Adequacy of Data Protection Regulation in Kenya

By

Antony Mugambi Laibuta

Student Number: 2425170

Supervisor:
Professor Emile Zitzke

October 2023

Thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy (PhD) in the School of Law, University of the Witwatersrand, Johannesburg, South Africa

Declaration

I, **Antony Mugambi Laibuta**, do hereby declare that this thesis is my own unaided work. It is submitted in fulfilment of the requirements for the degree of Doctor of Philosophy (PhD) in the School of Law at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Antony Mugambi Laibuta

Date: 02.05.2023

Signature:

Abstract

Article 31 of the Kenyan Constitution provides for the right to privacy. The Kenyan Data Protection Act, 2019 gives effect to Article 31(c) and (d) of the Constitution. This study is about whether data protection regulation in Kenya would inspire any confidence in data subjects who enjoy protection of their right to privacy under Article 31 of the Constitution.

Kenya, going with the global trend, in November 2019 enacted the Data Protection Act. Before the enactment, Kenya had debated data protection Bills for over a decade. But even with the enactment of the Data Protection Act, the question remains whether this was sufficient to guarantee the right to privacy and specifically data subject rights.

The main aim of this study is to determine the adequacy of data protection regulation in Kenya by responding to five questions: How has data protection evolved in Kenya? What framework should be used to determine the adequacy of data protection regulations? To what extent is the legal framework on state surveillance adequate? To what extent is the legal framework on commercial use of personal data adequate? How adequate are the available remedies in relation to data protection in Kenya?

To wit, no comprehensive academic discussion has explored the history of privacy and data protection in Kenya. This study fills this gap in the academic literature. It has established, through highlighting constitutional and statutory provisions, that the right to privacy in Kenya has been in existence since Kenya gained independence from colonial rule. Conversations during the clamour for constitutional reforms shaped the current text that provides for an individual right to privacy which has been the springboard for data protection rights to be introduced.

There is no immediately obvious framework that would be ideal to determine the adequacy of data protection regulation in Kenya. In light of this gap, this study has presented a simple set of questions used in day-to-day legal practice to be used as the determination-of-adequacy framework. The questions, “who?”, “why?”, “what?”, “when?”, “where?”, and “how?” are

posed on State surveillance, surveillance capitalism, and access to effective remedies. Responses to these questions are juxtaposed with provisions of the European Union's General Data Protection Regulation and South Africa's Protection of Personal Information Act. The responses reveal the level of adequacy of data protection regulation in Kenya.

On adequacy in State surveillance, surveillance capitalism, and availability of effective remedies, the study has revealed that while there are provisions of the law that adequately regulate the three issues, there are gaps and ambiguities that must be addressed to raise the level of adequacy and inspire confidence in data subjects. For the gaps and ambiguities, this study recommends law reforms in the form of amendments to provisions of the Kenyan Data Protection Act, Data Protection (General) Regulations, Competition Act, National Intelligence Service Act, and the Data Protection ADR Framework. This study also recommends enactment of new law including an Artificial Intelligence Act, Data Protection (Statutory Database) Regulations, and Regulations on interception of communications under the Prevention of Terrorism Act and other enabling statutes.

Acknowledgments

My express and sincere gratitude to everyone who facilitated my completion of this thesis. Specifically, I wish to thank my supervisor Dr. Emile Zitzke who generously, patiently, and thoughtfully offered me guidance throughout my research and writing process. I wish to thank Prof. Pamela Andanda who initially guided me as I drafted my proposal. My family has been a source of support, guidance, and inspiration. I am most thankful to my father, Hon. Justice Dr. Kibaya Imaana Laibuta who was my sounding board as I crafted arguments for my thesis and my mother Mrs. Agnes Mbuli Laibuta who was a constant source of encouragement. I sincerely wish to thank my sister Ms. Muthoni Laibuta for her never-ending moral support. I also wish to thank my '*Kikao*' brothers who sought to ensure I remained level-headed throughout my research process.

Dedication

To my late grandparents, Isaiah Imaana Laibuta and Zipporah Nyeera Laibuta; and to my parents Hon. Justice Dr. Kibaya Imaana Laibuta and Mrs. Agnes Mbuli Laibuta.

List of Abbreviations

AI – Artificial Intelligence

AIDS – Acquired Immunity Deficiency Syndrome

AU – African Union

CIPIT – Centre for Intellectual Property and Information Technology Law

CJEU – Court of Justice of the European Union

EDPB - European Data Protection Board

EU – European Union

GDPR – European Union General Data Protection Act

HAPCA – HIV/AIDS Prevention and Control Act

HIV – Human Immunodeficiency Virus

ICCPR – International Convention on Civil and Political Rights

IOT – Internet of Things

KDPA – Kenyan Data Protection Act

OECD - Organisation for Economic Co-operation and Development

POPIA – Protection of Personal Information Act

RICA - Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002

UDHR – Universal Declaration of Human Rights

UK – United Kingdom

UN – United Nations

UNCTAD - United Nations Conference on Trade and Development

USD – United States Dollars

ZAR – South African Rand

Table of Contents

CHAPTER ONE: INTRODUCTION

1.1 Introduction

In the last decade many countries have enacted data protection statutes. According to an UNCTAD report 137 out of 194 countries around the world have some form of legislation to regulate data protection and privacy.[1] Going with the trend, in November 2019, Kenya enacted the Data Protection Act (KDPA).[2] Has Kenya passed adequate legislation in this regard, or has it engaged in a window dressing charade by enacting inadequate legislation? This is what I seek to uncover in this thesis as far as adequacy of personal data protection regulation is concerned. The overarching theme in this thesis is thus whether personal data protection regulation in Kenya would inspire any confidence in individuals whose personal data is subject to incursions by the State and commercial actors.

In this chapter, I lay the basis of my study. In section 1.2 I discuss what data protection is as a concept. In section 1.3 I highlight classical elements of privacy under international instruments. In section 1.4 I discuss contemporary elements of privacy, while in section 1.5 I briefly indicate how Kenya has sought to regulate privacy and data protection. With the background in sections 1.2 to 1.5, in section 1.6 I set out the problem statement; in section 1.7 I lay out the objectives of this study; in section 1.8 I list the questions that form the basis of my inquiry; in section 1.9 I submit my methodology; and in section 1.10 I provide my chapter breakdown.

[1] UNCTAD "Data Protection and Privacy Legislation Worldwide" <Data Protection and Privacy Legislation Worldwide | UNCTAD> last accessed 6 September 2022.
[2] Act No. 24 of 2019.

1.2 Data protection as a concept

For decades, many scholars only sought to discuss the broad concept of privacy, with data protection as a concept only gaining global recognition in the last decade. As I demonstrate in this section, data protection (or "control of personal information" as some scholars cited below refer to it) is derived from the broader concept of privacy. In depth legal academic attempts to conceptualise privacy started more than 130 years ago; in 1890 Warren and Brandeis attempted to define privacy.[3]

Warren and Brandeis's attempt to define privacy was necessitated by what they called new technology that was invading privacy and domestic life.[4] The new technology they were referring to was "instantaneous photographs" and "newspapers".[5] This new technology enabled the broadcast of private information which in effect infringed upon the right to enjoy life and in extension, the "right to be let alone".[6] Warren and Brandeis identified harms caused by invasions into privacy. The harms included mental pain and distress on the affected individual.[7] With such harms caused by the intrusions into privacy, it was instructive that the law provide effective remedies for conduct such as the unauthorised circulation of portraits of private persons or disclosure of what would otherwise be private or intimate information about an individual.[8]

According to Warren and Brandeis, invasion of privacy inflicted injury that resembled wrongs such as slander and libel.[9] Their argument was that courts ought to have provided remedies for injurious disclosures of private matters or information.[10] The right to privacy discussed by Warren and Brandeis pointed to a "general right to privacy for thoughts, emotions, and

[3] S. D. Warren & L. D. Brandeis 'The Right to Privacy' (1890) *Harvard Law Review* 193.
[4] Ibid.
[5] Ibid 195.
[6] Ibid 205.
[7] Ibid 204.
[8] Ibid 211.
[9] Ibid 197.
[10] Ibid.

sensations".[11] However, they recognised that "the right to privacy does not prohibit any publication of matter which is of public or general interest".[12] This indicated that there may be justification to limit the right to privacy through intrusions into private space, or disclosure of what would essentially be regarded as private and personal information.[13] On designing the law on privacy, Warren and Brandeis stated:

> 'The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever their position or station, from having matters which they may properly prefer to keep private, made public against their will. It is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented.'[14]

A person's "affairs" mentioned by Warren and Brandeis is (very roughly) what we would call "personal information" or "data" today. Warren and Brandeis also identified invasion of privacy torts which related to commercialisation of personal information through appropriation, unreasonable publicity, and painting someone in false light.[15] Warren and Brandeis's writings that articulated the right to be let alone as what constituted the right to privacy set the tone for defining the concept of privacy going forward. The article remains relevant to date for academics, courts, and privacy practitioners.

From Warren and Brandeis's article, I draw several conclusions. First, there ought to be recognition of the right to privacy. Secondly, in reference to this study, there is recognition that an invasion upon this right to be let alone necessitates availability of effective remedies for aggrieved parties. Warren and Brandeis pointed to action for damages and injunctions as possible remedies for an invasion of the right to privacy.[16] Thirdly, the right may be limited where there is need to publish information "which is of public or general interest", such as information with legitimate connections to one's fitness for public office.[17] Fourthly, an

[11] Ibid 206.
[12] Ibid 214.
[13] Ibid.
[14] Ibid 214.
[15] C Tschider 'Meaningful Choice: A History of Consent and Alternatives to the Consent Myth' (2021) *North Carolina Journal of Law & Technology* 621.
[16] Warren and Brandeis (note 3 above) 219.
[17] Ibid 214 - 220.

individual's consent is key for the disclosure of private information. Fifthly, emerging technology may be used to infringe upon the right to be let alone.

Since publication of Warren and Brandeis' 1890 article, several scholars have sought to provide a nuanced approach to the conceptualisation of the right to privacy with specific reference to data protection or control over personal information which is the focus of this study.

In the African context, scholars such as Makulilo point to the fact that although in contemporary African constitutional frameworks, privacy and data protection are embraced, these concepts were not well defined within African societies before colonialism.[18] African societies had a communal model where the individual was largely subservient to the community and privacy was construed within the wider community interests.[19] Nonetheless, independence constitutions across the African continent contained elements of the right to privacy derived from the individualistic societal model of the colonisers.[20] Right to privacy elements in African independence constitutions shaped how the right to privacy has evolved around the continent. According to Makulilo, privacy, data protection, or control over personal information have been embraced as concepts that shape contemporary African societies including Kenya.[21]

Partly influenced by Warren and Brandeis work, control over personal information has emerged as a concept of privacy. According to Solove, "control over personal information" as a concept of privacy means that individuals, groups, and institutions determine for themselves when, how, and to what extent information about them is shared.[22] This as well relates to control over how personal information is acquired, disclosed, and used.[23]

[18] A Makulilo 'The Context of Data Privacy in Africa' (2016) in A Makulilo (Ed) *African Data Privacy Laws* 4 - 17.
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] D Solove 'Conceptualizing Privacy' (2002) *California Law Review* 1109- 1115.
[23] Ibid.

