17 of 2015
6. Computer Misuse and Cybercrimes Act No. 5 of 2018
7. Consumer Protection Act. No. 46 of 2012
8. Health Act, No 21 of 2017
9. Kenya Information and Communication (Amendment) Act, 2013
10. Private Security Regulation Act, No. 13 of 2016

PROPOSED STATUTES

1. Data Protection Bill, 2018

SUBSIDIARY LEGISLATION AND POLICIES

1. The Capital Markets (Securities) (Public Offers, Listing and Disclosures) (Amendment) Regulations, 2016
2. The Code of Corporate Governance Practices for Issuers of Securities to the Public, 2015 Gazette Notice No. 1420 of 2015
3. Corporate Governance Guidelines for Insurance and Reinsurance Companies (2011)
4. Credit Reference Bureau Regulations, 2013
5. Kenya Information and Communications (Consumer Protection) Regulations, 2010
6. Mwongozo, Code of Governance for State Corporations
7. National ICT Policy

8. Privacy and Data Protection Policy 2018
9. Prudential Guidelines for Institutions Licensed under the Banking Act: CBK/PG/02 Corporate Governance

LEGISLATION FROM OTHER JURISDICTIONS

1. Australia Information Privacy Amendment Act 2014
2. The Canadian Constitution
3. Canadian Privacy Act (1983)
4. Canadian Personal Information Protection and Electronic Documents Act
5. General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, 2016
6. USA Sarbanes Oxley Act of 2002
7. South Africa Protection of Personal Information Act (No. 4 of 2013)
8. South Africa's Electronic Communications and Transactions Act

TABLE OF CONVENTIONS

1. African Union Convention on Cybersecurity and Personal Data Protection 2008
2. Charter of Fundamental Rights of The European Union 2000
3. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 (Council of Europe Convention 108)
4. Draft EAC Legal Framework for Cyberlaws 2008
5. Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms 1950
6. International Covenant on Civil and Political Rights 1966

7. Montreux Declaration: The Protection of Personal Data and Privacy in a Globalized World: A Universal Right Respecting Diversities 2005
8. OECD Guidelines Governing the Protection of Privacy and Trans border Flows of Personal Data 2013
9. OECD Principles of Corporate Governance 2004
10. G20/OECD Principles of Corporate Governance 2015
11. OECD Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity 2015
12. OECD Guidelines for Consumer Protection in the Context of Electronic Commerce 1999
13. Universal Declaration of Human Rights 1948
14. UN Resolution on the right to privacy in the digital age 2013 A/RES/68/167

GUIDELINES

1. Committee on the Financial Aspects of Corporate Governance, Report with Code of Best Practice (Cadbury Report)
2. King Reports I, II, III and IV
3. Private Sector Initiative for Corporate Governance, Principles for Corporate Governance in Kenya and a Sample Code of Best Practice for Corporate Governance 2002

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

The world has become a global village. Technology has come of age in many countries and Kenya has not been left behind.[1] With the rapid growth in technology, information is increasingly becoming a critical source that needs to be managed carefully.[2] Generally, much of today's information collected and stored by both private and public organizations consists of personal data relating to individuals.[3] Vast amounts of personal data are being collected, transmitted and stored globally by ever growing computing and communication technologies.[4] Both the public and private sectors collect, use and transfer personal data at an unprecedented scale and for multiple purposes.[5] This is more apparent in the companies which have heavily invested in the use of websites and online mobile applications.[6]

Data protection and the privacy of citizens is one of the most important issues facing the global economy in the recent years.[7] Data protection or data privacy has been described as the relationship between the collection and dissemination of data, technology, the public expectation

[1] Bitange Ndemo, 'How Kenya Became the Cradle of Africa's Technological Innovation,' Newsweek, (2016) https://www.newsweek.com/how-kenya-became-cradle-africas-ict-innovation-534694 accessed 6 January 2019.
[2] Teresa Scassa, 'Data Governance in the Digital Age; Considerations for Canada'S National Data Strategy' Data Governance in the Digital Age (2018) Centre for International Governance Innovation <www.cigionline.org> accessed 5 January 2019.
[3] David Lyon, 'Surveillance, Power and Everyday Life' in Chrisanthi Avgerou and Others, *The Oxford Handbook of Information and Communication Technologies* (Oxford 2009) 17.
[4] Privacy and Data Protection Policy 2018- Kenya http://www.ict.go.ke/wp-content/uploads/2018/08/Kenya-Data-Protection-Policy-2018-15-8-2018.pdf accessed 4 December 2018.
[5] Ibid.
[6] Wolfie Cristl & Sarah Speikermann, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy*, (2016, Wien), 46.
[7] Sarah Spiekermann-hoff and Alexander Novotny, 'A Vision for Global Privacy Bridges : Technical and Legal Measures for International Data Markets'. *Computer Law and Security Review*, (2017) 31 (2). 181-200. ISSN 0267-3649 EPub WU Institutional Repository.

of privacy, legal and political issues surrounding them.[8] Personal data means any information relating to an identified or identifiable individual. An identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints, DNA).[9]

Several countries all over the world have recognized the importance of the right to privacy and the need to protect data and have put in place laws to regulate how a person's personal information is collected, stored and distributed.[10] In Europe, the European Parliament adopted the General Data Protection Regulation (GDPR) in April 2016, which has provisions that require businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states. [11] The GDPR also regulates the exportation of personal data outside the EU[12]. In Kenya, the right to privacy of a person's personal information is provided for under Article 31 of the Constitution of Kenya. Privacy of information is also articulated in the National ICT Policy.[13] However, Kenya still does not have any specific laws on data protection although it has provided for in the proposed Privacy and Data Protection Bill and Policy, 2018.

Corporate governance refers to the way the power of a corporation is exercised in the stewardship of the corporation's total portfolio of assets and resources with the objective of

[8] M G Michael and Katina Michael, *Uberveillance and the social implications of microchip implants : emerging technologies*, (2014 Hershey), PA.
[9] CNIL, 'Personal Data: definition' https://www.cnil.fr/en/personal-data-definition accessed 11 December 2018
[10] Andrew Gordon, 'Can advanced analytics help organizations make the transition to a new era of data privacy and protection?', (2018) https://www.ey.com/en_gl/trust/gdpr-compliance-how-data-analytics-can-help accessed 6 January 2019. Also see the EU General Data Protection Regulations, China's Cybersecurity Law, Australia's Privacy Amendment Act and South Africa's Electronic Communications and Transactions Act.
[11] Michael Nadeau, 'General Data Protection Regulation (GDPR): What you need to know to stay compliant,' https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html accessed 4 December 2018.
[12] Ibid.
[13] National ICT Policy, Article 4.3.9.

maintaining and increasing shareholder value and satisfaction of other stakeholders in the context of its corporate mission. [14] It is concerned with creating a balance between economic and social goals and between individual and communal goals while encouraging efficient use of resources, accountability in the use of power and stewardship and as far as possible to align the interests of individuals, corporations and society.[15]

In the realm of data protection, companies take the seat of a data controllers. For example, the GDPR recognizes companies as data controllers in the definition of a data controller which states that they are "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[16] Companies therefore bear specific responsibilities of data controllers bestowed upon them by law.

The use of personal data by companies as data controllers, has raised concerns regarding the privacy and control over such data, more so in countries such as Kenya where data protection laws are absent. The goal of this paper is to analyze whether in the absence of data protection laws in Kenya, corporate governance principles in the age of big data can fill this gap with a view to ensure that the consumers' data privacy remains protected.

[14] Private Sector Initiative for Corporate Governance, 'Principles for Corporate Governance in Kenya and a Sample Code of Best Practice for Corporate Governance,' http://www.ecgi.org/codes/documents/principles_2.pdf accessed 11 December 2018.
[15] Ibid.
[16] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, a 2016 (Official Journal of the European Union), Article 4.

1.2 Statement of the Problem

In the modern business world data has been described as the new oil.[17] This is to say that data is fast becoming one of the drivers of wealth creation and is now an essential part of the business strategy of companies.[18] Corporate controls also affect the everyday person to a much greater extent than in previous world history, which demands greater accountability and greater care when it comes to data protection.[19] For most people today, many companies possess data about a person which are subject to breaches both internally and externally, and the protections against these breaches require good governance practices or policies.[20] Checks and balances to protect data are expected on every level, from individuals who grant platforms access to it all the way up to governments that are expected to implement regulatory protections for it. [21]

Better corporate governance is better for business and everyone else.[22] Businesses are more profitable when users trust them and therefore use them more.[23] One of the pillars of good corporate governance is the protection of human rights and freedoms and the maintenance of

[17] Michael Haupt, '"Data is the New Oil" — A Ludicrous Proposition' (2016) Project 2030 https://medium.com/project-2030/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294 accessed 5 January 2019

[18] Rohinton Medhora, 'Data Governance in the Digital Age' Data Governance in the Digital Age (2018) Centre for International Governance Innovation 2 <www.cigionline.org> accessed 5 January 2019.

[19] Compliance Experts 'Facebook, Global Data, and Corporate Governance Deficiencies' (2018) http://complianceexperts.com/2018/06/05/facebook-global-data-corporate-governance-deficiencies/ accessed 11 December 2018

[20] Ibid

[21] Private Sector Initiative for Corporate Governance, "Principles for Corporate Governance in Kenya and a Sample Code of Best Practice for Corporate Governance," http://www.ecgi.org/codes/documents/principles_2.pdf accessed 11th December 2018

[22] Nada Korac-Kakabadse, Andrew K. Kakabadse and Alexander Kouzmin, 'Board governance and company performance: any correlations?', (2001) 1 Corporate Governance: The international journal of business in society, 1,24, https://doi.org/10.1108/EUM0000000005457 accessed 4th February 2019

[23] Ibid

essential order and security for the person and their property.[24] Article 31 of the Constitution specifically protects the right to privacy. [25]

Although, there are laws providing for corporate governance and the duties of directors in Kenya, nevertheless there is no specific legislation on data protection as well as the corporate's and board of directors' responsibilities to ensure consumer data protection. The Consumer Protection Act contains provisions on the confidentiality of information obtained in the course of exercising any power related to administration of the Act.[26] However, this is inadequate as it does not specifically provide for the duties of a company towards consumer data apart from confidentiality.

The study mainly seeks to find out whether corporate governance principles can be applied to ensure consumer data protection in Kenya and whether a board of directors has duty under company law to ensure that there is personal data in the hands of company should remain protected.

This study is comparative in nature. The study shall look at the data protection law in the EU and how corporate governance is affected by this law. It shall then analyze what principles Kenyan corporations can apply in order to ensure that consumer data is protected.

1.3 Main Objective of the Study

The main objective of this study is to assess whether corporate governance principles can be applied towards ensuring consumer data in a corporation remains protected in the absence of

[24] Private Sector Initiative for Corporate Governance, "Principles for Corporate Governance in Kenya and a Sample Code of Best Practice for Corporate Governance," (n. 21) 1.
[25] Constitution of Kenya, 2010
[26] The Consumer Protection Act No. 46 of 2012, Section 86(1)

privacy and data protection laws in Kenya. In order for this objective to be met, a set of specific objectives have been formulated. These are as follows:

1.4 Specific Objectives

1. To investigate whether a board of directors of a corporation have a duty under Kenya company law to ensure that consumer data in the hands of a corporation should remain protected.
2. To establish whether corporations have any role to play in ensuring protection of consumer data.
3. To explore how corporate governance is affected by data protection laws and policies in the European Union.

1.5 Research Questions

In order to achieve the specific objectives set, the following research questions are formulated. These are as follows:

1. Does a board of directors of a corporation possess a duty under Kenya company law to ensure that consumer data remains protected?
2. What role do corporations have in ensuring protection of consumer data?
3. How is corporate governance affected by data protection laws and policies in the EU?

1.6 Hypotheses

This research is hinged upon two hypotheses. The first is that the directors of a corporation have a duty to ensure that their consumers' data is protected. The second one is that corporate governance principles can be applied to ensure that consumer data in the hands of a corporation remains protected.

1.7 Theoretical Framework

This research relies on three main theories. These theories are; stakeholder theory, the value theory and the theory of propertisation. These theories are important because they inform the approach to a feasible solution of the problem in this study. This has shaped the interrogation of the interaction between the corporation and data protection rights of a consumer as a claim in the governance of the corporation.

1.7.1 Stakeholder theory

Sir Adrian Cadbury defines corporate governance as an area of law concerned with "...holding the balance between economic and social goals and between individual and communal goals. The aim is to align as nearly as possible the interests of individuals, of corporations, and of society."[27] The stakeholder theory states that a company owes a responsibility to a wider group of stakeholders, other than just shareholders.[28] Freeman defined a stakeholder as "those groups without whose support the organization would cease to exist.[29]. This includes employees, customers, suppliers, creditors and even the wider community and competitors.[30] Heath and Norman argue that for the supporters of the stakeholder theory, the firm and its managers have special obligations to the stakeholders which go beyond and above what is required by law.[31]

[27] Adrian Cadbury, in Stijn Claessens, *Corporate Governance and Development,* (2003, Washington DC: Global Corporate Governance Forum) 7.
[28] Corplaw 'Shareholder & Stakeholder Theories Of Corporate Governance', (2013) http://www.corplaw.ie/blog/bid/317212/Shareholder-Stakeholder-Theories-Of-Corporate-Governance accessed 6th January 2019
[29] R. Edward Freeman and Others, *Stakeholder Theory: The State of the Art,* (2010 Cambridge University Press), 31
[30] Ibid
[31] Joseph Heath and Wayne Norman, 'Stakeholder Theory, Corporate Governance and Public Management: What Can the History of State-Run Enterprises Teach Us in the Post-Enron Era?' (2004) Journal of Business Ethics 53, 3 247-65 accessed from http://www.jstor.org/stable/25123300 on 6th January 2019

Aaron Dhir argues that the corporation is a social entity, not a private property of the shareholders.[32] As per this approach, the corporation carries with it a public purpose such as protecting the interests of its stakeholders.[33]

Freeman recognized the stakeholder theory as an important element of Corporate Social Responsibility (CSR), a concept which recognizes the responsibilities of corporations in the world today, whether they be economic, legal, ethical or even philanthropic.[34]

One of the central theses propounded by Donaldson and Preston is that stakeholders are persons or groups with legitimate interests in the substantive aspects of a corporation's activity.[35] The interests of all stakeholders are of intrinsic value. Each group of stakeholders merits consideration for its own sake and not merely because of its ability to further the interests of some other group, such as the shareholders.[36] This led to calls for including consumers as corporate stakeholders on the observation that investors are not the only group that may provide value to corporate production and thus are not the only group to whom the corporation owes value.[37] Consumers are therefore a major stakeholder as they add value to the company through by increasing a company's profits.

---

[32] Aron A. Dhir, 'Realigning the Corporate Building Blocks: Shareholder Proposals as a Vehicle for Achieving Corporate Social and Human Rights Accountability,' (2006) 43 American Business Law Journal *2,* 370.
[33] Ibid.
[34] Freeman & Others, (n 29)
[35] Thomas Donaldson and Lee E Preston, 'The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications' (1995) 20 The Academy of Management Review 65 <https://www.jstor.org/stable/pdf/258887.pdf?refreqid=excelsior%3Ad3bbd6554c18aeaadaf72bf1c5d060b5> accessed 16 September 2019.
[36] ibid.
[37] Shlomit Azgad-Tromer, 'The Case for Consumer-Oriented Corporate Governance, Accountability and Disclosure' 17 University of Pennsylvania Journal of Business Law 227.<https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1475&context=jbl> accessed 16 September 2019.

1.7.2 Value Theory

Under the value theory, Sarah Spiekermann and Jana Korunovska argue that since personal data is viewed as 'the oil' of the digital economy, it has value to both an individual and companies collecting it, therefore there is a stake in ensuring that data is protected.[38] Analysts, investors and companies have recognized the value of personal data.[39] They view personal data is an intangible asset class which is even traded on the market. They went on to conduct research on how consumers view their data and concluded that they view data as something personal which has value.[40] Therefore, this data needs to be protected because it has value.

Alessandro Acquisti, Leslie K. John, and George Loewenstein contended that understanding the value that individuals assign to the protection of their personal data is of great importance for business, law, and public policy.[41] They stressed that understanding this value is important to businesses because by estimating how much customers value the protection of their personal data, they can seek to predict which privacy-enhancing initiatives may become sources of competitive advantage and which intrusive initiatives may trigger adverse reactions.[42] It is also important to because privacy is an issue that has become increasingly prominent in the law in recent years, in part because of the emergence of new technologies.[43]

[38] Sarah Spiekermann, Jana Korunovska, 'Towards a value theory for personal data,' (2017) 32 Journal of Information Technology, 62.
[39] Ibid.
[40] Ibid.
[41] Alessandro Acquisti, Leslie K. John, and George Loewenstein, 'What Is Privacy Worth?', *The Journal of Legal Studies*, Vol. 42, No. 2 (June 2013), 249, http://www.jstor.org/stable/10.1086/671754 accessed 6th January 2019.
[42] Ibid, 250.
[43] Ibid; *United States v. Antoine Jones, 132 S. Ct. 945 [2012].*

1.7.3 Instrumentalist Theory of Propertisation

The instrumentalist theory of propertisation of personal data was propounded by Lawrence Lessig as an economic argument to introduce property rights in personal data.[44] Lessig propounds that personal data is the personal property of a person, and therefore property rules would permit each individual to decide what information to disclose and protect.[45]

He puts forward several arguments to support this theory. First, he argues that data privacy is in essence control over personal information.[46] Second, the architecture or "code" of a cyberspace makes collection of information difficult to spot, and control over that information difficult for lay people.[47] Third, this architecture is a result of human activity and, therefore, can be modified.[48] Fourth, data processing practices are often based on self-regulation, *that is*, there is often no general legislation requiring businesses to alter this architecture and use privacy-friendly technologies.[49] There is also often no motivation to account for the best interests of the individuals. In absence of property interests, the companies make use of personal data for free. However, if individuals had property rights in personal data, it would force businesses to negotiate with the individuals, account for their interests, alter the architecture and invest into development of privacy-friendly technologies. An overall system of data protection would therefore be better secured by interaction of the law, market mechanisms and technologies.[50]

[44] Nadezda Purtova, 'Property in Personal Data: A European Perspective on Instrumentalist Theory of Propertization' [2010] Research Policy <https://core.ac.uk/download/pdf/45678038.pdf> accessed 21 September 2019.
[45] ibid.
[46] ibid.
[47] ibid.
[48] ibid.
[49] ibid.
[50] ibid.

1.8 Literature Review

Several authors have researched and written on disciplines of data protection and corporate governance respectively. However, only a few authors have focused on the interdisciplinary connection between consumer data protection law and corporate governance. Furthermore, there is limited literature available on data protection in Kenya. The literature review is therefore confined to the works on different, relevant and necessary concepts of consumer data protection and how it impacts on corporates and corporate governance in different jurisdictions.