With reference as to exercising control, Austin submits that control over personal information is operationalised through consent.[24] According to Austin, derogations from consent may be considered as derogations from the right to privacy.[25] Bygrave and Tosoni, on emphasising the need for consent, state that rules requiring data subject consent constitute and substantiate the general basic principle of data protection law, that a data subject influences what other people do with information about them.[26] What Solove, Austin, Bygrave, and Tosoni allude to is that for control over personal information, the control must be accorded to an individual to the exclusion of other persons. Secondly, that control over personal information ought to be provided for in law.

The challenge with conceptualisation of privacy primarily as control over personal information is that it is not particular on what specific information ought to be controlled and perhaps over-restrictively equates control with consent.[27] The focus on consent as an instrument for control over personal information omits the fact that there are other avenues to lawful processing of personal information that do not present an individual with full control. In view of this, the law ought to define personal information subject to control and indicate that there are other modes of control apart from consent.

To illustrate other control measures, in performance of contractual obligations an individual may cede control over their personal information. In a contract for employment, an individual may sign off control over some of their personal information to an employer, enabling the employer to inquire into the suitability of the employee to remain in employment. In compliance with statutory obligations, an individual may have weak or no control due to the need for compulsory disclosure of personal information to State agencies such as revenue authorities, social security funds, and statutory regulators.

[24] L Austin 'Is Consent the Foundation of Fair Information Practices? Canada's Experience under Pipeda' (2006) *The University of Toronto Law Journal* 187.
[25] Ibid.
[26] L Bygrave and L Tosoni 'Article 4(11) Consent' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 176 (emphasis added).
[27] L Austin (note 23 above) 188 – 190.

There are different aspects of control over personal information. Rule, on his part, extends the control over personal information discourse by defining privacy to be "the effective exercise of an option to withhold information about oneself".[28] But, he qualifies this by arguing that in as much as one may exercise the option to withhold information about themselves, not everyone exercises this option, be it willingly or unwillingly.[29] There is a constant struggle over control of personal information.[30] Rule argues that context plays an important role in determining whether one is to withhold or disclose information.[31] Rule gives this example to demonstrate context: people may have no qualms about telling friends that they have recently declared bankruptcy, but actively endeavour to keep such information from potential creditors.[32]

Rule's definition points to the rights a data subject may have over their personal data. While elaborating on context, Rule posits that what may determine whether one will cede control of their personal data include factors such as where the personal data will be extracted from, how it will be maintained, and what the intentions of those who wish to use the data are.[33] This presupposes that there is legitimate use or need for personal data for it to be disclosed. Furthermore, certain information needs to be provided to a data subject for them to make the informed decision on whether they will cede control over their personal data. This strikes a balance between an individual's choices and commercial or financial interests that seek to process their personal data.[34]

Rule's definition points to an individual's lack of full control of their personal data by acknowledging that there may be instances where an individual may cede control of their personal data. In legitimate processing of personal data, the constant struggle over control of personal data emerges when the processing is for contractual obligations, compliance with

[28] J Rule 'Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions (2004) *University of Toronto Law Journal* 187.
[29] Ibid.
[30] Ibid.
[31] Ibid 189, 192.
[32] Ibid 189.
[33] Ibid 192.
[34] Ibid 224 – 225.

statutory requirements, and processing of personal data for public interest or public purpose.[35]

Rule's definition refines Solove's concept of control over personal information. While Solove did not focus on the fact that an individual may cede control or may not have control at all, Rule acknowledges that an individual is not always in control. Rule's concept and Solove's are however not specific in defining the legal circumstances under which one may not have full control over their personal information.

Another scholar, Kang, similarly makes arguments about control of "flow of personal information" by an individual by indicating that as personal information flows from one person to another, the individual from whom the information is extracted from ought to have a measure of control over processing of their personal information.[36] Moore also sought to discuss control over personal information as follows:

> 'a right to privacy can be understood as a right to maintain a certain level of control over the inner spheres of personal information and access to one's body and specific locations.[37] It is a right to limit public access to oneself and to information about oneself'.[38]

Moore goes on to state that:

> 'privacy also includes a right over the use of bodies, locations, and personal information. If access is granted accidentally or otherwise, it does not follow that any subsequent use, manipulation, or sale of the good in question is justified. In this way privacy is both a shield that affords control over access or inaccessibility and a kind of use and control right that yields justified authority over specific items—like a room or personal information'.[39]

Moore, like Solove and Kang, refers to the right over personal information.

Read holistically, what all of the abovementioned scholars' arguments indicate is that conceptually, data protection has several elements. First, the control over personal

[35] Ibid.
[36] J Kang 'Information Privacy in Cyberspace Transactions' (1998) *Stanford Law Review* 1202 - 1203
[37] A Moore *Privacy Rights: Moral and Legal Foundations* (2010).
[38] Ibid 25.
[39] Ibid 25, 26.

information by an individual. Secondly, that to cede that control, consent may be required. Thirdly, where consent is not a key determinant to cede control over personal information, there ought to be legitimate reasons, recognising that an individual does not always have full control over their personal information. Fourthly, harms may be occasioned on an individual where their personal data is accessed or used in the wrong manner. Fifthly, there may be instances where personal information may be made public for public interest and public benefit purposes. Sixthly, emerging technologies have an impact on how personal information is controlled, accessed, and publicised. Seventhly, effective remedies ought to be availed to anyone aggrieved by how their personal information is handled.

As control over personal information is mapped from the broad right to privacy, Rodotà submits that data protection or control over personal information is a fundamental right like any other.[40] Thus, individual countries have legal obligations with regard to data protection.[41] Secondly, Rodotà argues that since data protection is a fundamental right, "restrictions or limitations are only admissible if certain specific conditions are fulfilled, rather than merely on the basis of the balancing of interests".[42] Thirdly, on the nature of control of personal information as a right, Rodotà indicates that "the right to data protection has to do with protecting one's personality – not one's property".[43] Fourthly, on the broadness of data protection as a right, Rodotà argues that "data protection is an expression of personal freedom and dignity; as such, it is not to be tolerated that data is used in such a manner as to turn an individual into an object under continuous surveillance".[44]

In my view, the main takeaway from Rodotà is that there is an intricate relationship between privacy and control over personal information or data protection. As the right to privacy informed the conceptualisation of personal data protection, Makulilo argues that privacy and data protection are concepts that may be used interchangeably, and their use depends on the

[40] S Rodotà 'Data Protection as a Fundamental Right' S Gutwirth, Y Poullet, P Hert, C Terwangne, S Nouwt (eds) *Reinventing Data Protection?* (2009) 77 -82.
[41] Ibid 82.
[42] Ibid.
[43] Ibid.
[44] Ibid.

context.[45] Roos, while considering Warren and Brandeis's arguments on privacy, posited that data protection law is related to the right to privacy.[46] But, according to Roos, data protection is a narrower concept because it relates only to the processing of personal information while privacy is something much wider.[47] In my view, Roos is correct in arguing that data protection is a just one of the subsets of the broader right to privacy.

Having established privacy as a right from which data protection is derived, it is instructive to note that privacy may be construed as either a legal or moral right. As a moral right, the right to privacy is recognised notwithstanding not being provided for through written law. The challenge with moral rights is that it is not only difficult to identify their origin, but also to recognize them, as well as how to resolve disputes in the event of conflict arising out of the rights.[48]

Feinberg while quoting Frey[49] defines moral right as "a right which product of community legislation or social practice, which persists face of contrary legislation or practice, and which prescribes beyond which neither individuals nor the community may go in pursuit overall ends".[50] Many community practices that amount to the right to privacy have however, over time been legislated on and transited to legal rights.[51] As a legal right, the right privacy may be traced from international legal instruments, constitutional texts, statutory regulations, and case law. This thesis is about data protection as a legal right provided for in legal texts.

Considering the conceptualisations of personal data protection by the scholars cited above, in my view, the essence of personal data protection law contains four elements. First, there must be an express legal provision for personal data protection. Secondly, there should be a measure of control over personal data by the individual from whom the data is derived from.

---

[45] A Makulilo 'Privacy and Data Protection in Africa: A State of the Art' (2012) *International Data Privacy Law* 163-178.
[46] A Roos 'Privacy in the Facebook Era: A South African Legal Perspective' (2012) *The South African Law Journal* 375 – 402.
[47] Ibid 378.
[48] J Feinberg 'In Defence of Moral Rights' (1992) *Oxford Journal of Legal Studies* 150.
[49] R Frey, *Interests and Rights, The Case* Against Animals (1980) 7.
[50] Feinberg (note 48 above) 151.
[51] Ibid.

Thirdly, the law must stipulate circumstances under which an individual may cede control over their personal data. Fourthly, there ought to be recourse for the individual for any harm caused through processing of their personal data in contravention of the law. Section 1.3 below highlights some of the older international instruments that provide for the right to privacy while section 1.4 sets out the more contemporary legal texts.

1.3 "Classical" privacy protection internationally

The right to privacy features in several international instruments that Kenya has ratified with the effect of conceptualising privacy as a right and a legal obligation for Kenya. Kenya ratified the International Covenant on Civil and Political Rights on 1 May 1972, the Convention on the Rights of the Child on 30 July 1990, and the Convention on the Rights of Persons with Disabilities on 19 May 2008.[52] These conventions were ratified before the Constitution of Kenya, 2010 was promulgated and they provide for the right to privacy. Article 2(6) of the Kenyan Constitution states that any treaty or convention ratified by Kenya forms part of the law of Kenya under the Constitution. Kenya is bound by the international legal obligations under these instruments to protect, respect, and promote the right to privacy.

The specific provisions in the international instruments ratified by Kenya that have provision for the right to privacy are Article 12 of the Universal Declaration of Human Rights (UDHR),[53] Article 17 of the International Covenant on Civil and Political Rights (ICCPR),[54] Article 16 of Convention on the Rights of the Child (CRC),[55] and Article 22 of Convention on the Rights of Persons with Disabilities (CRPD).[56]

[52] OHCR "Status Ratification" < https://indicators.ohchr.org/> last accessed 21 March 2022.
[53] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).
[54] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).
[55] Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC).
[56] Convention on the Rights of Persons with Disabilities of 13 December 2006: U.N. Doc. A/RES/61/106.

Article 12 of the UDHR reads:

> 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

Article 17 of the ICCPR provides as follows:

> '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.'

Article 16 of the CRC says:

> '1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
>
> 2. The child has the right to the protection of the law against such interference or attacks.'

Article 22 of the CRPD follows the same theme:

> '1. No person with disabilities, regardless of place of residence or living arrangements, shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.
>
> 2. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others.'

With Kenya having ratified the above instruments, the conclusion I make is that Kenya has an international obligation to ensure that its privacy and data protection regulation respects, protects, and promotes the spirit and letter of the international instruments. The instruments provide a basis for deciphering privacy and data protection. In addition to these general human rights instruments, there are contemporary international legal instruments which I highlight in the next section that specifically provide for the right to privacy and data protection.

1.4 "Contemporary" privacy protection

In June 2014, the African Union adopted the African Union Convention on Cyber Security and Personal Data Protection.[57] The Convention provides for among other matters, regulation of personal data, institution of national personal data protection authorities, basic principles governing the protection of personal data, and data subject rights. The Convention is to come in force after ratification by 15 member states of the African Union. Currently, only 13 countries have ratified the Convention; Kenya is yet to ratify it.[58] Once Kenya ratifies the Convention, it would add a layer of regional obligations on the right to privacy and personal data protection.

In addition to ratification of the international legal instruments, more and more countries are enacting data protection legislation.[59] Makulilo argues that international instruments provide the "normative basis for the data protection laws" as data protection laws mirror the principles set out in these instruments. [60] Another phenomenon that informs data protection laws as Makulilo rightly argues, is enactment of privacy and data protection statutes fuelled by concerns emanating from "big data, the cloud and Internet of Things".[61]

Makulilo points to the fact that with emerging technologies, the size, amount, and speed of data collection is ever increasing together with "increased storage capacities" and "increased possibilities of manipulation of our personal data as well as the easy with which personal information can be shared across space and social media".[62] Mobile phone technology and

[57] Adopted by the Twenty-Third Ordinary Session of the Assembly, Held in Malabo, Equatorial Guinea, 27th June 2014.
[58] AU "List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection"
< 29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (au.int)> last accessed 6 September 2022.
[59] In Africa countries such as Angola, Benin, Burkina Faso, Cape Verde, Gabon, Ghana, Ivory Coast, Kenya, Lesotho, Madagascar, Mali, Mauritius, Morocco, Nigeria, Senegal, Seychelles, South Africa, Tunisia, and Western Sahara have data protection laws.
[60] Makulilo (note 18 above) 18.
[61] Ibid 3.
[62] Ibid.

access to the internet which have enjoyed high penetration in the Kenyan market have been a catalyst to increased processing of personal data.

The Communication Authority of Kenya's Third Quarter Sector Statistics Report for The Financial Year 2021/2022 (1st January– 31st March 2022)[63] reported the following:

> 'As at 31st March 2022, the number of active1 mobile (SIM) subscriptions stood at 64.9 million from 65.1 million subscriptions recorded by the end of 31st December 2021, and representing a mobile (SIM) penetration rate of 131.4%.[64]
>
> 'The total data/internet and broadband subscriptions stood at 46.5 million and 30.2 million respectively during the reference period…'[65]

As per the 2019 census report, Kenya's population is 47.6 million.[66] Looking at the Communication Authority of Kenya's reported statistics, Kenya has a high penetration of mobile phones, internet, and data usage. This means that there are many ready avenues of processing personal data. This study emphasises that such technology influences personal data protection.

Emerging trends of regulating personal data protection, as Solove argues, is an indication of a worldwide consensus on the importance of the right to privacy and the need to protect the right.[67] Pillai and Kohli make the case that privacy is an emerging norm in customary international law, they state that "even in the absence of uniform practice across the world, it is safe to characterise the right to data privacy as … a powerful emerging norm".[68] This in their view is sufficient to "derive a legally binding customary international law protecting the

[63] Communication Authority "Third Quarter Sector Statistics Report for The Financial Year 2021/2022" < Sector-Statistics-Report-Q3-2021-2022.pdf (ca.go.ke)> last accessed 27 June 2022.
[64] Ibid 1.
[65] Ibid 12.
[66] KNBTS "Kenya 2019 census report" <https://www.knbs.or.ke/?p=5621> last accessed 25 March 2022.
[67] D Solove *Understanding privacy* (2008) 12.
[68] A Pillai and R Kohli 'A Case for a Customary Right to Privacy of an Individual: A Comparative Study on Indian and other State Practice' (2017) Oxford University Comparative Law Forum < https://ouclf.law.ox.ac.uk/a-case-for-a-customary-right-to-privacy-of-an-individual-a-comparative-study-on-indian-and-other-state-practice/#C_Data_Privacy_as_an_emerging_norm_of_customary_international_law> last accessed 23 July 2022.

right to privacy".[69] Rengel agrees with the notion that "gradually, the right to privacy has become universally recognised as a fundamental human right".[70]

With international instruments providing for the right to privacy and in view of the emerging trends necessitating regulation of personal data, African countries are formulating and enacting personal data protection laws. On this issue, Makulilo argues that "claims for privacy in Africa are slowly becoming commonplace due to an increased use in modern technologies by both individuals and institutions. As a result, the need to protect privacy arises".[71] With this effect, just like the right to privacy having been implanted into the African legal framework through independence constitutions, data protection legal frameworks are being "borrowed" and implanted in Africa.[72] Bearing this in mind, in the next section, I focus on how Kenya has responded to the urge to have personal data protection regulation.

1.5 Kenya's data protection responses

Parliamentary Hansard records indicate that debate on the need for personal data protection laws in Kenya started a while back. One example is when Members of Parliament (MPs) were debating a Kenya Communications (Amendment) Bill on 23 July 1998 where one MP expressed concern for the privacy of a consumer.[73] The MP requested the Attorney General to draft a Data Protection Act to protect individuals' confidential data.[74] On 2 May 2000 when debating a Capital Markets Bill, MPs reiterated the need to have a Data Protection Act due to issues such as "tapping telephones".[75] On 12 May 2004 when discussing the need to amend the

[69] Ibid.
[70] A Rengel 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace' (2014) *Groningen Journal of International Law* 41.
[71] Makulilo (note 18 above) 21.
[72] Ibid 20.
[73] Kenya National Assembly "Official Record (Hansard)" < Kenya National Assembly Official Record (Hansard) - Google Books> last accessed 7th September 2022
[74] Ibid.
[75] Kenya National Assembly "Official Record (Hansard)" < Kenya National Assembly Official Record (Hansard) - Google Books> last accessed 7th September 2022.

Companies Act, MPs indicated that there was need to enact a Data Protection Act to ensure protection of data stored in electronic form.[76]

When debating an Anti-Money Laundering and Proceeds of Crime Bill on 8 May 2008, MPs decried the fact that Kenya had no "privacy laws in terms of looking at the privacy of people's data".[77] On 25 June 2009, a Minister responding to a question on control of junk mail in electronic communications indicated that the government would ensure that "privacy rights are protected through passage of the Data Protection Bill that would lay down penalties for misuse of personal information collected in Kenya".[78]

Despite the Parliamentary debates going as far back as 1998, it is in 2019, in keeping with the global trends that Kenya enacted the KDPA which became operational on 25 November 2019. The long title of the KDPA states that the law gives effect to Article 31(c) and (d) of the Kenyan Constitution. Article 31 of the Constitution provides for the right to privacy as a legal right:

> 'Every person has the right to privacy and that this right includes the right to every person not to have –
>
> (a) their person, home or property searched;
> (b) their possessions seized;
> (c) information relating to their family or private affairs unnecessarily required or revealed; or
> (d) the privacy of their communications infringed.'

Section 3(c) of the KDPA also explicitly states that one of the objects and purpose of the Act is "to protect the right to privacy of individuals". The broader right to privacy, compared to data protection, is not a new concept in the Kenyan constitutional and statutory architecture. As I discuss in more detail in Chapter 2 of this study, the right to privacy may be traced from the Independence Constitution, the current Constitution and in select statutory provisions. The KDPA is, nevertheless, the central pillar in the inquiry I carry out in this study. This central

[76] Kenya National Assembly "Official Record (Hansard)" < Kenya National Assembly Official Record (Hansard) - Google Books> last accessed 7th September 2022.
[77] Kenya National Assembly "Official Record (Hansard)" < Kenya National Assembly Official Record (Hansard) - Google Books> last accessed 7th September 2022.
[78] Kenya National Assembly "Official Record (Hansard)" < Kenya National Assembly Official Record (Hansard) - Google Books> last accessed 7th September 2022.

pillar has weaknesses that I discuss in the next section; the weaknesses form the crux of the problem statement of this study.

1.6 Problem statement

This thesis fills certain gaps in scholarly work on privacy and data protection in Kenya plus five potential broad weaknesses in the KDPA.

As a point of departure, I problematise the fact that there are no scholarly texts that trace the evolution of the right to privacy and data protection in Kenya. There is a void in the legal historical literature in this regard. It is a gap that I fill in this thesis. I further problematise that no scholarly work currently exists that interrogates the adequacy of data protection regulation in Kenya. No Kenyan data protection thinkers have laid a theoretical basis for this exercise, and none have been able to properly critique Kenya's data protection framework as a result. This is another gap that I fill in this thesis.

In this thesis I will problematise five potential weaknesses in the KDPA that indicate possible areas of inadequacy. First, is the lack of legislative provisions that spell out how to determine adequacy. Secondly, the KDPA provides for vague statutory exemptions to cater for public purpose and public interest in data processing. Thirdly, there is insufficient regulation of commercial use of personal data. Fourthly, there is lack of effective remedies and lack of deterrent and punitive penalties for infractions related to personal data protection. Fifthly, there is no statutory independence for the Data Protection Commissioner.

1.6.1 Lack of guidelines to determine adequacy

In normal practice, "adequacy determination" in data protection regulation assess foreign countries where personal data is being transferred to. For example, Section 48 of the KDPA provides for conditions for transfer of personal data out of Kenya:

'A data controller or data processor may transfer personal data to another country only where—

(a) 'the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;
(b) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;'

Regulation 42 of the Data Protection (General) Regulations, 2021 on appropriate safeguards:

'For the purpose of confirming the existence of appropriate data protection safeguards anticipated under section 49 (1) of the Act and these Regulations, any country or a territory is taken to have such safeguards if that country or territory has—

(a) ratified the African Union Convention on Cyber Security and Personal Data Protection;
(b) a reciprocal data protection agreement with Kenya; or
(c) a contractual binding corporate rules among a concerned group of undertakings or enterprises.' [79]

Regulation 40(b) of the Data Protection (General) Regulations, 2021 states that "a data controller of data processor who is a transferring entity shall before transferring personal data out of Kenya ascertain that the transfer is based on – an adequacy decision made by the Data Commissioner". In making this adequacy decision, Regulation 44(1) states:

'A transfer of personal data to another country or a relevant international organization is based on an adequacy decision where the Data Commissioner makes a decision that—

(a) the other country or a territory or one or more specified sectors within that other country, or

(b) the international organization, ensures an adequate level of protection of personal data.'

[79] Legal Notice No. 263 of 2021.

The above provisions do not indicate what is to guide one in coming up with the proof required to demonstrate the appropriate and adequate safeguards. Without an objective framework to demonstrate appropriate and adequate safeguards, proof to be provided to the Data Commissioner will be varied and disjointed. Secondly, if an objective framework to demonstrate appropriate and adequate safeguards was in place, it would easily be used by Kenya to carry out some introspection into the adequacy of its own data protection regulation.