Sarah Speikermann and Wolfe Cristl in their book "*Networks of Control*",[51] discuss how corporate surveillance is being used and amplified using intelligent devices and the internet worldwide. They describe how companies co-operate at a large scale to complete their profiles about their consumers through various networks. These companies build profiles which they trade, filled with thousands of attributes per person. [52] These networked databases are not only abused to discriminate against people with specific profile attributes, but also attempt to make us change our behavior at scale. Data richness is increasingly used to correct us or incentivize us to correct ourselves. It is used to "influence" us to act differently. As a result of this continued influencing, the autonomy of the consumers suffers. The authors recommend that privacy laws are needed to ensure that this data is protected.[53]

Stefaan Verhulst in his article "*Corporate Social Responsibilities for a Data Age*",[54] discusses the responsibilities that companies have over consumer data. One of these responsibilities is to protect this consumer data. He argues that data responsibility is a type of corporate social

[51] Wolfie Cristl & Sarah Speikermann, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy*, (2016 Wien), 46.
[52] Ibid.
[53] Ibid, 139.
[54] Stefaan G. Verhulst, 'Corporate Social Responsibility for a Data Age,' (2017*) Stanford Social Innovation Review* https://ssir.org/articles/entry/corporate_social_responsibility_for_a_data_age accessed 8 January 2019.

responsibility for the 21st century. He states that "the consequences of failing to protect data are well documented. The most obvious problems occur when data is not properly anonymized or when de-anonymized data leaks into the public domain."[55]

Sarah Spiekermann-hoff and Alexander Novotny in their article *"A Vision for Global Privacy Bridges"*[56] purport that there need to be a balance between people's right to privacy and data protection on one hand and economic efficiency in collecting personal data on the other hand. They argue that this is because when data breaches are made public, consumers become irritated about a company's data handling practices and lose trust in the company.[57] In order to ensure that a consumer's data is protected, they came up with a four-space market model for personal data which is:

i) the customer relationship space which includes customers and customer relationship holders directly involved in a service exchange,
ii) the customer relationship holders-controlled data space which includes the distributed computing and service infrastructures that enables today's electronic business relationships. This space includes all companies providing services to the consumer relationship holders that directly enable and enrich the customer relationship,
iii) customer-controlled data space, which includes services that grant customers ownership of their personal information and manage and control it in a privacy-friendly way; and

[55] Ibid
[56] Sarah Spiekermann-Hoff and Alexander Novotny, 'A Vision for Global Privacy Bridges: Technical and Legal Measures for International Data Markets' (2015) 31 Computer Law and Security Review 181
[57] Ibid, 2

iv) the safe harbor for big data which grants equal access to anonymized people data to all market entities that need it.[58]

However, their research places most of the burden of data protection on the customer rather than the company. In conclusion, they also suggest that no one has demonstrated how this market model would benefit both people and companies.[59]

Sarah Ludington in her article "*Reining in the Data Traders: A Tort for the Misuse of Personal Information"*[60] argues that "a common law tort should be used to force reform and accountability on data traders, and to provide remedies for individuals who have suffered harm to their core privacy interests of choice and control-choice about who may receive their information, control over the information revealed, and how the recipient of that information may use it."

In the article, she examined the legislative and common law regimes in several American states in 2005 and concluded that there were no effective remedies for individuals who have suffered harm from data misuse.[61] Given this, she argued that common law privacy torts should be expanded to create a new tort for information misuse.[62] The new tort borrows from existing privacy torts; in particular, how standard of care should be applied to ensure that personal privacy is protected.[63]

[58] Ibid.
[59] Ibid, 24
[60] Sarah Ludington, 'Reining in the Data Traders: A Tort for the Misuse of Personal Information,' *Maryland Law Review,* 66 (2006) 86
[61] Ibid
[62] Ibid
[63] Ibid

Max Helvelston in his article "*Consumer Protection in the Age of Big Data*"[64] discusses how technological advances in recording a consumer's personal advances are transforming the way business is conducted in almost all sectors of the economy. He focuses on how insurance companies are collecting and storing their consumers data and the impact on contemporary insurance practices.[65] He goes ahead to identify eight societal interests that will be affected by a company's use of personal data which are actuarial fairness[66], loss prevention, autonomy, non-discrimination, justice, utility maximization, privacy, and good faith.[67] He concludes by recommending that insurance regulators should act to ensure that the markets advance public interest through consumer data protection. This can be done through developing regulation to attempt to control insurers' uses of data in a way that strikes a balance between a number of different values. [68]

Malcom Crompton in his book "*Privacy Governance: A Guide to Privacy Risk and Opportunity for Directors and Boards*",[69] gives guidance toward company directors and boards, the importance of privacy compliance and how to address it. He argues that privacy compliance is often left to the practitioners within an organization, while those in the boardroom rarely take part in the important work of building an effective privacy compliance program.[70] He looks at the historical development of privacy principles across different jurisdictions, leading to the

[64] Max N. Helveston, 'Consumer Protection in the Age of Big Data', (2016) 93 *Washington University Law Review* 859
[65] Ibid, 877
[66] Xavier Landes, 'How Fair Is Actuarial Fairness?' (2015) 128 Journal of Business Ethics 519 <https://curis.ku.dk/ws/files/136684188/Landes_Actuarial_Fairness.pdf> accessed 21 September 2019. That states that the fundamental idea of actuarial fairness is that "fairness means equal treatment for equal risks."
[67]Helvenston (n 64), 897
[68] Ibid, 916
[69] Malcom Crompton, *Privacy Governance: A Guide to Privacy Risk and Opportunity for Directors and Boards,* (2014 Australian Institute of Company Directors)
[70] JC Cannon, 'Privacy Governance: A Guide to Privacy Risk and Opportunity for Directors and Boards', The Privacy Advisor-IAPP https://iapp.org/news/a/book-review-privacy-governance-a-guide-to-privacy-risk-and-opportunity-for/ accessed 7 January 2019

creation of the Australian Privacy Act of 1988 then describes how the Act evolved and impacted how organizations should treat personal information.[71] He provides insight into how businesses, directors and customers can be negatively impacted when an organization fails to comply with privacy legislation via fines, lawsuits, loss of customers and decreases in market valuation. Crompton describes the importance of incorporating the tenets of Privacy by Design and privacy impact assessments into an entity's project management processes.[72] Crompton argues that directors are accountable for ensuring privacy governance, increasing privacy awareness, ensuring an effective privacy strategy is in place and validating privacy compliance via regular audits.[73]

Kenneth Bamberger and Deirdre Mulligan in their article "*Privacy in Europe*",[74] give a comparative analysis of privacy regulations in different countries in Europe and how they are applied. They argue that privacy debates generally focus on law in the books and ignore privacy on the ground such as what is practiced by corporations in different countries.[75] They look at how privacy protection laws are implemented on the ground in corporations in three different European countries.[76] They conclude that data privacy protection in corporations is shaped by public and private stakeholders and institutions which creates constraints more powerful than formal regulations, in that, "on the ground practices have brought about best practices on data which includes incorporating "privacy by design" into the corporate structure."[77]

---

[71] Ibid
[72] Ibid
[73] Ibid
[74] Kenneth A. Bamberger and Deirdre K. Mulligan, 'Privacy in Europe: Initial Data on Governance Choices and Corporate Practices', (2013) 81 George Washington Law Review 1529 <https://scholarship.law.berkeley.edu/facpubs> accessed 7 January 2019
[75] Ibid
[76] Ibid
[77] Ibid

David Banisar and Simon Davies in their article *"Global Trends in Privacy Protection"*,[78] examined the how the global trends of privacy protection have evolved over the years. They asserted that privacy rights have become an important human right in the modern era which has caused many countries to adopt laws to protect individual privacy.[79] This has also brought about several models of regulation personal data including self-regulation, in which companies and institutions establish codes of practice to regulate privacy.[80] However, they averred that the effect of self-regulation was disappointing with little evidence that the aims of the codes were fulfilled.[81]

Héctor J. Lehuedé in his paper "*Corporate governance and data protection in Latin America and the Caribbean*"[82] discusses the relation between cybersecurity and corporate governance with a special interest on data protection in Latin America and the Caribbean. He focuses on the growing role that data protection and privacy laws and regulations in developed countries reserve for corporate governance and argues that these laws increasingly assign responsibilities to boards of directors and management towards data protection. He avers that in the context of data protection, the role of the board involves asking the right questions to managers in order to get information, supporting the development of the necessary measures and policies on data protection, ensuring proper disclosure of risks and risk mitigation strategies through reporting, and keeping active oversight over the functioning of the framework.[83]

---

[78] David Banisar and Simon Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, (1999) 18 J. Marshall Journal of Computer & Information Law 1 <http://repository.jmls.edu/jitpl/vol18/iss1/1> accessed from 8 January 2018

[79] Ibid, 1

[80] Ibid, 14

[81] Ibid

[82] Héctor J Lehuedé, 'Corporate Governance and Data Protection in Latin America and the Caribbean' (2019) <https://repositorio.cepal.org/bitstream/handle/11362/44629/1/S1900395_en.pdf> accessed 21 September 2019.

[83] ibid, 22.

From the foregoing analysis, much of the literature covers the rights of consumers to data protection, how companies collect data and their roles in ensuring data protection, how data protection is regulated and the relation between corporate governance and data protection. However, not much has been documented on the interdisciplinary connection between consumer data protection law and corporate governance. Additionally, there is little research on the application of corporate governance principles to ensure that consumer data is protected. This is what this research proposes to study and therefore fill the existing knowledge gap on both data protection law and corporate governance in Kenya.

1.9 Justification

This study is justified by the fact that more people are becoming alive to the fact that corporations need to protect the information of their consumers. A number of claims have been made over the year by customers against companies' directors and officers alleging a breach of fiduciary duty for failing to adequately oversee data security programs.[84] The plaintiffs' claims against directors and officers in previous cases have generally revolved around breaches of fiduciary duty, and, more specifically, the respective boards' oversight of data security.[85] In the Wyndham case[86] plaintiffs alleged that Wyndham's directors had breached their fiduciary duties with respect to Wyndham's data security and the associated risks.[87] In each of those cases, the courts have examined the nature and extent of boards' oversight of data security programs and the data protection policies applied on the Board and whether data protection laws had been

[84] Brad Martorana, 'Yahoo! Data Breach Results in Another Lawsuit Against Corporate Directors and Officers,' (2017) S & W Cybersecurity and Data Privacy Blog <http://www.swlaw.com/blog/data-security/2017/01/31/yahoo-data-breach-results-in-another-lawsuit-against-corporate-directors-and-officers/> accessed 6 January 2019

[85] Ibid

[86] Palkon v. Holmes et al Civil Action No. 2:14-CV-01234 (SRC)

[87] Also see Re: Target Corporation Case Case 0:14-cv-00203-PAM-JJK, RE: The Home Depot, Inc. Shareholder Derivative Litigation Civil Action File No. 1:15-Cv-2999-Twt, Mark Madrack v. Yahoo Inc & Others Case 5:17-cv-00373

implemented. To date, the companies' oversight of the programs and the documentation of that oversight have been found to be enough to allow courts to rule in directors' and officers' favor.[88] However, this shows that there is a need for directors to be aware of their duties towards data protection.

Furthermore, in the wake of the various scandals involving the handling of personal data by companies, such as Facebook in the Cambridge Analytica data scandal,[89] more Kenyans are becoming aware of their data privacy rights regarding the data being collected by companies. Despite this awareness, and some of these international scandals having tentacles in Kenya, the legal landscape remains without safeguards.

Additionally, many corporations in Kenya, such as telecommunication services corporations, now handle personal data more than before.[90] There are several corporations that have incorporated digital business models that find new ways to generate value from access to large repositories of consumers' data. For example, the most popular mobile money transfer service M-Pesa produces a vast amount of data for the telecommunication services company, Safaricom.[91] This has enabled the company to gather data on its consumers such as frequency of transactions and credit scores and brought about the development of digital services such as Fuliza which is a mobile loan service. Similarly, mobile loan applications such as Tala collect

[88] Ibid
[89] John Walubengo, 'Why Facebook's suspension of Cambridge Analytica is instructive for Kenya,' Daily Nation (March 2018) <https://www.nation.co.ke/oped/blogs/dot9/walubengo/2274560-4349730-ldnsrp/index.html> accessed 8 January 2019
[90] Communications Authority of Kenya, 'Third Quarter Sector Statistics Report for the Financial Year 2018/2019' (2019) <https://ca.go.ke/wp-content/uploads/2019/06/Sector-Statistics-Report-Q3-2018-19.pdf> accessed 21 September 2019.
[91] Privacy International, 'Fintech: Privacy and Identity in the New Data-Intensive Financial Sector' (2017) <https://privacyinternational.org/sites/default/files/2017-12/Fintech report.pdf> accessed 21 September 2019.

extensive data on customers' financial habits to analyse it for credit scoring.[92] This application asks for a wide range of permissions, including access to installed applications, contacts, precise location via GPS, the content of SMS messages such as M-Pesa messages and call logs. [93]

This study will examine whether in the absence of a wholesome law on data protection, corporate governance can be used as a tool to fill in the existing legal gap.

1.10 Research Methodology

This study is primarily library based. It heavily relies on secondary sources of information. It therefore utilizes information from textbooks, referred journals, relevant municipal and foreign laws and relevant international legal instruments. Moreover, the study also relies on credible newspaper and magazine articles for purposes of obtaining information on current affairs on the research problem. Such information includes analyses and opinion relevant to the topic generally.

1.11 Limitations

The research is desk based and therefore there will be no data from interviews with actors. It will mainly rely on information that is derived from secondary sources of information. Secondly, there may also be difficulty in accessing materials in some online sources. Furthermore, the literature in this area of data protection in corporates in Kenya is quite sparse. This can be attributed to the fact that the issue of data protection in Kenya is relatively a new area of law. Therefore, the study shall rely more on literature from foreign jurisdictions.

[92] Kenya ICT Action Network, 'Policy Brief: Data Protection in Kenya' (2018) <https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf> accessed 22 September 2019.
[93] Privacy International (n 91).

1.12 Assumptions

The study assumes that most companies in Kenya collect, handle and store vast amounts of consumer personal data. It also assumes that consumer protection laws in Kenya are inadequate to ensure consumer data is protected. Another assumption is that corporate governance is applied across all companies that are data controllers.

1.13 Chapter Breakdown

This research is contained in five chapters. A breakdown of these chapters is as follows:

Chapter one is the introduction to this thesis and a background to the problem. It also contains the problem statement, research questions and hypothesis, the justification for undertaking the research and what the objectives of the research shall be. It also includes the theories that the study shall be based on and the articles and books that have been reviewed and the research methodology to be used in the research. It also includes the chapter breakdown.

Chapter two analyzes whether a board of directors of a corporation possess a duty under Kenyan company law to ensure that consumer data remains protected. It also looks at the incorporation of consumer data protection and data privacy in corporate governance mechanisms of corporations and how it can be implemented in Kenya.

Chapter three contains a historical background of data protection and data privacy. It includes the conditions for applying data protection policies in corporations by the board of directors as well as the models applicable in ensuring consumer data is protected.

Chapter four discusses how data protection has been implemented by corporations in the European Union. It also looks at how corporate governance practices have been affected by data

protection regulations. It analyses the GDPR as a data protection law and how it has impacted corporate governance of companies within the EU and worldwide.

Chapter five sums up the findings of the study as well as the conclusions of the study. The chapter also contains the recommendations drawn from the study on how corporate governance can be applied to ensure that consumer data is protected.

CHAPTER TWO

THE INCORPORATION OF CONSUMER DATA PROTECTION IN CORPORATE GOVERNANCE MECHANISMS IN KENYA

2.1 Introduction

Corporate governance is described as "the system by which companies are directed and controlled".[1] Sir Adrian further described corporate governance as being "concerned with holding the balance between economic and social goals and between individual and communal goals. The corporate governance framework is there to encourage the efficient use of resources and equally to require accountability for the stewardship of those resources. The aim is to align as nearly as possible the interests of individuals, corporations and society."[2] The Kenyan Code of Corporate Governance defines corporate governance as "the process and structure used to direct and manage the business and affairs of a company towards enhancing business prosperity and corporate accountability with the ultimate objective of realising long-term shareholder value, whilst taking account of the interests of other stakeholders."[3] Essentially, corporate governance affects all the functions and activities of a company that produces goods and provides services and it should therefore promote the interests of its stakeholders.

The single most important institution in corporate governance is the Board of directors.[4] In line with good corporate governance principles, the board is expected to ensure the strategic guidance

[1] Committee on the Financial Aspects of Corporate Governance, 'Report with Code of Best Practice [Cadbury Report]'.
[2] Magdi R Iskander and Nadereh Chamlou, *Corporate Governance: A Framework for Implementation Public* (2000).
[3] The Code of Corporate Governance Practices for Issuers of Securities to the Public 2015.
[4] ibid, 6.

of the company, effectively monitor management, and be accountable to the company and the shareholders, taking into account the interests of stakeholders.[5]

Corporate directors are faced with a wide array of duties to the company and its stakeholders arising by virtue of their board membership. These include a fiduciary duty to act in the best interests of the corporation and a duty to maintain the standard of care.[6] The statutory standard for the amount of care, diligence and skill required of directors is derived from the common law and codified in the Companies Act of 2015.[7] As a general rule, it has been held that a director need not exhibit in the performance of his duties a greater degree of skill than may reasonably be expected of a person carrying out the functions performed by the director in relation to the company and with the general knowledge, skill and experience that the director has.[8]

Increasingly, privacy has become one of the key issues on which directors must focus in order to execute their compliance and managerial oversight as well as mitigate risk.[9] Companies can help to protect the individual's right to privacy in several ways such as implementing data protection laws as well as through good corporate governance practices.

This chapter shall look at the duties of directors under Kenyan company law and corporate governance law in ensuring consumer data is protected as well as the incorporation of consumer data protection in corporate governance mechanisms of corporations in Kenya.

[5] Ibid, Section 2.3
[6] OECD Principles of Corporate Governance 2004.
[7] The Companies Act No 17 of 2015.
[8] Section 145, ibid., Re City Equitable Fire Insurance Co [1925] Ch 407.
[9] Ann Cavoukian, 'Privacy and Boards of Directors: What You Don't Know Can Hurt You (Revised)' <http://www.ipc.on.ca/images/Resources/director.pdf>.

2.2 Data Protection as a Corporate Governance Issue

In order to establish consumer data protection and data privacy as a duty of the Board of directors of a corporation, it is first important to recognize data protection as a corporate governance issue. Company relationships with their consumers have become shaky with the increased amount of data breaches happening.[10] These incidents cause consumers to lose faith and it is the job of the board of directors to improve their corporate governance to try to regain the faith in their organization and subsidiaries. [11] A data breach is a "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed."[12] This encompasses a variety of actions including cybersecurity hacking into a corporate data site to get personal data of another person. Lending states that historically, over 100 million individuals have been affected by specific data breaches worldwide.[13] This affects their reputation as consumers will lose trust in the company. It may also lead to a financial loss.[14] For example, a data breach at Yahoo cost its shareholders 350 million dollars when Verizon reduced its acquisition price of Yahoo in February 2017 after the data breach was revealed.[15]

Data breaches are not only external from hackers but can also be an issue of companies not taking the issue of data privacy and protection seriously. One such case is the recent Facebook-Cambridge Analytica scandal which on discovery cost Facebook a huge blow to their reputation.

---

[10] Nicholas J Price, 'The Correlation Between Corporate Governance and Compliance' (*Diligent Insights*, 2018) <https://insights.diligent.com/entity-governance/the-correlation-between-corporate-governance-and-compliance/> accessed 9 June 2019.
[11] ibid.
[12] Claire Lending, Kristina Minnick and Patrick J Schorno, 'Corporate Governance, Social Responsibility, and Data Breaches' (2018) 53 Financial Review 413.
[13] ibid.
[14] ibid.
[15] ibid.