In comparison, the European Union has provided for a loose framework to determine adequacy of countries where personal data of persons within the Union is transferred to. Article 45(2) of the European Union's General Data Protection Regulation (GDPR)[80] states that when assessing the adequacy of the level of protection, the European Commission is to take account of:

> '(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.'

[80] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

The KDPA does not have similar provisions to guide the determination of adequacy of another country's data protection regulation. Secondly, the GDPR provision does not provide for a situation where a country is undertaking a self-assessment on how adequate its data protection regulation is. Thirdly, academic discourse in Kenya is scant on determination-of-adequacy of data protection regulation.

To determine adequacy of data protection regulation in another country where personal data is being transferred to and to determine adequacy in Kenya, I ought to be guided by an objective framework that gives a wholistic view of the prevailing data protection regulatory framework. A framework to inquire into the adequacy of data protection regulation in Kenya does not exist in academic discourse. In this study I submit that there ought to be an objective framework to guide the determination-of-adequacy; in fact, I do propose an academic and objective framework.

1.6.2 Vague statutory exemptions for public purpose

Revelations by Snowden, a former Central Intelligence Agency employee and subcontractor,[81] and Wyle, a former Cambridge Analytica employee,[82] indicate the magnitude of State and non-state actors carrying out surveillance and extra-judiciously invading privacy to extract and use personal data. The right to privacy is at times relegated to the side lines, hence, the need to interrogate the adequacy of the regulatory framework that provides for State surveillance.

Lyon argues that in view of the revelations by Snowden on the extent of State surveillance in the United States of America, the State is always viewed with heightened mistrust.[83] Geist on the other hand submits that one of the challenges in regulating State surveillance is that laws were crafted before the current and emerging technologies were in use.[84] Current laws are

[81] E Snowden *Permanent Record* (Kindle Edn 2019).
[82] C Wyle *Mind F*ck: Cambridge Analytica and the Plot to Break America* (Kindle Edn 2019).
[83] D Lyon 'State and Surveillance' (2019) in CIG *Governing Cyberspace during a Crisis in Trust* 24.
[84] M Geist 'Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era' (2015) in M Geist (ed) *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* 225 – 249.

thus ineffective in providing oversight over the surveillance State.[85] State surveillance generally presents many challenges of which Duncan posits:

> 'Why should we be worried about surveillance? After all, governments argue, if people have nothing to hide, then they have nothing to fear: a saying whose origin is unclear, but which has been attributed to Orwell and, before him, the Nazi Minister of Propaganda, Joseph Goebbels. The problem with this argument is that it assumes that government motives in undertaking surveillance are pure: that is, they will not misuse these powers to spy on their political opponents and others whom they consider to be politically inconvenient, like investigative journalists intent on holding governments to account.'[86]

Duncan points out that emerging technologies are "making it easier for governments to place whole populations under surveillance".[87] These technologies as Duncan argues, provide the platform through which governments and commercial entities "gather vast amounts of information about people at a small fraction of the previous cost".[88] Essentially Duncan argues:

> 'the concerns about powerful institutions having such intimate knowledge about us have led to many becoming concerned that we are living in a surveillance society, where the collection, retention and analysis of vast quantities of data for the purposes of controlling human behaviour become central to our social fabric. Even more worryingly, we may be living under a surveillance state, in which the state uses this information to control citizens more effectively than in the past, because it has access to their most intimate details'.[89]

In Kenya, there have been reports of troubling breaches of privacy similar to the revelations made by Snowden and Wyle. One of them is the widely reported Cambridge Analytica scandal in the run up to the 2017 Kenyan general elections.[90] Wyle explains that the Cambridge

---

[85] Ibid.
[86] J Duncan *Stopping the Spies: Constructing and resisting the surveillance state in South Africa* (2018) 4.
[87] Ibid 5.
[88] Ibid.
[89] Ibid 8.
[90] E Auchard "Cambridge Analytica stage-managed Kenyan president's campaigns: UK TV" < https://www.reuters.com/article/us-facebook-cambridge-analytica-kenya-idUSKBN1GV300> last accessed 23 March 2022;
N Nyabola *"Politics in the digital age: Cambridge Analytica in Kenya"* < https://www.aljazeera.com/opinions/2018/3/22/politics-in-the-digital-age-cambridge-analytica-in-kenya> last accessed 23 March 2021 ; BBC "Cambridge Analytica's Kenya election role 'must be investigated'" < https://www.bbc.com/news/world-africa-43471707> last accessed 23 March 2021; The Star "Cambridge Analytica

Analytica scandal involved the use of personal data extracted from millions of Facebook users being used for targeted political messaging.[91] Extraction of personal data from Facebook was done without consent of the concerned Facebook users and without paying attention to basic data protection principles, not to mention undermining protected constitutional political rights.[92]

In another case of State surveillance, Privacy International, a non-governmental organisation, in March 2017 published a report dubbed 'Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya'.[93] The report describes how communications surveillance was carried out by State actors without oversight and contrary to procedures required by Kenyan law. The report indicates that intercepted communications content and data were used to facilitate gross human rights abuses, to spy on, profile, locate, track, and ultimately arrest, torture, kill, or disappear suspects.

In 2018 Citizen Lab published a report about "Pegasus Spyware" which is a mobile phone spyware sold by Israeli NSO Group.[94] The report indicates that the Kenyan government is most likely using the Spyware which has the capacity to snoop on all operations and information on a mobile phone.[95] In 2020, Citizen Lab published another report about "Circles" which they report is a "surveillance firm that reportedly exploits weaknesses in the global mobile phone system to snoop on calls, texts, and the location of phones around the globe".[96] The report concludes that the Kenyan government was a likely customer of "Circles". The Kenyan State is carrying out surveillance using unregulated technology.

---

confirms involvement in Kenyan elections" < https://www.the-star.co.ke/news/2018-03-20-cambridge-analytica-confirms-involvement-in-kenyan-elections/> last accessed 23 March 2022.

[91] Wyle (note 82 above).

[92] Ibid.

[93] Privacy International "Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya" <https://www.privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf> last accessed 23 March 2022.

[94] B Marczak, J Scott-Railton, S McKune, B Razzak, and R Deibert 'HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries' (2018). See also L Richard and S Rigaud *Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy* (2023).

[95] Ibid.

[96] B Marczak, J Scott-Railton, S Rao, S Anstis, and R Deibert 'Running in Circles Uncovering the Clients of Cyberespionage Firm Circles'(2020).

In another case of surveillance and notwithstanding that the KDPA took effect in 2019, in 2021, the Star newspaper reported that many Kenyans had found themselves registered to political parties without their consent.[97] Despite the illegal use of personal data to effect the registration, no action was taken against the political parties by either the Office of the Data Protection Commissioner or the Office of the Registrar of Political Parties.

To carry out State surveillance while making incursions into the right to privacy as illustrated above, the State may at times seek refuge under section 51(2) of the KDPA that provides for general exemptions. The provision states that the processing of personal data is exempt from provisions of the Act if it is necessary for national security or public interest. The Act, however, does not define what constitutes "national security" or "public interest".

In addition to section 51(2) of the KDPA, the State may also rely on statutes that provide for State surveillance. The statutes include the National Intelligence Service Act,[98] the National Police Service Act,[99] and the Kenya Defence Forces Act.[100] These statutes may be construed together with Article 24 of the Kenyan Constitution that provides that some fundamental rights and freedoms may be limited. In view of existence of the above statutes and Article 24 of the Constitution, the question that this thesis answers is whether Kenya's legal ecosystem on State surveillance is adequate *vis a vis* personal data protection.

1.6.3 Insufficient regulation of commercial use of personal data

Big data, and particularly personal data fuels the fourth industrial revolution. Taylor-Sakyi defines big data as "large sets of complex data, both structured and unstructured which traditional processing techniques and/or algorithms are unable to operate on. It aims to reveal hidden patterns and has led to an evolution from a model-driven science paradigm into a data-

[97] The Star "Kenyans protest registration as party members without consent" < Kenyans protest registration as party members without consent (the-star.co.ke)> last accessed 20 June 2022.
[98] National Intelligence Service Act, No. 28 of 2012.
[99] National Police Service Act Cap 84.
[100] Kenya Defence Forces Act, No. 25 of 2012.

driven science paradigm".[101] As we are in the fourth industrial revolution, Philbeck and Davis summarise the previous three industrial revolutions:

> 'The First Industrial Revolution, which first emerged in the United Kingdom in the 18th century, brought with it both steam power and factory politics, as women were pushed out of manufacturing roles in favor of a male-dominated workplace culture. The combination of steam power and mechanized production created a step change in output. This dynamic increase in capacity and productivity led to urbanization, the growth of regional and global market economies, the relevance of democratic governments, and a rising middle class in the western hemisphere.' [102]

> 'The Second industrial Revolution, which Vaclav Smil has persuasively dated between 1867 and 1914, is a subsequent wave of systems change that coalesced around the modern belief that science and technology are the way forward to a better life and that progress is in many ways a destiny for humanity. Entrepreneurs applied science to the ends of production, and the era saw a boon of products that were themselves the direct products of science and engineering.'[103]

> 'The Third Industrial Revolution, which began in earnest following the Second World War, brought a step change in information theory and the power of data. It bloomed alongside the discovery of the double helix, the space race, and the development of nuclear power. It shaped a post-war world that needed new economic structures and that had shifting conceptions of the human place in the cosmos, the natural world, and the political order. It also connected the planet's societies through infrastructure and applications, creating new flows of information sharing that continue to shape values, knowledge, and culture'[104]

Schwarb identifies drivers of the fourth industrial revolution to include personal data that has become an essential raw material for many important social and economic activities.[105] Schwarb argues that with the growing need for personal data, more "data-enhanced" technologies emerge.[106] Schwarb states that the Internet of Things (IOT) drive the fourth industrial revolution.[107] IOT as per Schwarb is "a relationship between things (products, services, places, etc.) and people that is made possible by connected technologies and various

[101] K Taylor-Sakyi 'Big Data: Understanding Big Data' (2016) ArXiv.
[102] T Philbeck and N Davis 'The Fourth Industrial Revolution' (2019) *Journal of International Affairs* 20.
[103] Ibid.
[104] Ibid.
[105] K Schwab *The Fourth Industrial Revolution* (2016) 18.
[106] Ibid 56.
[107] Ibid 22.

platforms".[108] It is because of IOT that there are billions of devices that depend on personal data to function connected to the internet.[109]

While discussing Schwarbs's concept of the fourth industrial revolution, Philbeck and Davis argue that "the concept of the Fourth Industrial Revolution affirms that technological change is a driver of transformation relevant to all industries and parts of society".[110] Constant exchange of information is at the centre of the fourth industrial revolution and technologies such as "robotics, advanced materials, genetic modifications, the Internet of Things, drones, neuro-technologies, autonomous vehicles, artificial intelligence, and machine vision" drive the revolution.[111] These technologies are integrated "into our physical, social, and political spaces, altering behaviours, relationships, and meaning".[112]

As big data fuels the fourth industrial revolution, the OECD's report on *Data-Driven Innovation: Big Data for Growth and Well-Being* in indicating the importance of big data states that analysis of big data that includes personal data drives knowledge and creates value within society. [113] Use of big data facilitates innovation, necessitates creation of new business models, enhances economic competitiveness, and fosters growth.[114] According to the OECD, big data empowers "entrepreneurs to develop new innovative commercial and social goods and services".[115] Data that is generated through social media, mobile devices and IOT offers opportunities to address challenges in both private and public sectors.[116]

The fourth industrial revolution has influenced unfettered use of personal data for commercial purposes. The linkages between the fourth industrial revolution and big data for commercial purposes may be described as surveillance capitalism. Macnish's defines surveillance as "the monitoring of a competent adult or adults over a period of time without

[108] Ibid.
[109] Ibid.
[110] Ibid 17.
[111] Ibid 18.
[112] Ibid.
[113] OECD *Data-Driven Innovation: Big Data for Growth and Well-Being* (2015).
[114] Ibid 20.
[115] Ibid 21.
[116] Ibid 31.

their consent. Surveillance can be carried out on other parties (e.g. children) and it may be carried out with consent".[117] Surveillance capitalism is carried out by private actors.

Zuboff explains that surveillance capitalism is about mass extraction of personal data that would be used by corporations for commercial purposes.[118] The data is analysed to make predictions about human behaviour and corporations use this information to target individuals with information that would likely guarantee certain changes in the behaviour of individuals. The more is known about an individual, the easier it is to control them.[119]

Corporations use personal data that captures behavioural data to shape individual's thinking and actions.[120] With copious amounts of data, corporations can nudge individuals towards certain directions with better precision and can predict the individual's thinking and actions.[121] Such nudging results into commercial gain for corporations, including fuelling the online direct marketing industry which in effect translates to purchase of goods and services by those targeted.[122]

Personal data is raw material for surveillance capitalism.[123] Technology that is engaged to extract large amounts of personal data evolves faster than States can regulate it, making surveillance capitalism thrive.[124] Surveillance capitalism as a business model has its origins in technology companies such as Google, Amazon, and Meta which found means to generate revenue using behavioural personal data collected for targeted advertising purposes.[125]

Crain narrates how growth of the internet was engineered through the surveillance capitalism model.[126] Crain details how technical, economic, and political underhandedness led to the creation of infrastructure based on vast data collection which is the essence of the internet

[117] K Macnish 'An Eye for an Eye: Proportionality and Surveillance' (2015) *Ethical Theory and Moral Practice* 530.
[118] S Zuboff *In the Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Kindle Edn 2019).
[119] Ibid Ch. 6.5.
[120] Ibid.
[121] Ibid.
[122] Ibid.
[123] Ibid Ch. 2.6.
[124] Ibid Ch. 4.2.
[125] Ibid Ch 3.1. Also see Digital Future Society *Privacy First: A New Business Model for the Digital Era* (2020).
[126] M Crain *Privacy Over Profit* (2021).

today.[127] Profit was prioritised at the expense of privacy. As Crain examines the social origins and effects of the internet's adoption of consumer monitoring, he describes how marketers and advertisers responded to the internet's existential threat by mobilizing start-up capital to create the now-pervasive business model known as surveillance advertising.[128] The business model thrives in Kenya as Meta, Google, Facebook, Amazon, Twitter (now 'X'), and TikTok with surveillance advertising operations offer services to data subjects in Kenya.

The Digital Future Society has attributed the growth of surveillance capitalism to rise of platforms, increase in mobile adoption, new ways of capturing data with IOT, and popularity of social media.[129] Ghosh and Couldry describe one aspect of surveillance capitalism as the "consumer internet".[130] In the "consumer internet", individuals are interconnected through the vast space of the internet which results in this space, online interactions, and exchanges being controlled for commercial gain.[131] Ghosh and Couldry argue that with these interaction and exchanges, "the world witnessed the revolutionary expanse of the big data economy – with tremendous increases in computing power and data storage combining to enable corporations to collect inordinate amounts of data – the digital media sector quietly built a novel commercial regime premised on such data collection".[132]

Ghosh and Couldry explain the business model of surveillance capitalism to consist of three elements to ensure monetisation of users.[133] First, is the collection of personal data which is instrumental in creating behavioural profiles.[134] Secondly, is the use of algorithms that curate content in social feeds and targeted advertisements.[135] Thirdly, is the addictive nature of engagement with the content on platforms that keep individuals "hooked".[136]

---

[127] Ibid.
[128] Ibid.
[129] Digital Future Society *Privacy First: A New Business Model for the Digital Era* (2020) 19.
[130] D Ghosh and N Couldry 'Digital Realignment Rebalancing Platform Economies from Corporation to Consumer' (2020) *M-RCBG Associate Working Paper Series* 6.
[131] Ibid.
[132] Ibid 15.
[133] Ibid 16.
[134] Ibid.
[135] Ibid.
[136] Ibid.

In Kenya, while platforms such as Google, META, Twitter, Apple, and Microsoft may be at the forefront of surveillance capitalism, industries such as telecommunications, banking, insurance, health, retail, transport, and education also adopt surveillance capitalism models. These industries use the services of data brokers whose business model is based on mass extraction of personal data for commercial purposes.

Just like State surveillance, surveillance capitalism involves incursions into individuals' privacy and disregard of personal data protection guidelines. On commercial use of personal data, section 37 of the KDPA provides:

> '(1) A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person—
>
> (a) has sought and obtained express consent from a data subject; or
>
> (b) is authorised to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.
>
> (2) A data controller or data processor that uses personal data for commercial purposes shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.
>
> (3) The Cabinet Secretary, in consultation with the Data Commissioner, may prescribe practice guidelines for commercial use of personal data in accordance with this Act.'

The Data Protection (General) Regulations, 2021,[137] provide for restrictions on commercial use of personal data. Regulation 14(1) of the Data Protection (General) Regulations, 2021 define commercial purposes to be:

> '…where personal data of a data subject is used to advance commercial or economic interests, including inducing another person to buy, rent, lease, join, subscribe to, provide or exchange products, property, information or services, or enabling or effecting, directly or indirectly, a commercial transaction.'

Regulation 14(2) states that "a data controller or data processor is considered to use personal data to advance commercial interests where personal data is used for direct marketing". The Regulations go on to set out permitted commercial use of personal data, features of opt out

[137] Legal Notice No. 263 of 2021.

messages, mechanisms to comply with opt out requirements, and requests for restriction of further direct marketing. Even with these provisions in place, the question is how they will apply to multinational digital platforms such as Facebook, Yahoo, Google, Twitter, TikTok, and Instagram that engage in mass data collection, processing, storage, and transfer. While these platforms have internal policies and are regulated in countries where they have their registered offices, in Kenya these platforms operate in an environment with weak personal data protection regulation.

Commercial use of personal data is not adequately regulated in sectors such as direct marketing, insurance, banking, education, health, gaming, betting, hospitality, communication, debt management, data brokerage, and transport. Kenyan law is also silent on emerging phenomenon such as artificial intelligence, machine learning, blockchain technology, facial recognition technology, and robotics. The Ministry of Information, Communication and Technology in 2020 launched a report dubbed *Emerging Digital Technologies for Kenya: Exploration and Analysis*.[138] The report makes a case for use of blockchain technology in Kenya while proposing legislative reforms that are yet to be realised.

Business entities have been criticised for their lackadaisical approaches to respecting the right to privacy of individuals. The Centre for Intellectual Property and Information Technology Law (CIPIT) at Strathmore University in 2020 published a report on privacy and data protection practices of digital lending apps in Kenya.[139] The digital lending apps studied included Tala, Branch, Okash, KCB, Equity (Eazzy Banking), Timiza, and Lioncash. CIPIT found that the digital lending apps studied did not comply with privacy and data protection principles outlined in the KDPA. CIPIT also established that the app shared personal data with third parties without the consent of data subjects plus they had embedded trackers that profiled user behaviour.[140]

---

[138] MoICT "Emerging Digital Technologies for Kenya — Exploration and Analysis" <http://www.ict.go.ke/blockchain.pdf> last accessed 3 April 2022.

[139] CIPIT "Privacy and Data Protection Practices of Digital Lending Apps in Kenya" (2020) <https://cipit.strathmore.edu/privacy-and-data-protection-practices-of-digital-lending-apps-in-kenya-report/> last accessed 26 June 2022.

[140] Ibid 31.

In October 2022, the Office of the Data Protection Commissioner issued notices to 40 digital lending companies.[141] The notices required the digital lending companies to demonstrate compliance with provisions of the KDPA. Being the first notices issued by the Office of the Data Protection Commissioner, it will be interesting to observe how the Office concludes the matter.

Another study by CIPIT interrogated data protection in the Kenyan banking sector with a focus on data policies.[142] The CIPIT study revealed that privacy policies within the banking sector did not pay attention to principles set out in the KDPA.[143] The revelations cast doubt on the fidelity to data protection principles by the banking industry in Kenya.

Unsolicited promotional messages are a menace in Kenya. Data brokers exploit poor regulation to sell personal data that is used for commercial purposes. While section 37 of the KDPA requires express consent before personal data is used for commercial purpose, Kenyans regularly receive unsolicited promotional messages. Before the KDPA was enacted, the Kenya Information and Communications (Consumer Protection) Regulations, 2010 under regulation 17(4) provides that "all automated direct-marketing schemes to be used in Kenya shall be based on an opt-in principle, in which potential subscribers shall be accorded the opportunity to accept or reject inclusion in a marketer's mailing list".[144]

The examples I have highlighted above indicate that potentially, there is inadequate data protection regulation in relation to commercial use of personal data in Kenya.

[141] Capital FM "Data Protection Office Probing 40 Digital Lenders Over Misuse Of Personal Data" <Data protection office probing 40 digital lenders over misuse of personal data - Capital Business (capitalfm.co.ke)> last accessed 14 December 2022.
[142] CIPIT "Data Protection in the Kenyan Banking Sector: A study of Publicly Available Data Policies of Commercial Banks operating in Kenya in Relation to a Set Data Protection Standard (2021)" < Data-Protection-in-the-Kenyan-Banking-Sector.pdf (strathmore.edu)> las accessed 8 September 2022.
[143] Ibid.
[144] Legal Notice 54 of 2010.

1.6.4 Lack of effective remedies

Ubi ius, ibi remedium - where there is a right there is a remedy. There ought to be accessible and effective remedies for the right to privacy and data protection. International instruments, constitutional provisions, and case law offer guidance on what constitutes an effective remedy to a violation of a fundamental right or freedom. On this, Article 8 of the Universal Declaration of Human Rights (UDHR) states that "everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law".[145] Similarly, Article 2(3) of the International Covenant on Civil and Political Rights (ICCPR) provides:

(a) 'To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;
(b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;
(c) To ensure that the competent authorities shall enforce such remedies when granted.'[146]

Article 47 of the Charter of Fundamental Rights of the European Union provides that "everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal".[147] An effective remedy as per the international instruments has four components. First, there ought to be a violation of a fundamental right that is recognised by law. Secondly, there ought to be a remedy for the violation. Thirdly, the determination of the remedy is to be undertaken by a competent authority. Fourthly, the remedy should be enforced by competent authorities once it is granted.