2.2.1 The Facebook – Cambridge Analytica Incident

In March 2018, it was revealed though a whistleblower that a British consulting firm, Cambridge Analytica, had acquired the personal data of 87 million Facebook users without the knowledge or permission of the users.[16] Cambridge Analytica had already been in the public spotlight due to the company's role in providing data-driven consulting services to multiple candidates in the US presidential campaign.[17]

Cambridge Analytica had used a personality quiz application which, in accordance with Facebook's own rules at the time, accessed the personal data available in their profiles.[18] This included the work histories, birthdays, interests and hobbies, and events calendars not only of the users of the applications, which were up to 300,000 people, but also the information of their friends and contacts on Facebook, yielding personal data of over 87 million people.[19]

Facebook became aware that Cambridge Analytica had acquired this data and received assurances that the firm would delete the improperly acquired data in 2015.[20] However, Facebook did nothing when they discovered this and the users whose data was implicated were not notified of this breach of Facebook's rules and Cambridge Analytica did not delete the data.[21]

The revelations had global implications, with many countries expressing concerns that improperly acquired personal data could have been used by Cambridge Analytica as a political

[16] Alex Hern, 'How to check whether Facebook shared your data with Cambridge Analytica' *The Guardian* (April 10, 2018) <https://www.theguardian.com/technology/2018/apr/10/facebook-notify-users-data-harvested-cambridge-analytica> accessed 9 June 2019

[17] Harry Davis, 'Ted Cruz Campaign Using Firm That Harvested Data on Millions of Unwitting Facebook Users | US News | The Guardian' *The Guardian* (2015) <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data> accessed 9 June 2019.

[18] Global Partners Digital, 'Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders'.

[19] ibid.

[20] ibid.

[21] ibid.

consultancies to influence elections or other democratic processes.[22] It was also a cause of major concern in Kenya as Cambridge Analytica had claimed to have worked with President Uhuru Kenyatta in the 2013 and 2017 elections, and many were worried that their personal information had been used to influence the outcome of the election.[23]

The fallout from this incident was great with Facebook being sued in the US and UK, the Facebook founder, CEO and Chairman, Mark Zukerberg facing governmental inquiries in the US, UK, and EU, and the institution of a #DeleteFacebook boycott campaign.[24] It also caused a sharp drop in share price that erased nearly 50 billion dollars of the company's market capitalization in a mere three days of the news breaking.[25]

While this was not necessarily a data breach, it was a breach of the trust of the consumers, as they had entrusted Facebook with their personal data and Facebook failed to protect it. This Facebook issue illustrates the need for corporate controls and the demands for greater accountability and care on the part of the leadership of a company when it comes to data privacy and protection. Companies that deal with the collection and processing of personal data must learn to incorporate privacy controls within their corporate governance mechanisms.[26] Company leaders should do more than just follow the letter of the law by putting themselves in the shoes of their consumers.[27]

---

[22] ibid.
[23] Njoki Chege, 'Your guide to Cambridge Analytica Kenya poll scandal,' *The Daily Nation* (21 March 2018) <https://www.nation.co.ke/news/politics/Guide-to-Cambridge-Analytica-Kenya-election-scandal/1064-4351156-jotwto/index.html> accessed 9 June 2019
[24] Iga Kozlowska, 'Facebook and Data Privacy in the Age of Cambridge Analytica' (*University of Washington*) <https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/> accessed 9 June 2019.
[25] ibid.
[26] ibid.
[27] ibid.

2.3 Duties of the Board of Directors under Kenyan Company and Corporate Governance Law

The law on corporate governance practices by companies in Kenya is statutorily provided for in the Companies Act 2015 and enforced by Capital Markets Authority through the Capital Markets Authority Act.[28] The Companies Act has codified the general common law duties and equitable principles of a director in the Act. These duties include the duty to act in good faith to promote the success of the company[29] and the duty to exercise reasonable care, skill and diligence.[30]

Under the duty to act in good faith, the Companies Act provides that a director of a company shall act in the way in which the director considers, in good faith, would promote the success of the company for the benefit of its members as a whole, and in so doing the director shall have regard to the long term consequences of any decision of the directors; the interests of the employees of the company; the need to foster the company's business relationships with suppliers, customers and others; the impact of the operations of the company on the community and the environment; the desirability of the company to maintain a reputation for high standards of business conduct; and the need to act fairly as between the directors and the members of the company.[31] There is an element of trust that a data subject places on a corporation while sharing his personal information. They trust that the company will not only protect their personal information and keep it private, but also use the information only to the extent necessary to

[28] Stephen Njoroge Gikera, Punit Vadgama and Nancy Muringo, 'Kenya Corporate Governance' (*Getting The Deal Through*, 2019) <https://gettingthedealthrough.com/area/8/jurisdiction/44/corporate-governance-kenya/> accessed 24 September 2019.
[29] ibid, Section 143.
[30] ibid, Section 145.
[31] ibid, Section 143.

provide the services and not use it for any other purposes.[32] Directors therefore have a duty to protect consumers' data to ensure that this trust is retained in order to promote the success of the company.

The Companies Act also provides that in performing the functions of a director, a director of a company shall exercise the same care, skill and diligence that would be exercisable by a reasonably diligent person with the general knowledge, skill and experience that may reasonably be expected of a person carrying out the functions performed by the director in relation to the company; and the general knowledge, skill and experience that the director has.[33] This means that Directors must continue to act with reasonable skill and care. If they have special skills or knowledge, then they will be expected to exercise them. Otherwise they will be measured against the standard of a reasonable person occupying their position. Directors therefore have a duty to exercise reasonable skill, care and diligence in order to ensure that consumers data is protected.

A board's failure to protect consumers' data, for example by failing to implement appropriate data protection measures, could equate to a breach of these duties.[34] The duty to exercise reasonable care, skill and diligence requires the standard of a reasonably diligent person with the knowledge and skill of the director in question. Directors who fail to institute adequate measures for data protection may not reach this standard.[35] Breach of directors' duties can lead to a claim being brought against the directors by the company or by shareholders through a derivative action. For instance, on January 4, 2019, the Superior Court of California approved a $29 million

[32] Ahalya Chalasani, 'Data Principal and Data Fiduciary in the Personal Data Protection Bill, 2018' (*Lakshmikumaran & Sridharan*) <https://www.lakshmisri.com/News-and-Publications/Publications/Articles/Corporate/data-principal-and-data-fiduciary-in-the-personal-data-protection-bill-2018> accessed 24 September 2019.
[33] The Companies Act No 17 of 2015, Section 145.
[34] 'Cyber Risk and Directors' Liabilities: An International Perspective' (*Norton Rose Fulbright*) <https://www.nortonrosefulbright.com/en/knowledge/publications/b0dae4a0/cyber-risk-and-directors-liabilities-an-international-perspective> accessed 24 September 2019.
[35] ibid.

settlement in derivative suits brought against directors and officers of Yahoo, Inc. for breach of their fiduciary duties arising out of two data breaches compromising sensitive information of over one billion Yahoo users.[36]

There are also various regulations and codes which stipulate principles of good corporate governance for companies in various sectors. These codes are anchored on the duties of the directors in the Companies Act. For public listed companies, the point of reference on corporate governance principles and recommendations is the Capital Markets (Securities) (Public Offers, Listing and Disclosures) (Amendment) Regulations, 2016[37] and the Code of Corporate Governance Practices for Issuers of Securities to the Public.[38] The Board of directors of public companies are responsible for formulating policies, procedures and guidelines, to ensure that these corporate governance practices are followed.[39] The principles of good corporate governance are divided into broad chapters which include: board operations and control, rights of shareholders, stakeholder relations, ethics and social responsibility, accountability, risk management and internal control, and transparency and disclosure.[40] These chapters contain the broad principles underpinning good corporate governance that companies should apply when implementing the recommendations, as well as the duties of directors to apply them.

The Code takes an "Apply or Explain" approach whereby non-compliance is acceptable in certain circumstances. The approach requires boards to fully disclose any non-compliance with the Code to relevant stakeholders including the Capital Markets Authority with a firm

[36] Re Yahoo! Inc. Shareholder Litigation., Case No. 17-CV-307054.
[37] Capital Markets (Securities) (Public Offers, Listing and Disclosures) (Amendment) Regulations 2016 (Kenya Gazette Supplement) 2249.
[38] The Code of Corporate Governance Practices for Issuers of Securities to the Public.
[39] The Code of Corporate Governance Practices for Issuers of Securities to the Public, Section 1.1.5.
[40] The Code of Corporate Governance Practices for Issuers of Securities to the Public

commitment to move towards full compliance.[41] However, the Code contains mandatory provisions which are the minimum standards that issuers must implement, and these are replicated in the Capital Markets (Securities) (Public Offers, Listing and Disclosures) Amendment Regulations, 2016 hereafter referred to as the "Capital Markets Regulations.".[42]

For state corporations, the principles and practices of good corporate governance are provided for under Mwongozo, the Code of Governance for State Corporations (Mwongozo).[43] These are organized into eight broad chapters namely:

i) Board of directors
ii) Transparency and disclosure
iii) Accountability, risk management and internal controls
iv) Ethical leadership and corporate citizenship
v) Shareholders rights and obligations
vi) Stakeholder relationships
vii) Sustainability and performance management
viii) Compliance with laws and regulation

These chapters contain the principles of good governance as well as the duties that the directors should comply with. Mwongozo is implemented on a "comply and explain" approach which expects full compliance of its provisions while recognizing that a satisfactory explanation and roadmap to full compliance by the Board may be acceptable.[44]

[41] Ibid.
[42] Ibid.
[43] Mwongozo, the Code of Governance for State Corporations (2015).
[44] Mwongozo, the Code of Governance for State Corporations (2015), xiii.

Banks in Kenya are also supposed to adhere to the Corporate Governance Prudential Guidelines for Institutions Licensed under the Banking Act which have been issued by the Central Bank of Kenya.[45] It addresses principles such as ethical leadership and integrity, responsibilities of shareholders, overall responsibilities of the board, risk management framework, compliance with laws, rules, codes and standards and governance of information technology. Insurance companies on the other hand are expected to adhere to the Corporate Governance Guidelines for Insurance and Reinsurance Companies issued by the Insurance Regulatory Authority.[46] These guidelines also contain principles for good governance such as the governance structure of the boards and the roles and responsibilities of the board.

These codes and guidelines embody the six principles of good governance developed by the OECD which are: ensuring the basis for an effective corporate governance framework, the rights of shareholders and key ownership functions, equitable treatment of shareholders, the role of stakeholders, disclosure and transparency and the responsibility of the Board. [47][48]

In line with the above mentioned good corporate governance principles, the board is expected to identify and deal with risky issues and oversee management, to ensure that they are mitigated in a way that can ensure the sustainability of the company.[49] In the context of data protection, the Board can therefore apply some of these principles to ensure that consumers data is protected.

[45] Prudential Guidelines for Institutions Licensed under the Banking Act: CBK/PG/02 Corporate Governance.
[46] Corporate Governance Guidelines For Insurance and Reinsurance Companies 2011.
[47] OECD Principles of Corporate Governance.
[48] Mwongozo, the Code of Governance for State Corporations (2015), xii
[49] Héctor J Lehuedé, 'Corporate Governance and Data Protection in Latin America and the Caribbean' (2019) <https://repositorio.cepal.org/bitstream/handle/11362/44629/1/S1900395_en.pdf> accessed 21 September 2019.

2.4 The Application of Corporate Governance Principles in Data Protection

Within corporate governance, the board of directors need to apply the principles of good corporate governance articulated in the above-mentioned regulations and guidelines, that may have an impact on ensuring data protection for consumers. These include the board composition and committees, stakeholder relationships, ethics and social responsibility, risk assessment and management, accountability and transparency, governance of information technology and compliance with laws and regulations.[50]

2.4.1 Board composition and committees

Recent cases of data breaches have shown that, many large and sophisticated companies are not sufficiently prepared to tackle the data protection risks facing the company. Some of the key factors that may be affecting them are the skills set of those who sit at the board and how they allocate responsibilities to specialized board committees.[51]

The Capital Markets Regulations provides that the board shall have an appropriate balance of skills, experience, independence and knowledge of the company to enable the board to operate effectively.[52] Mwongozo also provides that the composition and size of the board should provide a diversity of competencies and skills required for effective leadership of the organisation.[53]

A well-structured board of directors involves having directors with diverse skills and experience who can collectively address emerging challenging issues. As at 2017, a study by Deloitte showed that directors with skills and experience involving technology or data privacy are

[50] Jason Woywada, 'The Impact of Public Privacy on Corporate Governance: How Recent Findings in the Common Thread Network Can Impact Corporate Directors'.
[51] Lehuedé (n 49).
[52] Capital Markets (Securities) (Public Offers, Listing and Disclosures) (Amendment) Regulations, 2016, F.02 (2)(a)
[53] Mwongozo, the Code of Governance for State Corporations (2015), 1.

currently a minority,[54] which poses the risk that in the absence of the necessary knowledge at the board, the Board may not be able to discharge their duty in ensuring that consumer data is protected. Companies should therefore look to add this specific expertise to their boards, so that they can exercise ownership for these issues.[55]

It is also possible to improve the skills of those already at the board in order to ensure that they can address data protection issues. This is a good corporate governance practice provided for under the Code of Corporate Governance[56] as well as Mwongozo.[57]

Board committees are also a way to help boards to deal with particularly complex issues, as they allow the board to have a smaller group of members, sometimes with the help of external experts, to spend sufficient time on such issues to prepare the discussion at the board level, where they subsequently report.[58] The Code of Corporate Governance recommends that the Board shall establish committees to cover broad functions of the company such as risk management, audit and governance among others.[59] The committees shall be appropriately constituted with members who have the necessary skills and expertise to handle the responsibilities allocated to them. Where some skills are not available, the Board may nominate independent and external professionals to that committee.[60] Mwongozo also provides that the Board may establish committees to deal with technical matters.[61] Though the Code of Corporate Governance and the Mwongozo only specifically provide for the structure of an audit committee

[54] Tom Reeve, 'Only 5% of FTSE Companies Have Cyber-Security Expertise on the Board' (*SC Media*, 2017) <https://www.scmagazineuk.com/5-ftse-companies-cyber-security-expertise-board/article/1475347> accessed 25 September 2019.
[55] Lehuedé (n 49).
[56] The Code of Corporate Governance Practices for Issuers of Securities to the Public 2015, Recommendation 2.3.1
[57] Mwongozo, the Code of Governance for State Corporations (2015), 4
[58] Lehuedé (n 49).
[59] The Code of Corporate Governance Practices for Issuers of Securities to the Public 2015, Recommendation 2.2.2
[60] The Code of Corporate Governance Practices for Issuers of Securities to the Public 2015, Recommendation 2.2.2
[61] Mwongozo, the Code of Governance for State Corporations (2015), 1.7

and a nominations committee, companies can also create a committee to deal with data protection issues in order to safeguard the interests of the consumer who give their data to the company and protect their privacy.

2.4.2 Stakeholder Relations

The Code of Corporate Governance provides that a company's corporate governance framework should recognise the rights of stakeholders and encourage active co-operation between companies and stakeholders in creating wealth, and sustainability of financially sound enterprises.[62] It recommends that the board shall have a stakeholder-inclusive approach in its practice of corporate governance and that it should identify all its stakeholders.[63] It goes on ahead to state that "the board should strive, while acting in the best interests of the company, to achieve an appropriate balance between the interests of its various stakeholders, in order to achieve the long-term objectives of the company."[64] Mwongozo also provides that the board should identify the rights of key stakeholders and ensure that their rights are protected.[65]

Stakeholders are groups and individuals "who benefit from or are harmed by, and whose rights are violated or respected by, corporate actions."[66] This includes owners, customers, consumer advocates, competitors, media, employees, environmentalists, suppliers, governments, local community organizations, and special interest groups among others.[67]

[62] The Code of Corporate Governance Practices for Issuers of Securities to the Public, 4.0.
[63] The Code of Corporate Governance Practices for Issuers of Securities to the Public, Recommendation 4.1.1.
[64] The Code of Corporate Governance Practices for Issuers of Securities to the Public, Recommendation 4.1.1.
[65] Mwongozo, the Code of Governance for State Corporations (2015), 6.2.1.
[66] David Paas, 'Stakeholders and Participation in Corporate Governance: A Critique of Some of the Arguments' (1996) 15 Business & Professional Ethics Journal 3 <https://about.jstor.org/terms> accessed 8 June 2019.
[67] ibid.

The issue of corporate stakeholder relations in corporate governance is relevant to data privacy in companies given data and information is contributed by stakeholders, especially consumers who are contractual stakeholders, to an organization for it to collect, append, and store.[68]

2.4.3 Ethics and Social Responsibility

The Code of Corporate Governance provides that a company should establish an ethical relationship between the company and the society in which it operates.[69] It stipulates that companies should strive to be socially responsible.[70] The Mwongozo also provides that an organization should strive to operate ethically and promote corporate social responsibility.[71]

Ethics can be defined broadly as the study of what is right and wrong, and using principled decision making to choose actions that are good for human beings and do not hurt others.[72] It attempts to determine what people ought to do and what goals they should pursue. Business ethics is the study and determination of what is right and good in business settings.[73] Corporate Social Responsibility (CSR) is defined as "the commitment of business to contribute to sustainable economic development, working with employees, their families, the local community and society at large to improve quality of life, in ways that are both good for business and good for development."[74]

A study by Pollach shows that some companies are embracing data protection of their stakeholders as a corporate social responsibility by taking care of the way they collect and use

[68] Woywada (n 50).
[69] The Code of Corporate Governance Practices for Issuers of Securities to the Public.
[70] ibid.
[71] Mwongozo: The Code of Governance for State Corporations 2015.
[72] Joseph Weiss, *Business Ethics: A Stakeholder and Issues Management Approach* (2014, Berrett-Koehler Publishers) 14
[73] ibid.
[74] Djordjija Petkoski and Nigel Twose, 'Public Policy for Corporate Social Responsibility' (2005) <http://web.worldbank.org/archive/website01006/WEB/IMAGES/PUBLICPO.PDF> accessed 8 November 2019.

data, ensuring that their technology does not just violate privacy but also enhance privacy, developing privacy-enhancing products or committing themselves to educating consumers about privacy protection.[75] CSR has been categorized into economic, legal, ethical, and philanthropic responsibilities.[76] According to this classification, data protection can be categorized as an ethical responsibility, given that legislation is insufficient to govern corporate decision making in all areas of data handling.[77] It has also been argued that CSR initiatives can bring sustainable competitive advantages in the form of a first-mover advantage. The first mover advantage refers to an advantage gained by a company that first introduces a product or service to the market.[78] However, for this advantage to emerge, the company must not only be the first one to address a particular CSR comprehensively but must also continuously seek to enhance what it has achieved in order to secure this advantage.

Furthermore, Balboni argues that no present or forthcoming legal framework would ever be able to effectively regulate our data-centric society while also perfectly maximizing the benefits for citizens and effectively minimizing risks that new technologies pose.[79] Regulators can no longer be the police of the internet and it is now past the time when companies were able to consider data protection and fair competition practices as mere legal compliance obligations. In this data-

[75] Irene Pollach, 'Online Privacy as a Corporate Social Responsibility: An Empirical Study' (2011) 20 Business Ethics 88.
[76] Archie B. Carroll 'A Three-Dimensional Conceptual Model of Corporate Performance,' (1979) 4 The Academy of Management Review, 4, 497.
[77] Archie B. Carroll 'A Three-Dimensional Conceptual Model of Corporate Performance,' (1979) 4 The Academy of Management Review, 4, 497.
[78] Marvin B. Lieberman and David B. Montgomer 'First-Mover Advantages' (1988) 9 Strategic Management Journal 41 accessed www.jstor.org/stable/2486211 on 13 September 2019.
[79] Paolo Balboni, 'Data Protection as a Corporate Social Responsibility' (2018) Paolo Balboni | ICT, Policy and Data Science < https://www.paolobalboni.eu/index.php/2018/05/21/data-protection-as-a-corporate-social-responsibility/> accessed 13 September 2019.

centric world companies need to consider fair practices, privacy, and data protection as assets that can help companies to responsibly further their economic targets.[80]

Several authors therefore suggest that companies could benefit from embracing data privacy and protection as a CSR initiative, especially if they make this commitment visible to external audiences.[81] For example, some companies like Toshiba have implemented data protection as CSR, listing data protection as a section in their annual CSR reports.[82]

2.4.4 Risk Assessment and Management

As discussed previously, directors have a duty to act with the standard of care and diligence appropriate for a reasonable person acting in the same circumstances as the director and with the same responsibilities as the director.[83] It is therefore the duty of the board to establish a sound system of risk oversight and management and internal controls.[84] The Code of Corporate Governance as well as the Mwongozo also provide that the Board has a responsibility to ensure adequate systems and processes of risk management and internal control are in place in order to achieve its strategic objectives.[85]

Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives.[86]Risk assessment therefore is the process of identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity

[80] Ibid.
[81] Irene Pollach, 'Online Privacy as a Corporate Social Responsibility: An Empirical Study' (2011) 20 Business Ethics 88.
[82] Toshiba, '2014 Corporate Social Responsibility Report' <http://www.toshiba.co.jp/csr/en/report/pdf/report14_all.pdf> accessed 9 September 2019.
[83] The Companies Act No 17 of 2015.
[84] Malcolm Crompton, 'Privacy Governance : A Guide to Privacy Risk and Opportunity for Directors and Boards'.
[85] The Code of Corporate Governance Practices for Issuers of Securities to the Public, 6.0; Mwongozo: The Code of Governance for State Corporations, 20.
[86] Committee of Sponsoring Organizations of the Treadway Commission, 'Internal Control-Integrated Framework' (2013) <https://na.theiia.org/standards-guidance/topics/Documents/Executive_Summary.pdf> accessed 8 June 2019.

are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed.[87] One of the elements of a risk assessment and management is having an appropriate policy on how to implement data privacy.[88] Directors should satisfy themselves that management have implemented adequate systems and procedures to ensure that the risk of a potential breach of privacy is minimized.[89]

Trickery emphasizes the importance of risk assessment of information security by stating, "Security of corporate information has emerged as a virulent form of risk. No longer a technical issue at the operational level, boards need to involve information technology expertise in every major decision at the managerial and strategic levels."[90] Privacy impacts very many aspects of an organization and therefor it is important to assess it as a risk.[91]

In 2015, the OECD Council adopted the *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*[92] as a build up to the 1980 Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Trans border Flows of Personal Data. The Recommendation calls on the highest level of leadership in government and in public and private organizations to adopt an approach to digital security risk management that builds trust and takes advantage of the open digital environment for economic and social prosperity.[93] Digital security risk is described as " a category of risk related to the use, development and management of the digital environment in the course of any

[87] ibid.
[88] Crompton (n 84).
[89] ibid.
[90] Robert Tricker, *Corporate Governance: Principles, Policies, and Practices* (Oxford University Press 2015) <https://books.google.co.ke/books?hl=en&lr=&id=X4qQBgAAQBAJ&oi=fnd&pg=PP1&dq=agency+dilemma+in+corporate+governance&ots=G17Gxe_ScV&sig=9EcNQFsUPJwOuPAZ4tlp7a_OfQ4&redir_esc=y#v=onepage&q=agency dilemma in corporate governance&f=false> accessed 8 June 2019.
[91] Woywada (n 50).
[92] OECD, 'Digital Security Risk Management for Economic and Social Prosperity' (2015) <http://dx.doi.org/10.1787/9789264245471-en> accessed 8 June 2019.
[93] ibid.

activity. This risk can undermine the achievement of economic and social objectives by disrupting the confidentiality, integrity and availability of the activities and/or the environment. It includes aspects related to the digital and physical environments, the people involved in the activity and the organizational processes supporting it."[94] This definition can also encompass personal data and the risks associated with the protection of data. Boards, as the leaders of the organizations are therefore encouraged to manage digital risks effectively to avoid the loss of reputation as well as to enhance economic and social prosperity.

2.4.5 Accountability and Transparency

Accountability and transparency are important principles of good corporate governance articulated within the Code of Corporate Governance and the Mwongozo as well as the OECD Principles of Good Governance.[95] Accountability as a principle of good corporate governance is described as being answerable to the higher authority. The main focus of accountability in the corporate setting is the management of the companies including the board of directors who are entrusted with the responsibility of operating the business affairs of a company.[96] It reflects monitoring the work of the company and the board of directors so that they are delivering for the best interest of the all shareholders and shareholders.[97] This goes hand in hand with transparency which means the declaration of actual picture of the firm in manner of its operations to its shareholders and stakeholders have the right to the full true disclosure of information.[98]

---

[94] ibid.
[95] OECD Principles of Corporate Governance.
[96] Zain Ullah, Alam Rehman and Abdul Waheed, 'The Impact of Corporate Accountability and Transparency on the Performance of Manufacturing Sector Firms Listed on KSE' <http://ssrn.com/abstract=2756977iElectroniccopyavailableat:http://ssrn.com/abstract=2756977ii> accessed 8 June 2019.
[97] ibid.
[98] ibid.

Though these principles are mostly discussed in the context of financial transparency and accountability, they are also applicable in ensuring data protection within an organization. Under the principle of information privacy, companies that collect personal data in the course of their business should be accountable for the safe and fair management of that data. [99] This extends to ensuring that the data is protected. This principle is now increasingly being adopted into data protection laws and regulations. For example, Article 5 of the GDPR stipulates the accountability principle whereby the controller is responsible for making sure privacy principles are adhered to.[100] Article 24 further specifies the controller's responsibility of accountability that "the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."

Similarly, transparency is a core principle of data protection. This has also been incorporated into data protection laws such as the GDPR which provides that personal data must be processed lawfully, fairly and in a transparent manner.[101] Additionally, Articles 12 to 15 calls for technical means to support the obtaining of explicit consent from data subjects and the provision of transparency with respect to personal data processing and sharing.[102] Companies need to ensure that information about personal data processing activities and personal data transactions, for example, who shared what data with whom, for what purpose and under what usage conditions,

[99] James X Dempsey, Fred H Cate and Martin Abrams, 'Organizational Accountability , Government Use of Private-Sector Data , National Security , and Individual Privacy'.
[100] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[101] ibid.
[102] Consumers International, 'The State of Data Protection Rules around the World: A Briefing for Consumer Organizations' <https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf>.

must be provided to data subjects in a concise, transparent and easily accessible form, using clear and plain language record.[103]

2.4.6 Governance of Information Technology

Though the governance of information technology (IT) has not been discussed in many corporate governance codes, it is increasingly becoming an important emerging issue in the realm of corporate governance. The CBK recognized this and provided for it as a principle of corporate governance for banking institutions. The Prudential Guidelines defines IT governance as a framework that supports effective and efficient management of IT resources to facilitate the achievement of an institution's strategic objectives.[104] IT governance is the responsibility of the board.

According to Robert Smallwood, data governance is a subset of broader IT governance.[105] Data governance has been defined as 'A companywide framework for assigning decision-related rights and duties in order to be able to adequately handle data as a company asset'.[106] The main driver for data governance is considering data as an asset of the company.[107] Data governance also refers to the overall management of the availability, usability, integrity, and security of the data used in an organization.[108] Although the definition of data governance is still evolving, the discipline of data governance can be described as being a facilitator for managers to take control

[103] Piero Bonatti and others, 'Transparent Personal Data Processing: The Road Ahead' <https://www.specialprivacy.eu/images/documents/TELERISE17.pdf> accessed 8 June 2019.
[104] Prudential Guidelines for Institutions Licensed under the Banking Act: CBK/PG/02 Corporate Governance.
[105] Robert Smallwood, 'Information Governance, IT Governance, Data Governance: What's the Difference? - Information Governance: Concepts, Strategies, and Best Practices [Book]', *Information Governance: Concepts, Strategies, and Best Practices* (John Wiley & Sons 2016) <https://www.oreilly.com/library/view/information-governance-concepts/9781118218303/10_chap02.html> accessed 25 September 2019.
[106] Ibrahim Alhassan, David Sammon and Mary Daly, 'Data Governance Activities: An Analysis of the Literature' (2016) 25 Journal of Decision Systems 64 <http://dx.doi.org/10.1080/12460125.2016.1187397>.
[107] ibid.
[108] Zhang Ning and Qin JianYuan, 'An Overview of Data Governance' [2018] Valuing Data 9.

over all aspects of their data resource.[109] Though the studies on data governance emphasize it as being an issue for IT and data managers, it is also an issue of corporate governance.

As discussed previously, corporate governance is the highest level of organizational management, exercised by the board who oversee the organization's activities for the benefit of the shareholders and stakeholders. On the other hand, data governance concerns the management of the data universe. Since the study of data governance treats data as an asset, then data governance and corporate governance within the company ought to be aligned, especially in the terms of the Board ensuring proper management of data risks and security and making strategical decisions on the data that the company holds.

2.4.7 Compliance to Laws and Regulations

Griffith describes compliance is "the new corporate governance."[110] He defines compliance as the means by which firms adapt behavior to legal, regulatory, and social norms.[111] He argues that all firms exist within a nexus of legal, regulatory, and social norms and therefore they need to adapt their behavior to these constraints. Compliance is therefore the set of internal processes used by firms to adapt behavior to applicable norms.[112] A company establishes internal mechanisms to prevent and detect violations of law and regulation.

In line with this, a company practicing good corporate governance should ensure compliance to all laws that affect the running of the company. This includes data privacy rules and regulations. While some countries, including Kenya, do not have national legislation on data privacy and

[109] ibid.
[110] Sean J Griffith, 'Corporate Governance in an Era of Compliance' (2016) 57 William & Mary Law Review 2075 <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1872&context=faculty_scholarship> accessed 9 June 2019.
[111] ibid.
[112] ibid.

protection, many organizations will be affected by the GDPR as well as other international laws due to transborder flow of information.

Furthermore, some countries such as the United States of America (USA) have incorporated data protection standards into their corporate governance regulations. For example, the Sarbanes-Oxley Act of 2002, which sets corporate governance standards for all USA public company boards, management and public accounting firms contains sections that concern protecting data.[113] These data protection requirements in sections 302 and 404 are mostly concerned with the accuracy and content of required financial reports.[114] The compliance requirement implications for public companies to protect data are that:

- Any financial information needs to be safeguarded and its integrity assured.[115]
- Specific internal security controls need to be identified that protect this data and auditing must take place annually to ensure that this is done.[116]

Companies therefore need to ensure compliance to such laws in line with good corporate governance practice in order to ensure that data is protected.

2.5 Conclusion

This chapter has focused on the protection duties of directors with regards to data. It has looked at how data breaches can affect a company. It has also looked at the case of Facebook whereby a data breach affected the share price of the company as well as caused a breach of trust between the company and its consumers. The chapter then explored the duties of directors in relation to

[113] Sarbanes Oxley Act of 2002, Section 302 & 404
[114] ibid
[115] Thales, 'What is Sarbanes-Oxley (SOX) Act Data-at-Rest Security Compliance?' <https://www.thalesesecurity.com/faq/americas-compliance/what-sarbanes-oxley-sox-act-data-rest-security-compliance> accessed 19 November 2019
[116] Ibid

ensuring that consumer data is protected and then delved into the incorporation of data protection into corporate governance practices and how the principles of corporate governance overlap with the principles of data protection. The aim was to find out corporate governance practices can be applied to protect consumers' data in Kenya in the absence of a comprehensive data protection law.

The next chapter shall look at the development of data protection through international, regional and national initiatives. It shall also look at the various models of data protection applied in various parts of the world and examine the link between corporate governance and data protection in order to establish the role of corporations to ensure consumer data is protected.

CHAPTER THREE

BACKGROUND TO DATA PRIVACY AND CONSUMER DATA PROTECTION

3.1 Introduction

In the recent times, data privacy and data protection has emerged as one of the most pertinent issues globally. Every day, vast amounts of information are transmitted, stored and collected around the world, enabled by vast improvements in technology and communication power.[1] This is done mostly by governments and corporations. In the digital age, the processing of personal data is hugely valuable. It offers undeniable opportunities for economic growth, social advancement and research. It can also pose risks to an individual right to privacy.[2]

In developing countries such as Kenya, there has been a rapid increase of online social, economic and financial activities which have been facilitated through increased uptake of mobile money transactions and greater internet connectivity. For example, in the month of December 2018 there were approximately 155 million mobile transactions done in the value of about Kenya Shillings 367 billion.[3] Furthermore, the 2017 estimate of Internet users in Kenya from the International Telecommunications Union (ITU) is approximately 43 million corresponding to a penetration rate of 89.4%.[4] Arguably, due to this increase of internet users, the amount of consumer data being collected by businesses is increasing every day.

As more and more economic and social activities move online, the importance of data protection and privacy is increasingly recognized both globally as well as in Kenya. This chapter examines

[1] United Nations Conference on Trade and Development (UNCTAD), 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' [2016] United Nations Publication <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf>.
[2] Global Partners Digital, 'Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders'.
[3] Central Bank of Kenya, 'Mobile Payments,' accessed from https://www.centralbank.go.ke/national-payments-system/mobile-payments/
[4] Internet World Statistics accessed from https://www.internetworldstats.com/af/ke.htm

the development of consumer data protection and data privacy laws and their implementation in corporations. It begins by looking at the historical background of data protection and data privacy regulations and policy at a global level as well as consumer protection regulations. It then looks at the collection and processing of consumer data in corporations in order to illustrate the data problem as well as the models applicable in ensuring consumer data is protected.

3.2 Historical Development of Data Privacy and Data Protection Regulations

Personal data has been collected, stored, used, and disseminated throughout history.[5] For example, censuses have been conducted by governments since the ancient Roman times when administrators went door to door to gather information on citizens, ranging from the size of their household to the amount of land owned.[6] Data has also been used in experiments and studies to prove theories for hundreds of years.[7]

However, the development of the computer in the 1950s, and the increasing use of them in the 1960s, changed the nature of who and how personal data was collected and processed, and the extent of the need to protect it.[8] Even before the internet, the computer had already revolutionized the ways that data was collected, stored, used, and disseminated.[9] The development of data collection and storage through the use of computers led to public concerns in the 1960s, particularly in the United States and in Europe, where computers were beginning to be widely used at that time. While privacy laws already existed, they were broad and undefined, and did not offer much guidance on what to do about protecting the right to privacy when so much personal information was being processed. In response, governments in both the United

[5] Global Partners Digital (n 2).
[6] Ibid
[7] 'How the History of Data Gathering Lead to the Age of Big Data', accessed from https://www.smartdatacollective.com/history-data-gathering-lead-age-of-big-data-personalization/
[8] Global Partners Digital (n 2).
[9] Ibid

States and Europe agreed that there was a need to regulate the processing of personal data. This led to the development of international initiatives to ensure that the right to privacy was protected and that there was data protection.[10] This then cascaded into different regimes of data protection regulations regionally and nationally.

3.2.1 International Initiatives on Data Protection

This section shall look at four international initiatives with a near-global reach namely the United Nations, the Council of Europe Convention 108, the OECD and the International Data Protection Commissioner's Initiatives**.**

a) United Nations

The United Nations has a long provided for the right to privacy through its human rights treaties. Article 12 of the Universal Declaration of Human Rights stipulates, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[11] Article 17 of the International Covenant on Civil and Political Rights contains similar provisions.[12]

Moreover, since 2013, the United Nations started strengthening its provisions on privacy rights protection by providing for digital privacy rights. In December 2013, the United Nations General Assembly adopted resolution 68/167, which expressed concern for the negative impact that online communications and surveillance may have on human rights.[13] The General Assembly

[10] Global Partners Digital (n 2).
[11] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) article 12
[12] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR)
[13]United Nations, Right to Privacy in the Digital Age Resolution 68/167 <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx> accessed 14 April 2019.

called upon all States to respect and protect the right to privacy in digital communication. They also asked the signatory states to review their procedures, practices and legislation relating to the collection of personal data and emphasized the need for States to ensure the full and effective implementation of their obligations under international human rights law.[14]

In July 2015, the Human Rights Council appointed the first-ever Special Rapporteur on the right to privacy.[15] The Special Rapporteur was mandated by Human Rights Council Resolution 28/16: "

i) To gather relevant information and to study trends, developments and challenges in relation to the right to privacy and to make recommendations to ensure the right to privacy is protected in connection with the challenges arising from new technologies;
ii) To seek, receive and respond to information, from States, the United Nations and its agencies, programmes and funds, regional human rights mechanisms, national human rights institutions, civil society organizations, the private sector, including business enterprises, and any other relevant stakeholders or parties;
iii) To identify possible obstacles to the promotion and protection of the right to privacy, to identify and promote principles and best practices at the national, regional and international levels, and to submit proposals and recommendations to the Human Rights Council;
iv) To participate in and contribute to relevant international conferences and events with the aim of promoting a systematic and coherent approach on issues pertaining to the mandate;

[14] Ibid
[15] OHCHR 'Special Rapporteur on Privacy'
<https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx> accessed 30 April 2019.

v) To raise awareness concerning the importance of promoting and protecting the right to privacy;

vi) To integrate a gender perspective throughout the work of the mandate;

vii) To report on alleged violations of the right to privacy in connection with the challenges arising from new technologies;

viii) To submit an annual report to the Human Rights Council and to the General Assembly."[16]

The Special Rapporteur has been preparing annual reports on the right to privacy since 2016 which are submitted to the Human Rights Council and the UN General Assembly.[17]

However, though the UN initiatives have global implications, there are limitations to the initiatives as the current treaty provisions are too 'high level' for day-to-day impact as the right to privacy needs to be translated into further detailed principles.[18]

b) The Council of Europe Convention 108

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981 (usually referred to as Convention 108 or the Council of Europe Convention) was the first binding international instrument which provided for the protection of the individual against abuses to right to data privacy which may accompany the collection and processing of personal data and which seeks to regulate the trans-border flow of personal data.[19] The convention also stipulates the right of an individual to know that

[16] ibid.
[17] ibid.
[18] United Nations Conference on Trade and Development (UNCTAD) (n 1).
[19] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (adopted 28 January 1981 Treaty No.108 <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> accessed 30 April 2019.

information is stored on him or her and, if necessary, to have it corrected.[20] Furthermore, it imposes restrictions on trans-border flows of personal data to states which do not provide such protection under their laws and regulations.[21]

Although this Convention was established by the Council of Europe, it is open for accession by non-member states.[22] As of 2019, 54 countries have ratified or acceded the convention including all the forty-seven Council of Europe member States and 7 non-members states.[23] Consequently, most of the countries that have ratified the convention have implemented data protection laws that comply with it.[24] Two other countries, Morocco and Burkina Faso, are currently exploring membership.[25]

The convention is different from other international initiatives on data protection in that it is the world's only legally binding instrument specifically focused on data protection.[26] Signatories have to take the necessary measures in its domestic law to give effect to the basic principles for data protection provided for in the convention.[27]