It is established that the right to privacy and data protection are rights recognised by law in Kenya. Where a violation occurs, the next question is whether competent authorities are available to provide effective remedies. The courts are one avenue that may ensure the availability of effective

[145] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).
[146] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.
[147] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

remedies. On courts, Article 22(1) of the Kenyan Constitution provides that "every person has the right to institute court proceedings claiming that a right or fundamental freedom in the Bill of Rights has been denied, violated or infringed, or is threatened". Where a remedy requires administrative action, Article 47 of the Kenyan Constitution provides:

> (1) 'Every person has the right to administrative action that is expeditious, efficient, lawful, reasonable and procedurally fair.
> (2) If a right or fundamental freedom of a person has been or is likely to be adversely affected by administrative action, the person has the right to be given written reasons for the action.'

An adequate regulatory framework for data protection ought to provide for accessible and effective remedies. This is not present in Kenya. To illustrate the lack of effective remedies, in the run up to the 2017 general elections, the Cambridge Analytica scandal was uncovered.[148] Cambridge Analytica harvested data of thousands of Kenyans from Facebook and used the data to create targeted political messaging going against Facebook policies and data protection laws that regulated Cambridge Analytica and Facebook in different jurisdictions. While the two companies were taken to task in some countries, no action was taken in Kenya. The United Kingdom Information Commissioner's Office on the other hand, in its 6 November 2018 report to UK Parliament titled 'Investigation into the use of data analytics in political campaigns' stated:

> 'We issued Facebook with the maximum monetary penalty of £500,000 available under the previous data protection law for lack of transparency and security issues relating to the harvesting of data. We found that Facebook contravened the first and seventh data protection principles under the Data Protection Act 1998 (DPA1998). We are in the process of referring other outstanding issues about Facebook's targeting functions and techniques used to monitor individuals' browsing habits, interactions and behaviour across the internet and different devices to the Irish Data Protection Commission, as the lead supervisory authority for Facebook under the General Data Protection Regulation (GDPR).'[149]

---

[148] L Madowo, "How Cambridge Analytica poisoned Kenya's democracy (2018)" < https://www.washingtonpost.com/news/global-opinions/wp/2018/03/20/how-cambridge-analytica-poisoned-kenyas-democracy/> last accessed 1 April 2022.

[149] UK Information Commissioner's Office "Investigation into the use of data analytics in political campaigns: A report to Parliament (2018)" < https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf> 9 last accessed 1 April 2022.

Section 63 of the KDPA provides that in relation to an infringement of a provision of the Act, the maximum amount of the penalty that may be imposed by the Data Commissioner in a penalty notice is up to five million shillings (around USD 46 000, or ZAR 671 000) or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, whichever is lower. Owing to the scope and scale of use of personal data, the statutory fines may end up not being punitive or deterrent enough. Since coming into office in November 2020, the Data Protection Commissioner has been slow in making administrative or penal orders against public or private entities infringing on provisions of the KDPA. This could perhaps be due to the lack of independence as argued in the next section.

1.6.5 Lack of independence of the Data Protection Commissioner

Sajo contends that the independence of independent authorities is tied to their "distance from constitutionally recognized branches of power". [150] Independence speaks to the integrity of the service which the independent authority renders.[151] According to Sajo, "appointment, dismissal, qualification, fixed term, conflict of interest rules (*incompatibilite*) of commissioners and other independent authority leaders are considered fundamental guarantees of authority independence".[152]

Independence is not absolute as independent authorities ought to be subject to oversight from institutions such as Parliament and courts.[153] However, Parliament and courts may only engage in oversight within their constitutional mandates.[154] Oversight does not mean receiving order or instructions from organs of the State or private entities.[155]

[150] A Sajo, 'Independent Regulatory Authorities as Constitutional Actors: A Comparative Perspective' (2007) *Annales Universitatis Scientiarum Budapestinensis de Rolando Eotvos Nominatae* 14.
[151] Ibid.
[152] Ibid.
[153] Ibid 13, 24.
[154] Ibid 24.
[155] Ibid

To water down independence, the KDPA creates two centres of power, the Cabinet Secretary in charge of Information Communication and Technology, and the Data Protection Commissioner who both have critical roles under the Act. While data protection oversight ought to be undertaken by an independent data protection authority, the KDPA outlines the following roles for the Cabinet Secretary:

a. Section 5(5) states that "the Data Commissioner shall in consultation with the Cabinet Secretary, establish directorates as may be necessary for the better carrying of the functions of the Office".
b. Section 35(5) provides that "the Cabinet Secretary may by Regulations make provision to provide suitable measures to safeguard a data subject's rights, freedoms, and legitimate interests in connection with the taking of decisions based solely on automated processing".
c. Section 37(3) states that "the Cabinet Secretary, in consultation with the Data Commissioner, may prescribe practice guidelines for commercial use of personal data in accordance with the Act".
d. Section 50 provides that "the Cabinet Secretary may prescribe, based on grounds of strategic interests of the state or protection of revenue, certain natures of processing that shall only be effected through a server or a data centre located in Kenya".
e. Section 68(3) requires that the annual financial estimates of the Office of the Data Protection Commissioner to be "submitted to the Cabinet Secretary for tabling in the National Assembly".
f. Section 70 mandates the Data Commissioner to, "within three months after the end of each financial year, prepare and submit to the Cabinet Secretary a report of the operations of the Office for the immediately preceding year".
g. Section 71(1) states that "the Cabinet Secretary may make regulations, generally for giving effect to the Act, and for prescribing anything required or necessary to be prescribed by or under (the) Act".

The above provisions indicate that the Office of the Data Protection Commissioner is not an independent office. Further, on lack of independence, section 8(2) of the KDPA states that

the Office of the Data Commissioner may, in the performance of its functions collaborate with the national security organs. The national security organs as defined under Article 239 of the Kenyan Constitution are the Kenya Defence Forces, the National Intelligence Service, and the National Police Service. The nature of the kind of collaboration contemplated under the KDPA is not defined.

The Office of the Data Protection Commissioner having to consult with the Cabinet Secretary and being mandated to collaborate with national security organs indicates that the Office will receive orders from these quarters. This has impact on the independence of the Office. *De facto* and *de jure* independence are key for the Office of the Data Protection Commissioner to offer effective remedies to individuals aggrieved by incursions into their privacy and data protection. Independence ensures that the Office of the Data Protection Commissioner is a competent authority.

Having established broad weaknesses in the KDPA, in the next section I discuss the five objectives of this study.

1.7 Objectives of the study

This study critically examines Article 31 of the Constitution of Kenya 2010 and the KDPA, it interrogates the status of data protection laws, jurisprudence, and how they have evolved since independence from colonial rule. It traces data protection concepts within Kenya's legal framework and examines the gaps in the KDPA. This study interrogates the adequacy of Kenyan law in regulating State surveillance, surveillance capitalism, and the availability of effective remedies.

The inquiry into Kenya's data protection framework is within constitutional principles of openness, access to information, accountability, prudence, responsibility, and equity to all. The specific objectives of this study are:

1. To trace and discuss the evolution of the right to privacy and data protection in Kenya which sets the background from which this study is derived.
2. To determine the appropriate framework to interrogate the adequacy of data protection laws in Kenya. This provides an objective framework to determine whether regulation of State surveillance, surveillance capitalism, and availability of effective remedies is adequate.
3. To interrogate State surveillance in Kenya to determine whether legal provisions on state Surveillance in Kenya are constitutional, adequate, and proportional.
4. To examine the adequacy of regulation of commercial use of personal data as use of personal data for commercial purposes continues to experience unfettered growth and negatively impacts the right to privacy and data protection.
5. To determine the adequacy of remedies and the independence of the Office of the Data Protection Commissioner. Availability of effective remedies is tied to the independence of the Office of the Data Protection Commissioner.

These five objectives are the basis of the five-research question of this study that I set out in the next section.

1.8 Research questions

Considering the above broad objectives of this study, the key research questions are:

1. How has data protection evolved in Kenya?
2. What framework should be used to determine the adequacy of personal data protection regulation?
3. To what extent is the legal framework on State surveillance adequate?
4. To what extent is the legal framework on commercial use of personal data adequate?
5. How adequate are the available remedies in relation to personal data protection in Kenya?

To respond to these five questions and address the objectives of this study, I adopt a comparative approach that I expound on in section 1.9 below.

1.9 Methodology

This study is overall, a desktop review of the adequacy of personal data protection regulation in Kenya. It adopts descriptive, interpretive, comparative, and prescriptive techniques of analysis. The analysis of Kenya's legal framework on personal data protection is juxtaposed with two jurisdictions, the European Union, and South Africa. The European Union and South Africa have the right to privacy provisions similar to Article 31 of the Kenyan Constitution. The European Union and South Africa are apt comparators to Kenya because their data protection laws are derived from the right to privacy provided for in overarching legal documents such as international human rights conventions and constitutions. Simply, data protection laws in these jurisdictions have similar origins, a "constitutional" right to privacy.[156]

Starting with the European Union, Article 8 of the European Convention on Human Rights states the following on the right to respect for private and family life:

1. 'Everyone has the right to respect for his private and family life, his home and his correspondence.
2. 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.'[157]

Article 8 above forms the basis for the European Union's (EU) regulatory interventions on the right to privacy and personal data protection. The EU (and in extension the Council of Europe) have had the Council of Europe, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 January 1981, ETS 108; the EU Directive 95/46:

[156] See G Samuel *An Introduction to Comparative Law Theory and Method* (2014) 57.
[157] 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.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; the EU the 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; and the Council of Europe enacted the Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) now popularly known as "Convention 108 plus".

As this study interrogates the adequacy of Kenyan law in regulating State surveillance, surveillance capitalism, and the availability of effective remedies, EU's GDPR is an instrumental comparator. The GDPR provides a framework to interrogate the adequacy of the level of data protection regulation in countries not under the GDPR.

On the other hand, section 14 of the South African Constitution on the right to privacy provides:

> ' Everyone has the right to privacy, which includes the right not to have—
> (a) their person or home searched;
> (b) their property searched;
> (c) their possessions seized; or
> (d) the privacy of their communications infringed."[158]

Section 14 mirrors Article 31 of the Kenyan Constitution. From section 14, South Africa has had the Protection of Personal Information Act (POPIA) since 2013.[159] However, POPIA has been in operation since mid-2021. Since coming into force, the Information Regulator has enacted the Protection of Personal Information Act: Regulations: "Information register"[160] and put in

[158] Act 108 of 1996.
[159] Act 4 of 2013.
[160] GG 42110, RG 10897, GoN 1383, 14 Dec 2018.

place the "Standard for Making and Dealing with Complaints in a Code of Conduct",[161] "Checklist for Submission of Application for Approval of a Proposed Code of Conduct",[162] "Guidelines to Develop Codes of Conduct",[163] "Guidance Note on the Processing of Personal Information of a Voter by a Political Party in Terms of the Protection of Personal Information Act, 4 of 2013"[164] and "Guidance Note on the Processing of Personal Information in the Management and Containment of Covid-19 Pandemic in Terms of the Protection of Personal Information Act 4 of 2013 (POPIA)".[165]

Recently, in *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services,*[166] a case concerning bulk surveillance, the South African Constitutional Court affirmed a declaration by the High Court of South Africa that had held the Regulation of Interception of Communications and Provision of Communication Related Information Act (RICA)[167] to be unconstitutional. The South African Courts held that RICA failed to provide adequate safeguards to protect the right to privacy. Such extensive South African privacy law jurisprudence and legal framework are useful comparators for Kenya from the African continent.