According to UNCTAD, the Council of Europe Convention is one of the most promising international developments as "it provides comprehensive coverage; there is wide acceptance of the principles contained within; it provides the ability for any country to join; it works through a collaborative open process; the binding nature of the agreement drives harmonization; and it has strong support from other initiatives such as the International Data Protection Commissioners as

[20] ibid.
[21] ibid.
[22] ibid.
[23] ibid.
[24] ibid.
[25] ibid.
[26] Global Partners Digital (n 2).
[27] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, art 4 <https://rm.coe.int/1680078b37> accessed 30 April 2019.

the best global model available."[28] Nonetheless, it still has limits in that it is largely Eurocentric and faces challenges in accommodating the different national systems.[29]

c) OECD

The Organisation for Economic Co-operation and Development (OECD) is an intergovernmental organization of 36 high-income economy countries founded to promote policies that will improve the economic progress and social well-being of people around the world.[30] In 1980, it developed a privacy guideline to harmonies rules around personal data, and trans-border flows of personal data, known as the OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data in consultation with a broad group of stakeholders.[31] These guidelines were updated in 2013.[32]

The OECD Guidelines have had a major influence on the content of privacy laws around the world.[33] They stipulate eight privacy principles that are the pillar of most national privacy laws.[34] These are:

i) Collection limitation principle: There should be limited the collection of personal data and any such data should be obtained by lawful and fair means with the knowledge or consent of the data subject.[35]

ii) Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used, accurate, complete and kept up to date.[36]

[28] United Nations Conference on Trade and Development (UNCTAD) (n 1).
[29] ibid.
[30] OECD 'About the OECD' <http://www.oecd.org/about/> accessed 30 April 2019.
[31] United Nations Conference on Trade and Development (UNCTAD) (n 1).
[32] OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted on 23 September 1980, <https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm> accessed 30 April 2019.
[33] United Nations Conference on Trade and Development (UNCTAD) (n 1).
[34] ibid.
[35] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Article 7.

iii) Purpose Specification Principle: Personal data should be collected, stored and used for specified legitimate purposes only, and not in a way which is incompatible with those purposes.[37]

iv) Use Limitation Principle: Personal data should not be used or disclosed for purposes other than those specified when they are collected except with the consent of the data subject or by the authority of law.[38]

v) Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification or disclosure of data.[39]

vi) Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Guidelines should be readily available to establish the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.[40]

vii) Individual Participation Principle: An individual should be able to request from a data controller whether the data controller has data relating to him and to have the data relating to him communicated in a reasonable time and manner.[41]

viii) Accountability Principle: A data controller should be accountable to comply with the principles.[42]

---

[36] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Article 8.
[37] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Article 9.
[38] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Article 10.
[39] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Article 11.
[40] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Article 12.
[41] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Article 13
[42] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Article 14

These principles remained the same when the guidelines were updated in 2013. The updated Guidelines also introduced new concepts such as:

a) National privacy strategies which show the increased strategic importance of data privacy policy and the need for good cross department coordination within governments;[43]
b) Privacy management programmes to serve as the core operational mechanism through which organizations implement privacy protection;[44] and
c) Data security breach notification that covers both notice to an authority and notice to an individual affected by a security breach affecting personal data.[45]

Additionally, it introduced a new section on accountability; an updated section on trans-border data flows; and expanded the sections on national implementation and international cooperation.[46]

The revision focuses on the practical implementation of privacy through an approach grounded in risk assessment and management. Risk assessment helps determine which safeguards are necessary and should be assessed through a process of identifying and evaluating the risks to an individual's privacy.[47]

In 2015, the OECD also developed Recommendation on Digital Security Risk Management for Economic and Social Prosperity which emphasizes that digital risk should be treated as an economic risk instead of just a technical issue, but as an economic risk.[48] Furthermore, digital

[43] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
[44] ibid.
[45] ibid.
[46] United Nations Conference on Trade and Development (UNCTAD) (n 1).
[47] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
[48] OECD, 'Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document' (2015) <http://dx.doi.org/10.1787/9789264245471-en> accessed 30 April 2019.

risk should be an "integral part of an organization's overall risk management and decision making." The OECD Privacy Guidelines and this Recommendation complement each other and signify a shift towards a more rounded policy approach to digital data protection.[49] This Recommendation also calls for national strategies and strengthened international cooperation in digital risk management.[50]

In spite the OECD Guidelines being widely accepted, they still have several weaknesses in that: they are non-binding and have no global focus.[51]

The OECD Guidelines for Consumer Protection in the Context of Electronic Commerce also include provisions related to privacy and data protection.[52] The guidelines set out the core characteristics of effective consumer protection for online business-to-consumer transactions and emphasize the need for co-operation among governments, businesses and consumers.[53] These guidelines were updated in 2016 to address new and emerging trends and challenges faced by consumers in today's dynamic e-commerce marketplace.[54]

d) International Data Protection Commissioner's Initiatives

The International Conference of Data Protection and Privacy Commissioners is a global membership forum for data protection authorities.[55] Their main role is the regulation of national

[49] United Nations Conference on Trade and Development (UNCTAD) (n 1).
[50] OECD, 'Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document' (n 141).
[51] United Nations Conference on Trade and Development (UNCTAD) (n 1).
[52] OECD Guidelines for Consumer Protection in the Context of Electronic Commerce approved 9 December 1999 <www.oecd.org> accessed 1 May 2019.
[53] ibid.
[54] OECD, 'Consumer Protection in E-Commerce OECD Recommendation' (2016) <http://dx.doi.org/10.1787/9789264255258-en.> accessed 15 April 2019.
[55] 'International Conference of Data Protection and Privacy Commissioners' <https://icdppc.org/> accessed 1 May 2019.

data protection laws, but they are also involved s in the global privacy debate.[56] Their three main initiatives are having an annual meeting and conference, incorporating a system for cooperating in international and cross-border complaints; and making statements which reference international standards and agreements and shared commitments among the members with regards to global privacy.[57] It seeks to provide leadership at international level in data protection by connecting the efforts of data protection authorities worldwide.[58]

At their 2005 meeting, they issued a statement titled: 'The protection of personal data and privacy in a globalized world: a universal right respecting diversities (the Montreux Declaration).'[59] The Declaration called for the development of a legally binding international convention on data protection, for every government in the world to promote the adoption of legal instruments of data protection and privacy according to the basic principles of data protection, and for the Council of Europe to invite, non-member states which already have a data protection legislation to accede to the Council of Europe Convention.[60] It is one of the most significant efforts to harmonize data protection laws worldwide.[61] Nevertheless, it is non-binding and lacks a formal structure or follow-up.[62]

In 2009, they adopted a "Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data", which set out basic data protection

[56] United Nations Conference on Trade and Development (UNCTAD) (n 2).
[57] ibid.
[58] 'International Conference of Data Protection and Privacy Commissioners' (n 148).
[59] 'Montreux Declaration: The Protection of Personal Data and Privacy in a Globalized World: A Universal Right Respecting Diversities' (2005) <www.datenschutz-berlin.de/doc/intAwednUtc> accessed 14 April 2019.
[60] ibid.
[61] United Nations Conference on Trade and Development (UNCTAD) (n 1).
[62] ibid.

principles and was meant to serve as a background to deliberations of a data protection treaty by the UN General Assembly.[63]

3.2.2 Regional Initiatives on Data Protection

Regional initiatives in data protection are usually more advanced than the international initiatives because interests at the regional level are more similar than at a global context. Even with restrictions on membership, some of these regional developments can influence matters beyond their regional boundaries.[64] However, they take different approaches, posing that could create barriers to interoperability.[65]

a) The European Union

The European Union is an economic and political union between 28 European countries that together cover much of the Western Europe continent and accounts for a significant proportion of the global trade.[66] The EU has a long history of involvement in coming up with data protection initiatives which have had a worldwide impact due to trade between the EU and non-EU members states.[67]

In the European Union, there are three instruments that impact on data protection such namely the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Charter on Fundamental Rights of the European Union and the EU General Data Protection Regulation.

i) European Convention for the Protection of Human Rights and Fundamental Freedoms

---

[63] Global Partners Digital (n 2).
[64] United Nations Conference on Trade and Development (UNCTAD) (n 1).
[65] ibid.
[66] 'About the EU - The EU in Brief', <https://europa.eu/european-union/about-eu/eu-in-brief_en#from-economic-to-political-union> accessed 15th April 2019
[67] United Nations Conference on Trade and Development (UNCTAD) (n 1).

The Convention for the Protection of Human Rights and Fundamental Freedoms, referred to as the European Convention on Human Rights, which was adopted in Rome in 1950 and entered into force in 1953 sets forth a number of fundamental rights and freedoms including the right to privacy.[68]

Article 8 provides that "Everyone has the right to respect for his private and family life, his home and his correspondence."[69] It also states that "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." These provisions have been applied in several decisions on data protection. For example, in the case of *Rechnungshof v. Osterreichischer Rundfunk*[70] the court held that the collection of data by name relating to an individual's professional income, with a view to communicating it to third parties, falls within the scope of Article 8 and that communication of the data infringes the right of the persons concerned to respect for private life.

ii) Charter on Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union, which was adopted in 2000, and became legally binding in the EU in 2009, is the first example of an international human rights

[68] Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, (4 November 1950) ETS 5, https://www.refworld.org/docid/3ae6b3b04.html accessed 22 September 2019
[69] Ibid, Article 8
[70] Rechnungshof v. Osterreichischer Rundfunk C-465/00 AND C-138/01, (2003)

instrument which provides for the right to data protection as a fundamental human right which is distinct from the right to privacy.[71]

Article 8 provides that "everyone has the right to the protection of personal data concerning him or her".[72] It also provides that "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law" and guarantees that "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".[73] Finally, it also stipulates that EU member states designate an independent authority to ensure compliance with these rules.[74]

iii) EU General Data Protection Regulation

The General Data Protection Regulation, commonly referred to as the GDPR is a European Union law which entered into force in 2016 and became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring ratification by the EU Member States through national law.[75] It was developed to replace the EU Data Protection Directive of 1995.[76] It is a mandatory regulation that ensures the harmonization of data protection laws and regulations across all EU member states.[77] Primarily, the application of the GDPR depends on whether an organization is established in the EU. However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the EU where the processing activities are

[71] Global Partners Digital, 'Travel Guide to the Digital World: Encryption Policy for Human Rights Defenders'.
[72] Charter of Fundamental Rights of The European Union 2000 (Official Journal of the European Communities).
[73] ibid.
[74] ibid.
[75] 'The History of the General Data Protection Regulation', https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en accessed 15th April 2018
[76] Ibid.
[77] United Nations Conference on Trade and Development (UNCTAD) (n 1).

related to the offering of goods or services to such data subjects in the EU or the monitoring of their behaviour as far as their behaviour takes place within the EU.[78]

b) The African Union

In Africa, regional bodies have invested efforts in ensuring that data protection and privacy are prioritised by their Member States. For instance, in 2014 the African Union (AU) adopted the Convention on Cybersecurity and Personal Data Protection. In 2010, the Southern African Development Community (SADC) developed a model law on data protection which it adopted in 2013. Also, in 2010 the Economic Community of West African States (ECOWAS) adopted the Supplementary Act A/SA.1/01/10 on Personal Data Protection Within ECOWAS. The East African Community, in 2008, developed a Framework for Cyberlaws.[79] Notwithstanding these efforts, many countries on the continent are still grappling with enacting specific legislation to regulate the collection, control and processing of individuals' data.[80]

The African Union (AU) is a regional body consisting of the 55 member states within the African continent. It was established in 2002 as a successor to the Organisation of African Unity (OAU).[81] In 2014, the AU Assembly adopted the AU Convention on Cybersecurity and Personal Data Protection (AU Convention).[82]

The AU Convention's objective is setting the essential rules for establishing a credible digital environment (cyber space) and address the gaps affecting the regulation and legal recognition of

[78] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Article 3.
[79] CIPESA, 'Challenges and Prospects of the General Data Protection Regulation (GDPR) in Africa' (2018) <https://cipesa.org/?wpfb_dl=272> accessed 22 September 2019.
[80] ibid.
[81] African Union, 'About the African Union | African Union' <https://au.int/en/overview> accessed 15 April 2019.
[82] African Union Convention on Cyber Security and Personal Data Protection 2014 | African Union' <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed 15 April 2019.

electronic communications and electronic signature; as well as the absence of specific legal rules that protect consumers, intellectual property rights, personal data and information systems and privacy online.[83] The Convention aims to spur the development of national and sub-regional frameworks for cybersecurity and data protection on the continent as well as to harmonize the laws of African States on electronic commerce, data protection, cybersecurity governance and cybercrime control. The Convention also defines the objectives for the information society in Africa and seeks to strengthen existing ICT laws in Member States.[84] It also provides that each State party to the Convention shall establish a legal framework to strengthen the rights of protection of physical data.[85]

Part II of the AU Convention has provisions on protection of personal data. These provisions include the scope of application of the AU Convention with regard to personal data protection and preliminary personal data protection formalities,[86] and the institutional framework for the protection of personal data which stipulates that the state parties should have national personal data protection authorities.[87] Section 3 of Part II of the AU Convention stipulates the basic principles governing the processing of personal data such as:

- Principle of consent and legitimacy of personal data processing;
- Principle of lawfulness and fairness of personal data processing;
- Principle of purpose, relevance and storage of processed personal data;
- Principle of accuracy of personal data;
- Principle of transparency of personal data processing; and

[83] African Union Convention on Cybersecurity and Personal Data Protection 2014.
[84] ibid.
[85] ibid.
[86] ibid, Section 1.
[87] ibid, Section 2.

- Principle of confidentiality and security of personal data processing.[88]

Section 4 provides for data subject rights such as the right of information, right of access, right to object and the right of rectification or erasure.[89] Section 5 stipulates the obligations of personal data controllers which include confidentiality, storage and sustainability.[90]

By June 2019, only fourteen countries have signed the Convention and five have ratified it.[91] As a result, it is yet to come into effect in most countries, including Kenya which has not yet signed or ratified it, and has had no discernible impact on data protection standards on the continent.[92]

c) The East African Community

The East African Community (EAC) established a Task Force on Cyber-laws together with UNCTAD which had been providing legal advice and training to build awareness on policy and legal issues pertaining to e-commerce since 2007. A series of consultative Task Force meetings led to the Partner States discussing how to harmonize cyber laws.[93] The Task Force recommended that the process of developing a draft legal framework on cyber laws be divided into two phases In Phase 1 would cover electronic transactions, electronic signatures and authentication, cybercrime, consumer protection, data protection and privacy.[94]

On the topic of consumer protection, the Task Force recommended: "

[88] ibid, Section 3.
[89] ibid, Section 4.
[90] ibid, Section 5.
[91] African Union, 'Status List: African Union Convention on Cyber Security and Personal Data Protection' <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed 22 September 2019.
[92] African Union, 'African Union Convention on Cyber Security and Personal Data Protection | African Union' (n 173).
[93] United Nations, 'United Nations Conference on Trade and Development Harmonizing Cyberlaws and Regulations : The Experience of the East African Community'.
[94] 'UNCTAD | East African Community' <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-EastAfrican.aspx> accessed 15 April 2019.

- That the EAC Secretariat and Partner States give due consideration to consumer protection issues in cyberspace within a broader consumer protection framework, at both a national and regional level.
- That reforms should encompass information requirements, cancellation rights, payment fraud and performance obligations.
- That the EAC Secretariat and Partner States initiate programmes to raise consumer awareness about the benefits and risks of transacting in cyberspace, including such things as labelling schemes.
- That the EAC Secretariat and Partner States give further consideration to the regional and national implications of electronic money or digital cash and the need to develop an appropriate regulatory framework."[95]

With regard to data protection and privacy, the Task Force recommended that work needed to be done to ensure that the privacy of citizens is not eroded through the internet and that there was legislation and institutions to protect data taking into account international best practice in the area.[96] The implementation of the framework is currently in progress in EAC Partner States.[97]

3.2.3 National Initiatives on Data Protection: Kenya

Kenya does not currently have a generally applicable data protection law. A Data Protection Bill was tabled in Parliament in 2018 to establish a comprehensive data protection regime in Kenya.[98] The Bill has not yet passed. Once law, the Bill would give effect to Article 31 of the

[95] UNCTAD & EAC, 'Draft EAC Legal Framework for Cyberlaws' (2008) <http://hdl.handle.net/11671/1815> accessed 15 April 2019.
[96] ibid.
[97] UNCTAD, 'East African Community' (n 94).
[98] Daly & Inamdar, 'Review Of The Data Protection Bill 2018' (2018) <http://www.dalyinamdar.com/review-of-the-data-protection-bill-2018/> accessed 5 May 2019.

Constitution, which provides the right to privacy.[99] The Bill acknowledges that data protection is encompassed within the right to privacy. It provides for the legal framework for protection of a person's privacy in instances where personal information is collected, stored, used or processed by another person.[100] As of now it is unclear whether one of this bill will ultimately be passed.

However, there are various other legal sources that address data protection in Kenya, such as the Constitution of Kenya 2010, the Banking Act, the Capital Markets Act, the Credit Reference Bureau Regulations, the Access to Information Act, the Private Security Regulation Act, the Kenya Information and Communications (Consumer Protection) Regulations and the Consumer Protection Act 2012. [101]

Personal financial information is protected through confidentiality requirements under the Banking Act,[102] the Credit Reference Bureau Regulations[103] and Capital Markets Act[104]. Laws that require publication of data such as the Access to Information Act also have inbuilt mechanisms for protection of personal information.[105] The Private Security Regulation Act protects data collected during entry into buildings from being used for other purposes.[106]

The Kenya Information and Communications (Consumer Protection) Regulations, 2010 in particular were created to uphold consumer rights and entitlements in the ICT sector.[107] It is complemented by the Consumer Protection Act 2012 that provides for consumer protection regulations for all goods and services consumed in Kenya. Part IV of the Consumer Protection

[99] ibid.
[100] Data Protection Bill 2018 309.
[101] DLA Piper, 'Data Protection Laws of the World: Full Handbook'.
[102] Banking Act, Cap 488, Laws of Kenya, Section 31(2).
[103] Credit Reference Bureau Regulations, 2013, Section 26.
[104] Capital Markets Act, Cap 485A, Section 13 (2) and Section 13A (4).
[105] Access to Information Act, 2016, Section 6.
[106] Private Security Regulation Act, No. 13 of 2016, Laws of Kenya, Section 48 (3).
[107] Daly & Inamdar (n 98).

Act articulates rights and obligations related to specific consumer agreements, and goes on to recognize Internet agreements. This recognizes that while conventional transactions were entered into in the physical space, increasingly the novelty of agreements in the digital space continues to pose consumer protection challenges in Kenya.[108]

Courts have also weighed in on different aspects of the right to data privacy. After the 2010 Constitution was enacted, several petitions have been instituted on the grounds of breach to data privacy. For example, in the case of *Bernard Murage v Fineserve Africa Limited & 3 others* the petitioner instituted a petition on the basis that the decision to roll out the thin SIM technology was made in the absence of a data protection law in Kenya and as such there is an apparent fear of uncontrolled transmission of personal data to third parties without the consent of handset and Thin SIM owners which was in breach of data privacy. *[109]*

Furthermore, in April 2018, the High Court found that installation of a Device Management System (DMS) to access information on the International Mobile Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), Mobile Station Integrated Subscriber Directory number (MSISDN) and Call Data Records (CDRs) of subscribers with the objective of weeding out counterfeit phones would limit the right to privacy.[110]

[108] Consumer Protection Act 2012 1.
[109] Bernard Murage v Fineserve Africa Limited & 3 others [2015] eKLR.
[110] Kenya Human Rights Commission v Communications Authority of Kenya & 4 others [2018] eKLR.