South African privacy law also provides a good comparator to avoid what Zitzke refers to as "mimicry" where a coloniser or former coloniser seemingly imposes legal traditions upon the colonised or former colonies.[168] To avoid modern day "mimicry" where "Western values" do

[161] Prescribed in terms of section 65 of the Protection of Personal Information Act No 4 of 2013 <https://www.justice.gov.za/inforeg/docs/InfoRegSA-Standard-CodeOfConduct-Complaints-20210301.pdf> last accessed 5 April 2021.
[162] Checklist Code of Conduct <https://www.justice.gov.za/inforeg/docs/InfoRegSA-Checklist-CodeOfConduct-20210303.pdf> last accessed 5 April 2022.
[163] Issued under the Protection of Personal Information Act 4 of 2013 (POPIA) <https://www.justice.gov.za/inforeg/docs/InfoRegSA-Guidelines-DevelopCodeOfConduct-22Feb2021.pdf> last accessed 5 April 2022.
[164] Guidance Note for Political Parties <https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-PolParties.pdf> last accessed 5 April 2022.
[165] Guidance Note on Covid-19 <https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf> last accessed 5 April 2022.
[166] *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* (CCT 278/19; CCT 279/19) [2021] ZACC 3 (4 February 2021).
[167] Act 70 of 2002.
[168] E Zitzke 'Decolonial Comparative Law: Thoughts from South Africa' (2022) *Rabel Journal of Comparative and International Private Law* 209 – 213.

not steam roll "African values", it is critical that Kenya's data protection regulation is juxtaposed with that of another African state *to wit* South Africa.[169] Kenya just like South Africa has since independence from colonial rule been creating indigenous legal values; Kenya can learn from South Africa and South Africa can learn from Kenya.

This study recognises that while there are similarities between EU's, South Africa's, and Kenya's right to privacy and data protection regulation, there are differences that inform the study into the adequacy of data protection regulation in Kenya. This study adopts a comparative approach and in making comparisons, Samuel notes:

> 'the comparatist first to recognise differences in the facts or objects being compared; secondly, to construct a relevant axis of comparison; thirdly, to establish and set out the criteria (or plans) of comparison; and fourthly, to place the facts or objects to be compared in a non-hierarchical relationship.'[170]

For this study, the axis of comparison is data protection regulation. The criterion for comparison is the determination-of-adequacy framework proposed in this study. The facts and objects for interrogation are the personal data protection regulations in the three jurisdictions. This study also includes doctrinal legal research that delves into the analysis of scholarly work and judicial decisions relating to personal data protection regulation.[171]

1.10 Chapter breakdown

1.10.1 Chapter Two: evolution of data protection in Kenya

The chapter focuses on answering the question: How has data protection evolved in Kenya?

Chapter two adopts a descriptive, historical, and analytic approach. The chapter highlights constitutional provisions related to the right to privacy since Kenya became independent from

[169] Ibid 21.
[170] Samuel (note 155 above) 54.
[171] See T Hutchinson and N Duncan 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) *Deakin Law Review* 83-120

colonial occupation in 1963. Secondly, it outlines current legislation that protects the right to privacy or elements of the right. The KDPA is afforded special focus as it refines privacy rights by outlining data subject rights, data protection principles, and lawful processing of personal data. Thirdly, the chapter highlights legislation that broadly or expressly limits the right to privacy in Kenya. Fourthly, the chapter draws special attention to court decisions that have dealt with the right to privacy and data protection. The chapter paints a picture of how the right to privacy has historically been structured within the Kenyan legal system.

1.10.2 Chapter Three: evaluating data protection regulation.

Chapter three responds to the question: What framework should be used to determine the adequacy of data protection regulation?

The core objective of the chapter is that it identifies the framework from which adequacy of data protection laws may be evaluated. The chapter proposes a nuanced approach to determine adequacy by applying an "adequacy test" that has "who?", "why?", "what?", "when?", "where?", and "how?" questions. The chapter asserts that comprehensive responses to these questions would aid in determining the adequacy of data protection regulation in Kenya.

On the "who?" question the chapter indicates that it is key that the law identifies the players in the personal data protection realm. These are essentially data subjects, data processors, and data controllers. Further, it is instructive that the law provides a framework to mitigate the negative impact of power asymmetry between the players.

For the "why?" question, the chapter identifies the explicit and specified purposes for use of personal data by the State and commercial entities while arguing that such uses ought to be provided for in law. The chapter argues that the responses to the "why?" question must pay attention to issues such as liberty and the harms that may be caused by processing of personal data.

The chapter through the "what?" question emphasises the requirement for the law to define the kind personal data being regulated. Moving to the "when?" question, the chapter makes the point that there are limitations to personal data protection which ought to be spelt out in the law. Secondly, the law ought to outline the principles to be used in striking a balance between processing of personal data and the right to privacy of an individual. Thirdly, the law must spell out what constitutes lawful processing of personal data.

Regarding the "where?" question, the chapter make arguments on jurisdictional issues in data protection. The law must answer the question of the territorial scope of the law. Where the law has extra-territorial application, the law ought to be clear and specific on the boundaries of the application.

The chapter focuses on the "how?" question pointing out that data processing operations should be regulated by law. Does the law regulate among others, the collection, storage, disclosure, transmission, dissemination, destruction, and analysis of personal data? Does the law identify and regulate technology as where personal data is processed? This is bearing in mind that technology has an impact on effecting personal data protection.

Secondly, on the "how?" question the chapter make arguments on how the law deals with oversight of data protection regulation. Is there an independent oversight authority and what the powers and functions of that authority? Thirdly, how does the law deal with access to effective remedies for data subjects?

1.10.3 Chapter Four: adequacy in State surveillance

Chapter four focuses on the question: To what extent is the legal framework on state surveillance adequate?

The chapter applies the "adequacy test" that has "who?", "why?", "what?", "when?", "where?", and "how?" questions on State surveillance. This determines whether there is

constitutional or statutory basis to have State surveillance use of personal data and whether the basis is proportional to data protection principles.

The chapter analyses legislation that allows the state to collect, collate, and analyse personal data for national security purposes. The chapter investigates mass surveillance, interception of private communications, and exemptions allowed within the KDPA.

The chapter brings out the vagueness and potential for State abuse of the exemptions under the KDPA. It makes the case for limited State surveillance use of personal of data while emphasizing the need for greater protection of an individual's right to privacy and data protection *vis a vis* the State. The State institutions that receive sharp focus in the chapter are the National Police Service, the Kenya Defence Force, and the National Intelligence Service.

The chapter through a comparative analysis of Kenya, the EU, and South Africa, proposes law reforms in State surveillance use of personal data in Kenya.

1.10.4 Chapter Five: adequacy in surveillance capitalism

Chapter five dwells on the question: To what extent is the legal framework on commercial use of personal data adequate?

The chapter applies the "adequacy test" that has "who?", "why?", "what?", "when?", "where?", and "how?" questions on surveillance capitalism. This determines whether there is constitutional or statutory basis to have surveillance capitalism processing of personal data and whether the basis is proportional to data protection principles.

The chapter through a comparative analysis of Kenya, the EU, and South Africa, proposes law reforms for commercial processing of personal data in Kenya. This is done over the backdrop of the need for commercial entities to comply with data protection principles outlined under the KDPA.

1.10.5 Chapter Six: effective remedies

Chapter six answers the question: How adequate are the available remedies in relation to data protection in Kenya?

The chapter applies the "adequacy test" that has "who?", "why?", "what?", "when?", "where?", and "how?" questions on accessibility of effective remedies. The chapter through a comparative analysis of Kenya, the EU, and South Africa points to the fact that remedies under the KDPA are inadequate. The chapter makes the case for law reforms to ensure statutory provision for accessible, adequate, and effective remedies.

Through application of the "adequacy test", the chapter examines the powers and functions of the Office of the Data Protection Commissioner and whether they are effective owing to the role the KDPA accords to the Cabinet Secretary in charge of information, communication, and technology. The chapter examines the role of the Office of the Data Protection Commissioner in regulating data controllers and data processors. The chapter makes the argument that the Office of the Data Protection Commissioner as framed under the KDPA is not independent; a predicament that must be remedied through law reforms.

The chapter through application of the "adequacy test" analyses the data protection dispute resolution process that includes conciliation, mediation, negotiation, and judicial intervention. The chapter proposes a model for independence of the Office of the Data Protection Commissioner and appropriate dispute resolution processes.

1.10.6 Chapter Seven: conclusion

Chapter seven concludes the study with proposals for law reforms in regulations protecting and promoting data protection in Kenya. The conclusion indicates the need to constantly apply the "adequacy test" for a nuanced approach towards interrogating the adequacy of data protection regulation.

CHAPTER TWO: EVOLUTION OF PRIVACY AND DATA PROTECTION IN KENYA

2.1 Introduction

This chapter focuses on the evolution of the right to privacy in Kenya. It adopts a descriptive, partly historical, and analytic approach. It provides an exploration of the current privacy-law and by extension, the data-protection framework in Kenya. This chapter lays the foundation for understanding and determining the adequacy of Kenya's data protection regulation.

This historical chapter matters for two main reasons. The first relates to the importance of the study of legal history generally. The second relates to the gap in historical research on privacy and data protection in Kenya in particular.

Bhat posits that "history gives a better understanding of the background in which any idea or institution or system originated, the purposes for which they emerged, their working, factors of their success or failure, and reasons for the same".[1] This chapter is an account of how the right to privacy and data protection have evolved and provides a contextual background of the constitutional and statutory origins of the rights. This chapter allows for better understanding of how the right to privacy has been construed in Kenya since independence from colonial rule. Bhat argues that "historical legal research exposes the social transformation dimension of law and gives clues for understanding the present law".[2]

A historical understanding of the right to privacy allows for reflection and better vision looking forward while interrogating the adequacy of data protection regulation.[3] Historical understanding allows the current generation of law makers, scholars, jurists, and legal

[1] P Bhat *Idea and Methods of Legal Research* (2019) 201.
[2] Ibid 206.
[3] Ibid 205.

practitioners to craft laws that aptly fit prevailing circumstances.[4] As Boorstin contends, the present is a culmination of the past,[5] but, the future must be recalibrated with an understanding of the past and present.[6]

It important to note that currently no robust academic analysis has taken place relating to the Kenyan constitutional right to privacy, provisions of the KDPA, and how they relate to the statutory provisions described below. The novel academic contribution of this chapter lies in the fact that it plugs this gap. Additionally, throughout this chapter, I flag potential problems in the current privacy-law scheme in Kenya, with the aim of indicating how they impact the adequacy of data protection regulation.