3.3 Models of Data Protection

There are several models for data privacy protections around the world.[111] These models are used simultaneously in many countries. The countries that protect privacy the most have all the models working together to ensure that data is protected adequately. [112]

3.3.1 Comprehensive Model

This refers to having a general law governing the collection, use and dissemination of personal information by the public sector as well as private sector.[113] It is characterised by having an oversight body, which ensures compliance with the legislation.[114]

Many countries and jurisdictions currently have or are in the process of adopting comprehensive data protection laws which regulate the collection and management of personal information by both the government and private sector.[115] The best examples for this approach are the EU and Latin American countries.[116]

The GDPR is an example of the comprehensive model. It is a set of rules that unifies the data privacy laws across all EU countries. It also sets out a requirement for specific minimum standards of data protection in countries that will be receiving information from EU member

[111] David Banisar & Simon Davies, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments, 18 *J. Marshall Journal of Computer & Information Law* 1 (1999) accessed from http://repository.jmls.edu/jitpl/vol18/iss1/1 on 8th January 2019.
[112] Ibid.
[113] Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights Report : An International Survey of Privacy Laws and Development* (Electronic Privacy Information Center 2007).
[114] Ibid.
[115] CIPP Guide, 'Comparing the Co-Regulatory Model, Comprehensive Laws and the Sectoral Approach « CIPP Guide' <https://www.cippguide.org/2010/06/01/comparing-the-co-regulatory-model-comprehensive-laws-and-the-sectoral-approach/> accessed 22 September 2019.
[116] Luis Alberto Montezuma, 'The Case for a Hybrid Model on Data Protection/Privacy' (*IAPP*, 2018) <https://iapp.org/news/a/the-case-for-a-hybrid-model-on-data-protectionprivacy/> accessed 22 September 2019.

states. A supervisory authority is established within each EU member states to monitor the level of data protection.[117]

3.3.2 Sectoral model

The sectoral model sets data protection or data privacy rules and standards applicable to specific sectors or issues, taking account the features of each industry for example financial or health services, or the type of data collected.[118] Different regulatory agencies are responsible for the implementation and enforcement of regulations within its sectors.[119] Some countries, such as the United States, avoid enacting general data protection rules in favor of specific sectoral laws.[120] However, one of the limitations with this approach is that it requires that new legislation be introduced with each new technology so protections frequently lag behind.[121]

This model of data protection has existed even prior to the advent of the internet and e-commerce. Under this model, personal data is protected by binding professional codes of ethics. For example, advocate client privilege, bank-customer relationships and doctor patient confidentiality prevents sharing of personal data with a third party.[122] Similarly, media codes of ethics protects the personal information of sources, victims and minors details from being published while academic research anonymizes sensitive personal data.[123] Therefore, this model has been in place all over the world, including in Kenya, where the various codes of ethics for those relationships apply.

---

[117] *EU General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
[118] Montezuma (n 116).
[119] Ibid
[120] Electronic Privacy Information Center and Privacy International (n 113).
[121] Ibid
[122] Kenya ICT Action Network, 'Policy Brief: Data Protection in Kenya' (2018)
[123] Ibid.

3.3.3 Self-regulatory model

The self-regulatory model is a binding system by which participating companies and industry bodies establish codes of practice and engage in self-policing or choose to comply with guidelines or codes of practice set by third parties.[124] This model is non-legislative. However, its compliance is compulsory. [125] This model is normally administered and monitored by non-governmental associations or bodies representing categories of the organizations.[126] Companies like Cisco[127] and Google[128] have had their own self-regulation models through privacy policies. Google also offers "Do Not Track" options on its web browser-Google Chrome-that allow internet users to prevent the program from tracking their online activities.[129]

However, a universal lack of transparency by companies has rendered the market uninformed and thus an ineffective method of data protection. Users simply do not read the information given to them-usually through long and convoluted privacy policies-and thus are often unable to make informed choices about whom they can trust.[130] Furthermore, sometimes they do not adhere to these self-regulatory mechanisms. For instance, Google has disbanded its ethics

[124] Montezuma (n 116).
[125] Ibid.
[126] Ibid
[127] CISCO, 'Global Personal Data Protection & Privacy Policy - Cisco' <https://www.cisco.com/c/en/us/about/trust-center/data-protection-and-privacy-policy.html> accessed 22 September 2019.
[128] Google, 'Privacy Policy – Privacy & Terms' <https://policies.google.com/privacy?hl=en> accessed 22 September 2019.
[129] Google, 'Ads Preferences Manager, google.com,' https://www.google.com/settings/ads/ plugin accessed 22 September 2019
[130] John Schinasi, 'Practicing Privacy Online: Examining Data Protection Regulations Through Google's Global Expansion' (2014) 52 Columbia Journal of Transnational Law 569, 585 <http://jtl.columbia.edu/wp-content/uploads/sites/4/2014/05/52ColumJTransnatlL569_Practicing-Privacy-Online_Examining-Data-Protection-Regulations-Through-Googles-Global-Expansion.pdf> accessed 22 September 2019.

committees several times established with respect to some projects involving Artificial Intelligence (AI) and data collection.[131]

3.3.4 Co-regulatory model

The co-regulatory model combines both legislation and self-regulatory models in support of the regulation. The government and industry share responsibility for drafting and enforcing regulation.[132] Usually, the industry develops the rules for privacy protection while these rules are enforced by the industry and overseen by a state agency. This approach aims to involve individuals, organizations, industry associations and governments, within a legal framework.[133] One example of this approach is Canada.[134]

Elements of a co-regulatory data protection model include legislation establishing government regulations and incentives for compliance, a comprehensive set of data protection principles, as well as consequences for privacy violations; a government privacy protection agency with adequate jurisdiction to ensure compliance with privacy legislation; having self-regulatory watchdog agencies to help to enforce privacy legislation by providing expert consultation; negotiating and approving codes and standards; supervising compliance; imposing penalties on violators; researching new technologies; and providing a means to adapt the law in a practical context and the public which should be aware of the privacy legislation in place, privacy agencies, industry agencies and complaints processes.[135]

[131] John Leonard, 'Google Disbands Another AI Ethics Committee' (*Computing*, 2019) <https://www.computing.co.uk/ctg/news/3064293/ai-and-ml-latest-google-disbands-another-ai-ethics-committee> accessed 22 September 2019.
[132] Ibid
[133] CIPP Guide (n 115).
[134] Montezuma (n 116).
[135] CIPP Guide (n 115).

Canada's privacy protection framework offers a working example of a co-regulation model with the following elements:

a) Legislation

The fundamental right to privacy is protected in the Canadian Constitution, the Charter of Rights and Freedoms. At the federal level, the Canadian Privacy Act (1983) regulates 150 federal government departments regarding the collection, use and disclosure of personal information.[136] The Personal Information Protection and Electronic Documents Act (PIPEDA) is federal legislation which governs the use of electronic documents.[137]

b) Government Agency

Canada has a Privacy Commissioner who is a designated ombudsperson and officer of Parliament who can investigate complaints and violations of the Privacy Act or the PIPEDA. The Office of the Privacy Commissioner (OPC) investigates complaints, conducts audits, publishes information about personal data handling practices, researches privacy issues and promotes awareness and understanding of privacy issues.[138]

c) Watchdog Agencies

These are formed as self-regulatory mechanisms. There are several non-profit organizations formed to promote the right to privacy on the internet, to promote knowledge and understanding of privacy legislation and to research into consumer vulnerabilities such as the Public Interest

[136] Montezuma (n 116).
[137] ibid.
[138] ibid.

Advocacy Center (PIAC), the Canadian Access and Privacy Association (CAPA) and the Electronic Frontier Canada (EFC).[139]

d) Individuals

The Office of the Privacy Commissioner regularly encourages and organizes informal awareness-raising activities with the public.[140]

3.3.5 Privacy-enhancing technologies

With the development of commercially available technology-based systems, data protection has also moved into the hands of individual users. Privacy-enhancing technologies allow online users to protect the privacy of their personally identifiable information provided to certain services or applications.[141] This has further evolved in to the "Privacy by Design" principle which has been provided for in some current the data protection guidelines and regulations such as the GDPR.[142] Privacy by Design is an approach taken when creating new technologies and systems. Privacy is incorporated into the technology you are using and the systems by default.[143]

Privacy enhancing technologies have traditionally been limited to 'pseudonymisation tools' which are software and systems that allow individuals to withhold their true identity from those operating electronic systems or providing services through them, and only reveal it when

[139] ibid.
[140] ibid.
[141] Electronic Privacy Information Center (n.113)
[142] *EU General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
[143] Search Encrypt, '7 Principles of Privacy By Design,' < https://medium.com/searchencrypt/7-principles-of-privacy-by-design-8a0f16d1f9ce> accessed 21 April 2019

absolutely necessary.[144] These technologies help to minimise the information collected about individuals and include anonymous web browsers, specialist email services, and digital cash.[145]

Examples of privacy enhancing technologies include secure online access for individuals to their own personal data to check its accuracy and make amendments, software that allows browsers to automatically detect the privacy policy of websites and compares it to the preferences expressed by the user, highlighting any clashes; and contradictory electronic privacy policies that are attached to the information itself preventing it being used in any way that is not compatible with that policy, encryption tools to prevent unauthorized access to communications, files, and computers,[146] anonymous tools such as VPN that masks the IP address and personal information among others.[147]

3.4 The Link between Data Protection and Corporate Governance

Companies collect and utilize consumer personal information at unprecedented levels.[148] Large online platforms, such as Google and Facebook, have a lot of information about the everyday lives of billions of people around the globe.[149] However, online platforms are not the only companies that collect extensive personal data about consumers. Businesses in all industries e.g. the retail, travel, consumer goods, media, telecommunication, banking, and insurance sectors that sell consumer products or services have all been collecting, using, and partly also sharing,

[144] Data Protection Office, 'Privacy Enhancing Technologies: An Absolute Necessity for Effective Compliance with Data Protection Laws' (2012) <http://dataprotection.govmu.org/English/Documents/Publications/Guidelines/DPO_Vol7_EnhancingTechnology.pdf> accessed 22 September 2019.
[145] ibid.
[146] Steve Kenny, 'An Introduction to Privacy Enhancing Technologies' (*IAPP*, 2008) <https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/> accessed 22 September 2019.
[147] Data Protection Office (n 144).
[148] Wolfie Christl, Katharina Kopp and Patrick Urs Riechert, 'How Companies Use Personal Data Against People' (2017).
[149] Wolfie Christl, 'Corporate Surveillance In Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions' (2017) <http://crackedlabs.org/en/corporate-surveillance>.

information about prospects and customers for many years.[150]For example, retailers often have loyalty programs which has intensified the amount and detail of collected personal data well as companies' ability to make use of it and to trade it with other companies.[151] Online advertising also largely depends on tracking and profiling consumers, which involves the buying of prospective consumers personal data which has been shared with other companies.[152]

The increasing amount of data being processed and the more sophisticated analysis of data has resulted in widespread benefits for companies as well as individuals and societies.[153] This is done through creating more user-friendly consumer products and services, which now routinely customize themselves to users' specific tastes and needs through processing consumer data.[154] However, it also means that the risks to breach of data privacy rights are increasing. In this context, companies are meant to protect human rights, including the right to privacy.[155]

As discussed in the previous chapter, company directors are faced with a wide range of responsibilities arising from their board membership. The Companies Act provides that directors have a fiduciary duty to act in the best interests of the company in order to promote the success of the company for the benefit of its members as a whole.[156] In so doing the director shall have regard to, among other things, "the long term consequences of any decision of the directors; the interests of the employees of the company; the need to foster the company's business relationships with suppliers, customers and others; the impact of the operations of the company

[150] ibid.
[151] Christl, Kopp and Riechert (n 148).
[152] Christl (n 149).
[153] Global Partners Digital (n 71).
[154] ibid.
[155] ibid.
[156] The Companies Act No 17 of 2015 Laws of Kenya (2015) Section 143.

on the community and the environment; and the desirability of the company to maintain a reputation for high standards of business conduct."[157]

Furthermore, in exercising their powers they must act with reasonable skill, care and diligence that a reasonable person would exercise if they the general knowledge, skill and experience that the director has.[158] The requisite standard of care has been raised significantly over the years and continues to increase in line with contemporary community expectations.[159] Data privacy is one of the key issues on which directors must focus in order to execute their compliance and managerial oversight as well as mitigate risk.[160] Furthermore, Article 20(1) of the Constitution of Kenya provides that "The Bill of Rights applies to all law and binds all State organs and all persons." A corporation is a legal person as illustrated in the case of *Salomon V. Salomon and Co. Ltd* with a legal personality that is separate from its members.[161] This translates into corporations having duties towards the protection of human rights including the right to privacy. Corporations should then protect their consumer's right to privacy in several ways including ensuring that data protection laws and policies are implemented.

3.5 Conclusion

This chapter has surveyed data protection regulation, through international, regional and national initiatives. It has also looked at the various models of data protection applied in various parts of the world. It has also examined the link between corporate governance and data protection. The influx of using data by corporates has led to data protection laws being created. The next chapter discusses how data protection has been implemented by corporations in other jurisdictions. This

[157] ibid.
[158] ibid, Section 145.
[159] Ann Cavoukian, 'Privacy and Boards of Directors: What You Don't Know Can Hurt You (Revised)' <http://www.ipc.on.ca/images/Resources/director.pdf>.
[160] ibid.
[161] Salomon v A Salomon and Co Ltd [1897] AC22

shall be done by looking at the scope of data protection laws. It shall also look at how corporate governance practices have been affected by data protection regulations.

CHAPTER FOUR

AN ANALYSIS ON DATA PROTECTION AND DATA PRIVACY REGULATIONS IN THE EUROPEAN UNION

4.1 Introduction

At present there is no general data protection legislation in place in Kenya.[1] However, there is a growing awareness in the country that when personal information is processed, the interests of the persons whose information is involved, deserve protection. There is legislation currently being discussed in Parliament to deal with this issue.[2]

A Data Protection Bill was tabled in Parliament in 2012 and another one 2015. The Bills would give effect to Article 31 of the Constitution which provides for the right to privacy. It would also regulate the collection, retrieval, processing, storing, use and disclosure of personal data.[3] These Bills have not yet been passed.

Furthermore, in May 2018 the ICT Cabinet Secretary Joe Mucheru formed a taskforce to develop a Policy and Regulatory Framework for Privacy and Data Protection in Kenya.[4] The draft policy presents legislative proposals and recommendations for stakeholder consultation through a transparent process with the object of developing the draft policy and legislation for privacy and data protection.[5] Additionally, Data Protection Bill 2018 was presented before the Senate and

[1] DLA Piper, 'Data Protection Laws of the World: Full Handbook'.
[2] Privacy International, 'State of Privacy Kenya' <https://privacyinternational.org/state-privacy/1005/state-privacy-kenya#commssurveillance> accessed 19 May 2019.
[3] ibid.
[4] Ministry of Information Communications and Technology, 'Request for Comments on the Proposed Privacy and Data Protection Policy and Bill, 2018' <http://www.ict.go.ke/request-for-comments-on-the-proposed-privacy-and-data-protection-policy-and-bill-2018/> accessed 19 May 2019.
[5] ibid.

released for public debate and scrutiny. The legislation specifically addresses data collection, processing and storage.[6]

As discussed in the previous chapter, data protection laws date from the 1980s.[7] The emergence of the global market has led to an increase in the exchange of information across national boundaries resulting in data protection becoming an international issue.[8] International organizations such as OECD and the EU became involved and adopted documents dealing with data protection due to realizing the burden of multinational corporations in being expected to conform to differing standards of data protection in every country in which they processed or stored data.[9] Additionally, as discussed in Chapter 3, there are several models of regulation applied in various countries to ensure that data protection is applied in both the public and private sectors.

To understand the scope of data protection this chapter discusses how data protection has been implemented in corporations in other jurisdictions by looking at the scope of data protection laws. It also looks at how corporate governance practices have been affected by data protection regulations.

Since Kenya is yet to enact a data protection law therefore this chapter looks at the legislation in the European Union since the European Union has taken a firm stance on data protection.

[6] Data Protection Bill.
[7] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
[8] Anneliese Roos, 'Core Principles of Data Protection Law' (2006) 39 Comparative and International Law Journal of Southern Africa 103.
[9] ibid.

4.2 Data Protection in the European Union

On May 25, 2018, the GDPR[10] took legal effect in the European Union (EU) and the European Economic Area (EEA) which together comprises of 31 countries. The GDPR is a complex data protection law that was designed to harmonize data privacy laws across Europe, protect and empower all EU citizens data privacy and reshape the way organizations across the region approach data privacy.[11] GDPR is the replacement for the EU Data Protection Directive 95/46/EC of 1995.[12]

GDPR has enormous impacts on organizations in both Europe and around the world as it reshapes the way in which organizations manage data, as well as redefines the roles for key leaders in businesses. It changes the way organizations collect, use and share personal data.[13] There are many provisions that affect how organizations protect personal data which will be discussed below.

4.2.1 Definitions

Personal data is described in the GDPR as,

> "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical,*

[10] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[11] 'EUGDPR – Information Portal' <https://eugdpr.org/> accessed 24 May 2019.
[12] ibid.
[13] Edward S. Dove 'The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era.' (2018) The Journal of Law, Medicine & Ethics 46, no. 4, 1013–30. doi:10.1177/1073110518822003.

physiological, genetic, mental, economic, cultural or social identity of that natural person."[14]

This definition has a wide concept of personal data taking into consideration factors such as genetic and mental identity as well as the development of technology by providing for online identifiers such as IP addresses, cookies and RFID tags within the definition of personal data.[15]

The GDPR is concerned with the "processing" of personal data. Processing has been described as any operation which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure or destruction of the data.[16]

Personal data may be processed by either a "controller" or a "processor". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*". The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller.[17] The controller and processer may be natural or legal person, public authority, agency or other body This definition encompasses a company as a legal person.

[14] Article 4, General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[15] W Gregory Voss and Kimberly A Houser, 'Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies' (2019) 56 American Business Law Journal 287 <https://onlinelibrary.wiley.com/doi/abs/10.1111/ablj.12139>.
[16] Article 4, General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[17] ibid.

The "data subject" is a living, natural person whose personal data are processed by either a controller or a processor.[18]

4.2.2 Territorial scope

GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the EU or not.[19] The GDPR therefore has an extended jurisdiction as it applies to are to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location around the world.[20] Article 3 (2) of the GDPR also provides that it applies to the processing of personal data of data subjects in the EU by a company not established in the EU, where the activities relate to: offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU.[21] In this case, non-EU businesses processing the data of EU citizens also have to appoint a representative in the EU.[22]

4.2.3 Sanctions

GDPR has very high sanctions for non-compliance of the provisions of the regulations. Organizations in breach of GDPR or an order by the supervisory authority are subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.[23] This

[18] ibid.
[19] Ibid, Article 3.
[20] 'Key Changes with the General Data Protection Regulation – EUGDPR' <https://eugdpr.org/the-regulation/> accessed 24 May 2019.
[21] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[22] Ibid, Article 27.
[23] Ibid, Article 83 (6).

compounds the risk for multinational businesses as fines are imposed based on the revenues of an undertaking rather than the revenues of the relevant controller or processor which may be a subsidiary. Recital 150 of GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union.[24] However, in several cases such as *Skanska Industrial Solutions and Others*[25] group companies have been regarded as part of the same undertaking. This is will affect multinational companies as it means that in many cases group revenues will be taken into account when calculating fines, even where some of those group companies have nothing to do with the processing of data to which the fine relates provided they are deemed to be part of the same undertaking.

There is a tired approach to imposing fines which are split into two broad categories. The highest category of fines provided for under Article 83(5) of up to 20,000,000 Euros or up to 4% of total worldwide turnover of the preceding year in the case of an undertaking, whichever is higher apply to breach of:

i. the basic principles for processing including conditions for consent;
ii. data subjects' rights;
iii. international transfer restrictions;
iv. any obligations imposed by Member State law for special cases such as processing employee data;
v. certain orders of a supervisory authority.

[24] Ibid, Recital 150.
[25] Skanska Industrial Solutions and Others Case C-724/17.

The lower category of fines provided for under Article 83(4) of up to 10,000,000 Euros or in the case of an undertaking up to 2% of total worldwide turnover of the preceding year, whichever is the higher apply to breach of:

i. obligations of controllers and processors, including security and data breach notification obligations;
ii. obligations of certification bodies;
iii. obligations of a monitoring body.

These fines can be imposed in combination with other sanctions. Article 58 of the GDPR provides that supervisory authorities enjoy wide investigative and corrective powers including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities. [26]

GDPR also makes it easy for individuals to bring claims against data processors or controllers. Article 79 stipulates that data subjects enjoy the right to an effective legal remedy against a controller or processor.[27] Moreover, any person who has suffered "material or non-material damage" as a result of a breach of GDPR has the right to receive compensation from the controller or processor.[28] Non-material damage means that individuals will be able to claim compensation for distress and hurt feelings even where they are not able to prove financial loss.[29]

[26] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[27] ibid.
[28] Ibid, Article 82(1).
[29] DLA Piper (n 1).

Additionally, data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf.[30]

4.2.4 Consent

GDPR provides that where processing is based on consent, the controller should be able to demonstrate that the data subject has consented to processing of his or her personal data.[31] The request for consent must be given in an intelligible and easily accessible form, using clear and plain language, with the purpose for data processing attached to that consent. The data subject also has the right to withdraw consent at any time and it must be as easy to withdraw consent as it is to give it.[32] This strengthens the conditions for consent and companies are no longer able to use long illegible terms and conditions full of legalese to justify the consumers giving of consent.

4.2.5 Individual Rights

GDPR has enhanced rights enjoyed by individuals backed up with provisions making it easier to claim damages for compensation and for consumer groups to enforce rights on behalf of consumers. These rights include:

i) Transparency

ii) Right to Access

iii) Right to Rectification

iv) Right to be Forgotten

v) Right to Restriction of Processing

vi) Right to Data Portability

[30] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Article 80.

[31] ibid, Article 7.

[32] 'Key Changes with the General Data Protection Regulation – EUGDPR' (n 20).

vii) Right to Object

i) Transparency

Article 12 stipulates that various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language.[33] The following information must be provided at the time the data is obtained[34]:

i. the identity and contact details of the controller;
ii. the Data Protection Officer's contact details;
iii. the purpose for which data will be processed and the legal basis for processing;
iv. the recipients or categories of recipients of the personal data;
v. details of international transfers;
vi. the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
vii. the existence of rights of the data subject including the right to access, rectify, require erasure (the "right to be forgotten"), restrict processing, object to processing and data portability; where applicable the right to withdraw consent and the right to complain to supervisory authorities;
viii. the consequences of failing to provide data necessary to enter into a contract;
ix. the existence of any automated decision making and profiling and the consequences for the data subject.

Additionally, if a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.[35]

[33] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[34] ibid, Article 13(1).

ii) Right to Access

Data subjects have the right to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This information must be provided within one month with a limited right for the controller to extend this period for up to three months.[36]

iii) Right to Rectification

Article 16 provides for the right for data subjects to have their inaccurate personal data about themselves rectified or completed if incomplete including by means of providing a supplementary statement. This should be done without any undue delay.[37]

iv) Right to be Forgotten

The right to be forgotten entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.[38] This is also known as the right to Data Erasure. This right had been delved into before the GDPR came into effect in the case of *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*[39] when the court ruled against Google requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

---

[35]ibid, Article 13(2.
[36]ibid, Article 15.
[37] bid, Article 16.
[38]ibid, Article 17.
[39] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González Case C-131/12

The impact of this decision on companies is that there have been an increased number of requests made to search engines for search results to be removed.[40]

v) Right to Restriction of Processing

GDPR provides the right of data subjects to request the restriction or suppression of personal data from being processed. In this case, the data is not destroyed but cannot be used.[41] This right can be obtained if:

- the accuracy of the personal data is being contested by the data subject;[42]
- the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use;[43]
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the exercise or defence of legal claims;[44]
- the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.[45]

vi) Right to Data Portability

GDPR introduces the right to data portability under Article 20 which has not been provided for under any other previous laws.[46] This is the right for a data subject to receive the personal data

[40] DLA Piper (n 1).
[41] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Article 18.
[42] Ibid, Article 18(1)(a).
[43] Ibid, Article 18(1)(b).
[44] Ibid, Article 18(1)(c).
[45] Ibid, Article 18(1)(d).

concerning them – which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller.[47]

vii) Right to Object

GDPR provides for the right of data subjects to object to the processing of their personal data at any time in certain circumstances, including if processing is necessary for the performance of a task carried out in the public interest, if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party or for direct marketing.[48]

viii) Right against automated profiling

Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. This right allows data subjects to ask to be excluded from such processes.[49]

4.2.6 Privacy by Design and by Default

Privacy by design is now a legal requirement with the GDPR under Article 25.[50] The GDPR also introduces the concept of privacy by default. This means that by default, companies should ensure that personal data is processed with the highest privacy protection (for example only the

[46] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[47] 'Key Changes with the General Data Protection Regulation – EUGDPR' (n 20).
[48] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Article 21.
[49] Ibid, Article 22.
[50] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

data necessary should be processed, short storage period, limited accessibility) so that by default personal data is not made accessible to an indefinite number of persons.[51]

Privacy by design means data protection through technology design.[52] It calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.[53] More specifically, 'The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.'

4.2.7 Breach Notification

Under the GDPR, it is mandatory to notify the supervisory authority of a personal data breach where a data breach is likely to "result in a risk for the rights and freedoms of individuals".[54] This must be done within 72 hours of first having become aware of the breach. Data processors are also required to notify their customers and the controllers of a personal data breach after first becoming aware of a data breach without any undue delay.[55]

[51] European Commission, 'What does data protection 'by design' and 'by default' mean?" <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en> accessed 23 September 2019
[52] 'Privacy by Design | General Data Protection Regulation (GDPR)' <https://gdpr-info.eu/issues/privacy-by-design/> accessed 15 May 2019.
[53] ibid.
[54] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, Article 33.
[55] 'Key Changes with the General Data Protection Regulation – EUGDPR' <https://eugdpr.org/the-regulation/> accessed 19 May 2019.

4.2.7 Data Protection Officers

The GDPR stipulates that there should be an internal requirement of record keeping, with a mandatory of appointing Data Protection Officers (DPOs) for public authorities, controllers or processors whose core activities consist of processing operations which by virtue of their nature, scope or purposes require regular and systemic monitoring of data subjects on a large scale and controllers or processors whose core activities consist of processing sensitive personal data on a large scale.[56] DPOs must have "expert knowledge" of data protection law and practices though it is possible to outsource the DPO role to a service provider.[57] This is a governance burden for those organizations which are caught by the requirement to appoint a DPO.

4.2.8 Data Protection Principles

The GDPR sets out several principles relating to processing of personal data under Article 5.[58] These are:

i) the lawfulness, fairness and transparency principle: personal data must be processed lawfully, fairly and in a transparent manner;
ii) the purpose limitation principle: personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
iii) the data minimization principle: the data must be adequate, relevant and limited to what is necessary in relation to the purposes;
iv) the accuracy principle: the data must be accurate and kept up-to-date;

[56] Article 37, General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[57] Article 37(5), ibid.
[58] ibid.

v) the storage limitation principle: the data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the data are processed;

vi) the integrity and confidentiality principle: personal data must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures.

The GDPR also includes the accountability principle whereby the controller is responsible for making sure all the above privacy principles are adhered to. An organization also needs to demonstrate compliance and accountability with all the principles. [59]

4.3 The impact of the GDPR on Corporate Governance

Catalin Grigorescu argues that the GDPR is mainly about corporate governance of a company rather than security.[60] The protection of consumer personal data is one of the significant concerns facing companies all over the world. In case a security breach occurs and personal data is lost or put at risk, it would have a big reputational and financial impact on businesses, hence companies need to worry about data protection.[61] It is therefore noteworthy that the GDPR affects corporate governance of companies around the world in many ways.

[59] DLA Piper (n 1).
[60] Catalin Grigorescu, 'GDPR Is Mainly about Corporate Governance' <https://www.linkedin.com/pulse/gdpr-mainly-corporate-governance-catalin-grigorescu> accessed 19 May 2019.
[61] ibid.

First, as illustrated previously, the GDPR has global reach in that it also applies to organizations that are not established within the EU or EEA when they process personal data of individuals who are in the EU or EEA.[62]

Furthermore, the GPDR introduces heightened requirements on companies which brings about many challenges for legal and compliance functions to manage, and, in the case of failure or non-compliance, directors may be held personally liable for damages.[63] What's more, the supervisory authority has the power to impose fines of up to 20 million Euros or 4 percent of annual global turnover. The GDPR also creates the potential for increased invasive investigations, and grants supervisory authorities extensive powers and responsibilities, which include broad investigative and corrective powers.[64]

In addition, as noted in a study by Deloitte, the compliance to the GDPR is a key area of risk for organizations.[65] Organizations need to identify the current and emerging risks associated with data privacy and the rights of data subjects as well as demonstrate they have risk management solutions in place in order to ensure compliance with the GDPR.[66]

It is the boards responsibility to implement a robust corporate governance framework, which should include an enterprise risk management framework.[67] The audit or risk committee within the board should therefore consider the risks and requirements under the GDPR together with the IT committee, if any, or IT personnel to identify, monitor and improve any gaps in the risk

[62] Article 3, General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[63] Nicholas J Price, 'UK Corporate Governance and the GDPR' (*Diligent*, 2018) <https://diligent.com/en-gb/blog/uk-corporate-governance-general-data-protection-regulation-gdpr/> accessed 19 May 2019.
[64] ibid.
[65] Deloitte, 'Building Trust: 2017 Planning Priorities for Internal Audit in Financial Services'.
[66] Robert L Ford, 'The Impacts of the GDPR on Corporate Governance Practices in the GCC'.
[67] ibid.

management for data and information storage, processing and control.[68] The GDPR provides guidance on how organizations can implement risk impact assessments for projects which involve personal data and information of individuals, especially for EU citizens.[69] If a board or the management of a company that is responsible of defining a company's risk management framework ignores GDPR compliance as a board matter, then they might be in breach of their fiduciary duty to the company.

The appointment of a DPO at the board level is another important requirement stipulated within the GDPR. As Price notes, this would present a challenge to many organizations as such skills and experience cannot be found easily.[70]

The GDPR also brings about increased accountability and transparency for corporate governance at the board level. As pointed out by Price, "The principle of accountability provides an opportunity for organizations to bolster individuals' trust in them by showcasing their robust data protection efforts and for demonstrating transparency and corporate responsibility. Responsible information handling practices can attract customers, investors, and talent."[71]

4.4 Conclusion

This chapter has focused on the GDPR as a data protection law and how it has impacted corporate governance of companies within the EU and worldwide. The best practices discussed in this chapter as well as the previous chapters shall be discussed as recommendations in the next chapter.

---

[68] ibid.
[69] Article 35, General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[70] Price (n 315).
[71] ibid.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Review of the Study

This study has looked at the various aspects of data privacy and data protection and analyzed the need for better corporate governance in the age of big data and the role of corporate governance to ensure that the consumers' data privacy is protected. The study focuses on the fact that many companies all over the world including Kenya collect, store and process the data of their consumers. This data has been described severally as an asset and therefore the paper has emphasized the need to protect consumer data. The paper has also focused on what Kenya can do to close the gap of not having a comprehensive data protection regulation.

The study has rotated around three questions namely whether a board of directors of a corporation possess a duty under Kenya company law to ensure that consumer data remains protected, what role corporations have in ensuring protection of consumer data and how corporate governance is affected by data protection laws and policies in the EU.

Whether a board of directors of a corporation possess a duty under Kenya company law to ensure that consumer data remains protected was considered by delving into the duties of the directors under the Companies Act as well as various codes of corporate governance in Kenya. It was established that consumer data protection is one of the key issues on which directors must focus in order to execute their compliance and managerial oversight as well as mitigate risk and therefore it the directors fiduciary duty as well as their duty of skill and care to ensure that consumer data is protected. Organizations can therefore help to protect the individual's right to privacy in several ways such as implementing data protection laws as well as through good

corporate governance practices. The study ascertained that data protection can be applied into corporate governance mechanisms in Kenya in the absence of a comprehensive data protection law through the incorporation of data protection into corporate governance mechanisms.

The role of corporations in ensuring consumer data protection was discussed through the lenses of the development of consumer data protection and data privacy laws and their implementation in corporations. The historical background of data protection and data privacy regulations and policy by looking at the historical development of data collection and processing. as well as consumer protection regulations. The chapter then looked at the development of international initiatives to ensure that the right to privacy which then cascaded into different regimes of data protection regulations regionally and nationally. It then looked at the data protection models applied in different countries in the world. It then examined the link between corporate governance and data protection in order to illustrate the data problem. The aim of this chapter was to derive lessons the various ways data protection can be achieved.

The study then investigated how is corporate governance affected by data protection laws and policies in the EU. Since Kenya is yet to enact a data protection law it examined the GDPR since the European Union has taken a firm stance on data protection. A look at the provisions of the GDPR that are applicable to companies such as the definitions, how the territorial scope of the GDPR goes beyond the boundaries of the EU, sanctions within the GDPR, the rights provided for under the GDPR as well as data protection principles illustrated the legal requirements of a corporation in the EU as well as corporations all over the world to ensure consumer data is protected. It also established that corporate governance practices have been affected by the GDPR by introducing heightened requirements on corporations and in the case of failure or non-compliance, directors may be held personally liable for damages

The study has established that although companies in Kenya collect and process the personal data of their consumers, Kenya does not have an adequate comprehensive legal framework to ensure that the privacy of these consumers has been protected. Chapter two looks at how data protection is a corporate governance issue. This is important in order to emphasize that companies should come up with data protection policies in order to protect their consumers' data.

Chapter three then delved into the historical development of data protection. From this, it can be seen that there are several international initiatives such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data that have global effects due to providing for the right to data privacy. Additionally, the EAC also has their own initiative to develop cyber laws that will touch on data protection and privacy. [1] Additionally, though Kenya does not have a comprehensive data protection regulation, there are various other legal sources that address data protection in Kenya, including the Constitution of Kenya 2010, the Banking Act, the Capital Markets Act, the Credit Reference Bureau Regulations, the Access to Information Act, the Private Security Regulation Act, the Kenya Information and Communications (Consumer Protection) Regulations and the Consumer Protection Act 2012 as well as case law that has addressed consumer data protection. [2] Furthermore, Kenya can look at the various models that have been applied around the world and find one that is fitting for it, such as applying a self-regulatory model in the absence of a data protection law.

[1] UNCTAD & EAC, 'Draft EAC Legal Framework for Cyberlaws' (2008) <http://hdl.handle.net/11671/1815> accessed 15 April 2019.
[2] DLA Piper, 'Data Protection Laws of the World: Full Handbook'.

Chapter four focuses on an analysis of the GDPR. From these, Kenya can look at the principles provided within the regulation and how it affects corporates. It is opined that these principles can be applied in coming up with company policies on data privacy.

5.2 Recommendations

The study has established that by October 2019 there is no general data protection legislation in place in Kenya.[3] However, there is a growing awareness in the country that when personal information is processed, the interests of the persons whose information is involved, deserve protection. There is legislation currently being discussed in Parliament to deal with this issue.[4] However, it opines that data protection can be looked at as a corporate governance issue as data breaches affects companies reputation as consumers will lose trust in the company and may also lead to a financial loss.[5] In light of these, there is a comprehensive corporate governance framework with corporate board directors having a wide array of duties to the company and its stakeholders arising by virtue of their board membership. These include a fiduciary duty to act in the best interests of the corporation and a duty to maintain the standard of care.[6] Board directors should therefore implement several things to ensure that their consumers privacy is protected:

Directors should ensure that they have enough up-to-date knowledge about best privacy practices is current and up-to-date.[7] Since the Board members have a fiduciary duty to act in the best interest of the organization they need to be knowledgeable on data privacy and protection in order to apply the right policies. The board can do this through recruiting directors with skills

[3] ibid.
[4] Privacy International, 'State of Privacy Kenya' <https://privacyinternational.org/state-privacy/1005/state-privacy-kenya#commssurveillance> accessed 19 May 2019.
[5] Claire Lending, Kristina Minnick and Patrick J Schorno, 'Corporate Governance, Social Responsibility, and Data Breaches' (2018) 53 Financial Review 413.
[6] OECD Principles of Corporate Governance.
[7] Ann Cavoukian, 'Privacy and Boards of Directors: What You Don't Know Can Hurt You (Revised)' <http://www.ipc.on.ca/images/Resources/director.pdf>.

and experience on data privacy and data protection or enhancing their skills on data privacy through continuous board development. There also needs to be an emphasis on how data breaches can affect a company. For example, the board could invite privacy experts or organize a privacy workshop for directors and senior officers of their organizations.[8]

It has been shown that accountability and transparency are some of the main principles that affect both corporate governance and data protection. The Board can therefore demonstrate accountability through the appointment of a member of senior management whose responsibilities include privacy or whose primary responsibility is data privacy.[9] This can be done through appointing a data protection officer (DPO) such as the one that has been provided for in within the GDPR.[10] The DPO can be the organization's resident privacy expert. The DPO must be given the authority to oversee the design, implementation, monitoring and reporting on the organization's privacy policies and to ensure that there are company privacy controls to protect the privacy of consumers data.[11]

The Board of directors can also apply data governance mechanisms within the company. As discussed in chapter four this refers to the overall management of the availability, usability, integrity, and security of the data used in an organization.[12] Through this, the Board can ensure that there is proper management of data risks and security and making strategical decisions on the data that the company holds.

[8] ibid.

[9] Malcom Crompton, *Privacy Governance: A Guide to Privacy Risk and Opportunity for Directors and Boards,* (2014 Australian Institute of Company Directors).

[10] General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[11] Crompton (n 9).

[12] Zhang Ning and Qin JianYuan, 'An Overview of Data Governance' [2018] Valuing Data 9.

The Board can also apply data protection measures as a CSR policy. As discussed above, companies can successfully leverage the benefits of big data while at the same time limiting risks to privacy, but this can only be done effectively at the company level. Sound CSR policy can allow for data processing in a responsible and sustainable way, furthering the potential of data to improve human existence. This may also work to gain the trust of consumers.[13]

[13] Paolo Balboni, 'Data Protection as a Corporate Social Responsibility' (2018) Paolo Balboni | ICT, Policy and Data Science < https://www.paolobalboni.eu/index.php/2018/05/21/data-protection-as-a-corporate-social-responsibility/> accessed 13 September 2019.