This chapter first highlights constitutional provisions related to the right to privacy since Kenya became independent from colonial rule in 1963. Secondly, it identifies current legislation that protects the right to privacy or elements of the right. The KDPA is afforded special focus as it refines privacy rights by outlining data subject rights, data protection principles, and lawful processing of personal data. Thirdly, the chapter highlights legislation that limits the right to privacy.

This chapter paints a picture of how the right to privacy has been structured within the Kenyan legal system. It sets out the constitutional, legislative, and jurisprudential framework that is instrumental in interrogating the adequacy of data protection regulation. This chapter provides the lenses through which one may anticipate how the right to privacy and data protection may be protected, respected, and promoted.

2.2 Constitutional protection of privacy in Kenya

As I interrogate the evolution of the right to privacy in Kenya, I note that privacy may be construed as a moral right or legal right or both depending on jurisdiction. Neethling

[4] Ibid 207.
[5] D Boorstin 'Tradition and Method in Legal History' (1941) *Harvard Law Review* 430.
[6] M Dubber 'Historical Analysis of Law' (1998) *Law and History Review* 159.

maintains that "since by nature a person has a fundamental interest in particular facets of his personality (such as his body, good name, privacy, dignity, et cetera), these interests exist autonomously *de facto*, independently of their formal recognition *de iure*".[7] *De facto* elements of the right to privacy are not considered in this study that focuses on the written law; the formal recognition of elements of the right to privacy in Kenya. The written law includes the constitutional text, legislation, and judicial decisions that have elements of the right to privacy and data protection in them.

This chapter and this study by extension do not delve into how privacy was construed in the Kenyan cultural context or as a purely moral right. Kenya is not an ethnically homogenous society; with over 43 ethnic groups that had their laws and customs passed through oral literature it is not within the scope of this study to interrogate ethnic laws and customs.

Boshe, Hennemann, and Meding have given a glimpse of privacy in the African context, they state that "the communal perspective in most African areas provides for little emphasis on an individual as a right bearer".[8] In other words, the allusion is that privacy might be regarded by some as an un-African concept. While this hypothesis about privacy in the African context is relevant to understanding how privacy laws are formulated in certain African contexts, we must be conscious of the problem of treating Africa as a uniform entity with no diversity within it. On this, Silungwe laments the futility of a purist notion of African legal theory because of the internal contradictions that exist within African communities.[9] In other words, there is no singular version of what it means to be African or, for this study, what an African approach to privacy might involve. With over 43 ethnic laws and customs, it is difficult to say what constitutes an indigenous Kenyan approach to privacy and data protection. Hence, my focus on the written law.

Before the independence Constitution, indigenous communities did not have written legal provisions on the right to privacy. The independence Constitution like most Commonwealth

[7] J Neethling 'The Concept Of Privacy In South African Law' (2005) *South African Law Journal* 19.
[8] P Boshe, M Hennemann and R Meding 'African Data Protection Laws Current Regulatory Approaches, Policy Initiatives, and the Way Forward' (2021) *Global Privacy Law Review* 34.
[9] C Silungwe 'On 'African' Legal Theory: A Possibility, an Impossibility or Mere Conundrum? (2014) in O Onazi (ed) *African Legal Theory and Contemporary Problems* 28.

countries was drafted in Lancaster, United Kingdom and as Dale narrates, Constitutions drafted for Commonwealth countries seeking independence post World War II had similar provisions.[10] Perhaps, it is for this reason that the right to privacy found its way into Kenya's independence constitutional text as it did in other Commonwealth countries' constitutions.

There have been three Constitutions governing Kenya since independence: the independence Constitution enacted in 1963, the post-independence Constitution that endured decades of amendments,[11] and the current Constitution promulgated on 27 August 2010. This section demonstrates that elements of the right to privacy have since independence found ground in the constitutional text.

Section 14 of the 1963 independence Constitution provided for protection of the right to privacy while section 20 provided for protection from arbitrary search and entry. Section 14 reads:

> 'Whereas every person in Kenya is entitled to the fundamental rights and rights and freedoms of the individual, that is to say, the right, whatever his race, tribe, place of origin or residence or other local connexion, individual, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, to each and all of the following, namely—
>
> (a) life, liberty, security of the person and the protection of the law;
> (b) freedom of conscience, of expression and of assembly and association; and
> (c) *protection for the privacy of his home and other property* and from deprivation of property without compensation, (emphasis added)
>
> the provisions of this Chapter shall have effect for the purpose of affording protection to those rights and freedoms subject to such limitations of that protection as are contained in those provisions, being limitations designed to ensure that the enjoyment of the said rights and freedoms by any individual does not prejudice the rights and freedoms of others or the public interest.'

[10] W Dale 'The Making and Remaking of Commonwealth Constitutions' (1993) *The International and Comparative Law Quarterly* 67 – 83.

[11] The independence constitution endured twenty-eight amendments between 1964 to 1997. See also G Muigai "Constitutional amendments and the constitutional Amendment process in Kenya (1964-1997) a study in the politics of the constitution (2001)" available at <Constitutional amendments and the constitutional Amendment process in Kenya (1964-1997) a study in the politics of the constitution (uonbi.ac.ke)> last accessed 7 March 2022 and G Muigai and D Juma *Power, Politics & Law: Dynamics of Constitutional Change in Kenya, 1887 – 2002* (2022).

On the other hand, Section 20 stipulates:

(1) 'Except with his own consent, no person shall be subjected to the search of his person or his property or the entry by others on against his premises.

(2) Nothing contained in or done under the authority of any law shall be held to be inconsistent with or in contravention of this section to the extent that the law in question makes provision—

(a) that is reasonably required in the interests of defence, public safety, public order, public morality, public health, town and country planning, the development and utilization of mineral resources, or the development or utilization of any other property in such a manner as to promote the public benefit;

(b) that is reasonably required for the purpose of promoting the rights or freedoms of other persons;

(c) that authorizes an officer or agent of the Government of Kenya, or of a Region, or of the East African Common Services Organization, or of a local government authority, or of a body corporate established bylaw - for public purposes, to enter on the premises of any person in order to inspect those premises or anything thereon for the purpose of any tax, rate or due or in order to carry out work connected with any property that is lawfully on those premises and, that belongs to that Government, Region, Organization, authority or body corporate, as the case may be; or

(d) that authorizes, for the purpose of enforcing the judgment or order of a court in any civil proceedings, the entry upon any premises by order of a court,

and except so far as that provision or, as the case may be, anything done under the authority thereof is 'shown not to be reasonably justifiable in a democratic society.'

The post-independence Constitution which was repealed on 27 August 2010 had section 70 providing for protection of the privacy of the home and other property while section 76 provided protection against arbitrary search and entry. The post-independence provisions mirror the provisions under the 1963 independence Constitution.

While there are no academic commentaries on these provisions, the courts were often called upon to determine the constitutionality of searches and seizures. For example, in *Standard Newspapers Limited v Attorney General* where a search and seizure had been carried out against the Petitioner, the High Court ruled "that the petitioners' rights under sections 76 and 79 of the constitution were violated by the respondents' action of arbitrary search and seizure".[12] In *Heiwua Auto Kenya Limited v The Office Commanding Police Division Central Police*

[12] *Standard Newspapers Limited & another v Attorney General & 4 others* [2013] eKLR.

Station, the court recognised the fact that a search could be carried out within the confines of the law, referring to section 76 of the then Constitution.[13] In these two cases, the courts ruled that searches and seizures were carried out contrary to provisions of the criminal procedure code and police procedures, and thus violated the constitutional right against arbitrary searches and seizures.

The two decisions demonstrate that the right to privacy found protection from constitutional provisions and pronouncements by the courts. This is notwithstanding the fact that the then Constitution did not provide for an express individual right to privacy. The provisions were about protection for the privacy one's home and property and protection against arbitrary searches and seizures. It was not until Kenya's clamour for constitutional change in the early 2000's that the express and broader individual right to privacy gained traction. No information is available to explain why there was a shift to an individual right to privacy in the constitutional text.

I hypothesise that the shift could be explained by the fact that international human rights instruments contain a broader right to privacy, covering more than just privacy in property and hence, the constitutional drafters may have been persuaded to have constitutional provisions that mirror the international human rights instruments. The drafters could also have been inspired by progressive constitutional frameworks on the African continent, such as South Africa's 1996 Constitution that contains an individual right to privacy. Section 14 of South Africa's Constitution states:

> 'Everyone has the right to privacy, which includes the right not to have-
>
> a. their person or home searched;
> b. their property searched;
> c. their possessions seized; or
> d. the privacy of their communications infringed.'

[13] *Heiwua Auto Kenya Limited &3 Others V The Office Commanding Police Division Central Police Station & 3 Others* [2010] eKLR.

Section 14 above is almost a word-for-word mirror of draft Constitutions debated in Kenya and the current constitutional provision on the right to privacy. I suggest that international cosmopolitanism and comparative constitutional architecture could be another reason why currently Kenya has a broad constitutional provision on the right to privacy.

The final report of the Constitution of Kenya Review Commission published in 2005, on protection of privacy stated that "a provision should also give general protection to privacy of the home, person, correspondence and other forms of communication. This is relevant to the behaviour of law enforcement agencies, and of fellow citizens".[14] This is the reason for having an individual right to privacy in the draft constitutional texts.

Since independence, Kenya has considered several draft constitutions in the quest for constitutional reforms. The proposed draft constitutions provided for an express individual right to privacy. They included: clause 47 of the Proposed New Constitution of Kenya, 2005 which was rejected by voters in the 2005 referendum; clause 43 of the Constitutional Amendment Bill proposed by the report of the Constitution of Kenya Review Commission in 2003;[15] and clause 47 of the Constitutional Amendment Bill proposed by the National Constitutional Conference in 2004.[16] As there was no debate on the right to privacy clauses, it was never clear whether the right to privacy would finally find its way into Kenya's constitutional text.

In the run up to the promulgation of the Constitution of Kenya, 2010, the proposed text on the right to privacy came up for debate. When the Committee of Experts on Constitutional Review submitted a proposed draft Constitution to the National Assembly for consideration, the Assembly flagged out the proposed clause 31 that provided for the right to privacy. The National Assembly wanted the following clauses deleted:

> 'Every person has the right to privacy, which includes the right not to have—

[14] The Final Report of the Constitution of Kenya Review Commission (2005) 122.
[15] The draft Constitutional Amendment Bill was revised to come up with the Proposed New Constitution subjected to the 2005 referendum.
[16] This Bill informed the text of the Constitutional Amendment Bill proposed by the report of the Constitution of Kenya Review Commission in 2003.

(a) their person, home or property searched;

(b) their possessions seized;'

According to the National Assembly:

'Clause (a) would affect security measures with regard to searches, especially in this era of terrorism.

Clause (b) would complicate financial transactions as