BIBLIOGRAPHY

Books

Cadbury A, in Claessens S, *Corporate Governance and Development,* (2003, Washington DC: Global Corporate Governance Forum

Cristl W and Speikermann S, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy*, (2016, Wien)

Crompton M, *Privacy Governance: A Guide to Privacy Risk and Opportunity for Directors and Boards,* (2014 Australian Institute of Company Directors)

DLA Piper, *Data Protection Laws of the World: Full Handbook* (2019)

Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights Report : An International Survey of Privacy Laws and Development* (2007 Electronic Privacy Information Center).

Freeman R E and Others, *Stakeholder Theory: The State of the Art,* (2010 Cambridge University Press)

Iskander MR and Chamlou N, *Corporate Governance: A Framework for Implementation Public* (2000)

Lyon D, 'Surveillance, Power and Everyday Life' in Chrisanthi Avgerou and Others, *The Oxford Handbook of Information and Communication Technologies* (2009).

Michael M G and Michael K, *Uberveillance and the social implications of microchip implants : emerging technologies,* (2014 Hershey), PA

Smallwood R, 'Information Governance, IT Governance, Data Governance: What's the Difference? - Information Governance: Concepts, Strategies, and Best Practices [Book]', *Information Governance: Concepts, Strategies, and Best Practices* (John Wiley & Sons 2016)

Tricker R, *Corporate Governance: Principles, Policies, and Practices* (Oxford University Press 2015)

Journal Articles

Acquisti A, John L. K and Loewenstein G, 'What Is Privacy Worth?', (2013), 42 The Journal of Legal Studies, 2 249.

Alhassan I, Sammon D and Daly M, 'Data Governance Activities: An Analysis of the Literature' (2016) 25 Journal of Decision Systems 64

Azgad-Tromer S, 'The Case for Consumer-Oriented Corporate Governance, Accountability and Disclosure' 17 University of Pennsylvannia Journal of Business Law 227

Bamberger K A and Mulligan D K, 'Privacy in Europe: Initial Data on Governance Choices and Corporate Practices', (2013) 81 George Washington Law Review 1529

Banisar D and Davies S, 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments,' (1999) 18 J. Marshall Journal of Computer & Information Law 1

Carroll A.B, 'A Three-Dimensional Conceptual Model of Corporate Performance,' (1979) 4 The Academy of Management Review, 4, 497.

Christl W, Kopp K and Riechert PU, 'How Companies Use Personal Data Against People' (2017) Cracked Labs

Christl W, 'Corporate Surveillance In Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions' (2017) Cracked Labs http://crackedlabs.org/en/corporate-surveillance

Dhir A A, 'Realigning the Corporate Building Blocks: Shareholder Proposals as a Vehicle for Achieving Corporate Social and Human Rights Accountability,' (2006) 43 American Business Law Journal 2

Donaldson T and Preston LE, 'The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications' (1995) 20 The Academy of Management Review 65

Griffith SJ, 'Corporate Governance in an Era of Compliance' (2016) 57 William & Mary Law

Review 2075

Heath J and Norman W, 'Stakeholder Theory, Corporate Governance and Public Management: What Can the History of State-Run Enterprises Teach Us in the Post-Enron Era?' (2004) Journal of Business Ethics 53, 3 247-65 <http://www.jstor.org/stable/25123300> accessed 6 January 2019

Helveston M N, 'Consumer Protection in the Age of Big Data', (2016) 93 Washington University Law Review 859

Korac-Kakabadse N, Kakabadse A K and Kouzmin A, 'Board governance and company performance: any correlations?', (2001) Corporate Governance: The international journal of business in society, 1: 1,24, https://doi.org/10.1108/EUM0000000005457 accessed 4th February 2019

Landes X, 'How Fair Is Actuarial Fairness?' (2015) 128 Journal of Business Ethics 519 <https://curis.ku.dk/ws/files/136684188/Landes_Actuarial_Fairness.pdf> accessed 21 September 2019

Lending C, Minnick K and Schorno PJ, 'Corporate Governance, Social Responsibility, and Data Breaches' (2018) 53 Financial Review 413

Lehuedé HJ, 'Corporate Governance and Data Protection in Latin America and the Caribbean' (2019) <https://repositorio.cepal.org/bitstream/handle/11362/44629/1/S1900395_en.pdf> accessed 21 September 2019

Lieberman M.B and Montgomer D.B, 'First-Mover Advantages' (1988) 9 Strategic Management Journal 41 accessed www.jstor.org/stable/2486211 on 13 November 2019.

Ludington S, 'Reining in the Data Traders: A Tort for the Misuse of Personal Information,' (2006) 66 Maryland Law Review, 86

Pollach I, 'Online Privacy as a Corporate Social Responsibility: An Empirical Study' (2011) 20 Business Ethics 88

Paas D, ‘Stakeholders and Participation in Corporate Governance: A Critique of Some of the Arguments’ (1996) 15 Business & Professional Ethics Journal 3 <https://about.jstor.org/terms> accessed 8 June 2019

Purtova N, ‘Property in Personal Data: A European Perspective on Instrumentalist Theory of Propertization’ (2010) Research Policy <https://core.ac.uk/download/pdf/45678038.pdf> accessed 21 September 2019.

Roos A, ‘Core Principles of Data Protection Law’ (2006) 39 Comparative and International Law Journal of Southern Africa 103

Scassa T, ‘Data Governance in the Digital Age; Considerations for Canada’s National Data Strategy’ Data Governance in the Digital Age (2018) Centre for International Governance Innovation <www.cigionline.org> accessed 5 January 2019.

Schinasi J, ‘Practicing Privacy Online: Examining Data Protection Regulations Through Google’s Global Expansion’ (2014) 52 Columbia Journal of Transnational Law 569

Shlomit Azgad-Tromer, ‘The Case for Consumer-Oriented Corporate Governance, Accountability and Disclosure’ 17 University of Pennsylvannia Journal of Business Law 227

Spiekermann-Hoff S and Novotny A, ‘A Vision for Global Privacy Bridges: Technical and Legal Measures for International Data Markets’ (2015) 31 Computer Law and Security Review 181

Spiekermann S and Korunovska J, ‘Towards a value theory for personal data,*’* (2017) 32 Journal of Information Technology, 62.

Verhulst S G, ‘Corporate Social Responsibility for a Data Age,’ (2017*)* Stanford Social Innovation Review <https://ssir.org/articles/entry/corporate_social_responsibility_for_a_data_age> accessed 8 January 2019

Voss WG and Houser KA, ‘Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies’ (2019) 56 American Business Law Journal 287

Online Articles and Websites

African Union 'About the African Union' <https://au.int/en/overview> accessed 15 April 2019

Balboni P, 'Data Protection as a Corporate Social Responsibility' (2018) Paolo Balboni | ICT, Policy and Data Science < https://www.paolobalboni.eu/index.php/2018/05/21/data-protection-as-a-corporate-social-responsibility/> accessed 13 November 2019

Bonatti P and others, 'Transparent Personal Data Processing: The Road Ahead' <https://www.specialprivacy.eu/images/documents/TELERISE17.pdf> accessed 8 June 2019

Cannon JC, 'Privacy Governance: A Guide to Privacy Risk and Opportunity for Directors and Boards', The Privacy Advisor-IAPP https://iapp.org/news/a/book-review-privacy-governance-a-guide-to-privacy-risk-and-opportunity-for/ accessed 7 January 2019

CNIL, 'Personal Data: definition' https://www.cnil.fr/en/personal-data-definition accessed 11 December 2018

Cavoukian A, 'Privacy and Boards of Directors: What You Don't Know Can Hurt You (Revised)' <http://www.ipc.on.ca/images/Resources/director.pdf>

Chalasani A, 'Data Principal and Data Fiduciary in the Personal Data Protection Bill, 2018' (*Lakshmikumaran & Sridharan*) <https://www.lakshmisri.com/News-and-Publications/Publications/Articles/Corporate/data-principal-and-data-fiduciary-in-the-personal-data-protection-bill-2018> accessed 24 September 2019

CIPESA, 'Challenges and Prospects of the General Data Protection Regulation (GDPR) in Africa' (2018) <https://cipesa.org/?wpfb_dl=272> accessed 22 September 2019

CIPP Guide, 'Comparing the Co-Regulatory Model, Comprehensive Laws and the Sectoral Approach « CIPP Guide' <https://www.cippguide.org/2010/06/01/comparing-the-co-regulatory-model-comprehensive-laws-and-the-sectoral-approach/> accessed 22 September 2019

CISCO, 'Global Personal Data Protection & Privacy Policy - Cisco' <https://www.cisco.com/c/en/us/about/trust-center/data-protection-and-privacy-policy.html>

accessed 22 September 2019

Compliance Experts 'Facebook, Global Data, and Corporate Governance Deficiencies' (2018) <http://complianceexperts.com/2018/06/05/facebook-global-data-corporate-governance-deficiencies/> accessed 11 December 2018

Consumers International, 'The State of Data Protection Rules around the World: A Briefing for Consumer Organizations' <https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf>

Corplaw 'Shareholder & Stakeholder Theories Of Corporate Governance', (2013) <http://www.corplaw.ie/blog/bid/317212/Shareholder-Stakeholder-Theories-Of-Corporate-Governance> accessed 6th January 2019

'Cyber Risk and Directors' Liabilities: An International Perspective' (*Norton Rose Fulbright*) <https://www.nortonrosefulbright.com/en/knowledge/publications/b0dae4a0/cyber-risk-and-directors-liabilities-an-international-perspective> accessed 24 September 2019

Daly & Inamdar, 'Review Of The Data Protection Bill 2018' (2018) <http://www.dalyinamdar.com/review-of-the-data-protection-bill-2018/> accessed 5 May 2019

Data Protection Office, 'Privacy Enhancing Technologies: An Absolute Necessity for Effective Compliance with Data Protection Laws' (2012) <http://dataprotection.govmu.org/English/Documents/Publications/Guidelines/DPO_Vol7_EnhancingTechnology.pdf> accessed 22 September 2019

Davis H, 'Ted Cruz Campaign Using Firm That Harvested Data on Millions of Unwitting Facebook Users | US News | The Guardian' *The Guardian* (2015) <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data> accessed 9 June 2019

Dempsey JX, Cate FH and Abrams M, 'Organizational Accountability , Government Use of Private- Sector Data , National Security , and Individual Privacy'

'EUGDPR – Information Portal' <https://eugdpr.org/> accessed 24 May 2019

Ford RL, ‘The Impacts of the GDPR on Corporate Governance Practices in the GCC’ Lexis Nexis

Gikera SN, Vadgama P and Muringo N, ‘Kenya Corporate Governance’ (*Getting The Deal Through*, 2019) <https://gettingthedealthrough.com/area/8/jurisdiction/44/corporate-governance-kenya/> accessed 24 September 2019

Google, ‘Privacy Policy – Privacy & Terms’ <https://policies.google.com/privacy?hl=en> accessed 22 September 2019

Gordon A, ‘Can advanced analytics help organizations make the transition to a new era of data privacy and protection?’, (2018) https://www.ey.com/en_gl/trust/gdpr-compliance-how-data-analytics-can-help accessed 6 January 2019.

Grigorescu C, ‘GDPR Is Mainly about Corporate Governance’ <https://www.linkedin.com/pulse/gdpr-mainly-corporate-governance-catalin-grigorescu> accessed 19 May 2019

Haupt M, ‘“Data is the New Oil”—A Ludicrous Proposition’ (2016) Project 2030 <https://medium.com/project-2030/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294> accessed 5 January 2019

‘International Conference of Data Protection and Privacy Commissioners’ <https://icdppc.org/> accessed 1 May 2019

Kenny S, ‘An Introduction to Privacy Enhancing Technologies’ (*IAPP*, 2008) <https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/> accessed 22 September 2019

Kenya ICT Action Network, ‘Policy Brief: Data Protection in Kenya’ (2018) <https://www.apc.org/sites/default/files/Data_protection_in_Kenya_1.pdf> accessed 22 September 2019

EUGDPR ‘Key Changes with the General Data Protection Regulation’ <https://eugdpr.org/the-regulation/> accessed 24 May 2019

Kozlowska I, ‘Facebook and Data Privacy in the Age of Cambridge Analytica’ (2018, University of Washington) <https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/> accessed 9 June 2019

Leonard J, ‘Google Disbands Another AI Ethics Committee’ (*Computing*, 2019) <https://www.computing.co.uk/ctg/news/3064293/ai-and-ml-latest-google-disbands-another-ai-ethics-committee> accessed 22 September 2019

Medhora R, ‘Data Governance in the Digital Age’ Data Governance in the Digital Age (2018) Centre for International Governance Innovation 2 <www.cigionline.org> accessed 5 January 2019.

Martorana B, ‘Yahoo! Data Breach Results in Another Lawsuit Against Corporate Directors and Officers,’ (2017) S & W Cybersecurity and Data Privacy Blog <http://www.swlaw.com/blog/data-security/2017/01/31/yahoo-data-breach-results-in-another-lawsuit-against-corporate-directors-and-officers/> accessed 6 January 2019

Montezuma LA, ‘The Case for a Hybrid Model on Data Protection/Privacy’ (*IAPP*, 2018) <https://iapp.org/news/a/the-case-for-a-hybrid-model-on-data-protectionprivacy/> accessed 22 September 2019

‘Montreux Declaration: The Protection of Personal Data and Privacy in a Globalized World: A Universal Right Respecting Diversities’ (2005) <www.datenschutz-berlin.de/doc/intAwednUtc> accessed 14 April 2019

Nadeau M, ‘General Data Protection Regulation (GDPR): What you need to know to stay compliant,’ <https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html> accessed 4 December 2018

Ndemo B, ‘How Kenya Became the Cradle of Africa’s Technological Innovation,’ Newsweek, (2016) <https://www.newsweek.com/how-kenya-became-cradle-africas-ict-innovation-534694> accessed 6 January 2019

Ning Z and JianYuan Q, ‘An Overview of Data Governance’ (2018) Valuing Data

OECD ‘About the OECD’ <http://www.oecd.org/about/> accessed 30 April 2019

Petkoski D and Twose N, ‘Public Policy for Corporate Social Responsibility’ (2005) <http://web.worldbank.org/archive/website01006/WEB/IMAGES/PUBLICPO.PDF> accessed 8 June 2019

Price NJ, ‘The Correlation Between Corporate Governance and Compliance’ (*Diligent Insights*, 2018) <https://insights.diligent.com/entity-governance/the-correlation-between-corporate-governance-and-compliance/> accessed 9 June 2019

Price NJ, ‘UK Corporate Governance and the GDPR’ (*Diligent*, 2018) <https://diligent.com/en-gb/blog/uk-corporate-governance-general-data-protection-regulation-gdpr/> accessed 19 May 2019

GDPR ‘Privacy by Design, General Data Protection Regulation (GDPR)’ <https://gdpr-info.eu/issues/privacy-by-design/> accessed 15 May 2019

Privacy International, ‘State of Privacy Kenya’ <https://privacyinternational.org/state-privacy/1005/state-privacy-kenya#commssurveillance> accessed 19 May 2019

Privacy International, ‘Fintech: Privacy and Identity in the New Data-Intensive Financial Sector’ (2017) <https://privacyinternational.org/sites/default/files/2017-12/Fintech report.pdf> accessed 21 September 2019

Reeve T, ‘Only 5% of FTSE Companies Have Cyber-Security Expertise on the Board’ (*SC Media*, 2017) <https://www.scmagazineuk.com/5-ftse-companies-cyber-security-expertise-board/article/1475347> accessed 25 September 2019

Thales, ‘What is Sarbanes-Oxley (SOX) Act Data-at-Rest Security Compliance?’ <https://www.thalesesecurity.com/faq/americas-compliance/what-sarbanes-oxley-sox-act-data-rest-security-compliance> accessed 19 November 2019

Toshiba, ‘2014 Corporate Social Responsibility Report’ <http://www.toshiba.co.jp/csr/en/report/pdf/report14_all.pdf> accessed 9 June 2019

Ullah Z, Rehman A and Waheed A, 'The Impact of Corporate Accountability and Transparency on the Performance of Manufacturing Sector Firms Listed on KSE' <http://ssrn.com/abstract=2756977iElectroniccopyavailableat:http://ssrn.com/abstract=2756977ii> accessed 8 June 2019

Walubengo J, 'Why Facebook's suspension of Cambridge Analytica is instructive for Kenya,' Daily Nation (March 2018) <https://www.nation.co.ke/oped/blogs/dot9/walubengo/2274560-4349730-ldnsrp/index.html> accessed 8 January 2019

Woywada J, 'The Impact of Public Privacy on Corporate Governance: How Recent Findings in the Common Thread Network Can Impact Corporate Directors' IAPP (2018) < https://iapp.org/resources/article/the-impact-of-public-privacy-on-corporate-governance-how-recent-findings-in-the-common-thread-network-can-impact-corporate-directors/> accessed 8 January 2019

Reports

African Union 'Status List: African Union Convention on Cyber Security and Personal Data Protection | African Union' <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed 22 September 2019

Committee of Sponsoring Organizations of the Treadway Commission, 'Internal Control-Integrated Framework' (2013) <https://na.theiia.org/standards-guidance/topics/Documents/Executive_Summary.pdf> accessed 8 June 2019

Committee on the Financial Aspects of Corporate Governance, 'Report with Code of Best Practice [Cadbury Report]'

Communications Authority of Kenya, 'Third Quarter Sector Statistics Report for the Financial Year 2018/2019' (2019) <https://ca.go.ke/wp-content/uploads/2019/06/Sector-Statistics-Report-Q3-2018-19.pdf> accessed 21 September 2019

Deloitte, 'Building Trust: 2017 Planning Priorities for Internal Audit in Financial Services'

Global Partners Digital, 'Travel Guide to the Digital World: Encryption Policy for Human Rights

Defenders’

Ministry of Information Communications and Technology, ‘Request for Comments on the Proposed Privacy and Data Protection Policy and Bill, 2018’ <http://www.ict.go.ke/request-for-comments-on-the-proposed-privacy-and-data-protection-policy-and-bill-2018/> accessed 19 May 2019

OECD, ‘Guidelines for Consumer Protection in the Context of Electronic Commerce’ <www.oecd.org> accessed 1 May 2019

OECD, ‘Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document’ (2015) <http://dx.doi.org/10.1787/9789264245471-en> accessed 30 April 2019

OECD, ‘Digital Security Risk Management for Economic and Social Prosperity’ (2015) <http://dx.doi.org/10.1787/9789264245471-en> accessed 8 June 2019

OECD, ‘Consumer Protection in E-Commerce OECD Recommendation’ (2016) <http://dx.doi.org/10.1787/9789264255258-en.> accessed 15 April 2019

OECD 'Privacy Guidelines - OECD’ <https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm> accessed 30 April 2019

OHCHR 'Right to Privacy in the Digital Age’ <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx> accessed 14 April 2019

OHCHR 'Special Rapporteur on Privacy’ <https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx> accessed 30 April 2019

UNCTAD & EAC, ‘Draft EAC Legal Framework for Cyberlaws’ (2008) <http://hdl.handle.net/11671/1815> accessed 15 April 2019

UNCTAD ‘East African Community’ <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-EastAfrican.aspx> accessed 15 April 2019

United Nations, ‘United Nations Conference on Trade and Development Harmonizing

Cyberlaws and Regulations : The Experience of the East African Community'

United Nations Conference on Trade and Development (UNCTAD), 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' [2016] United Nations Publication <http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf>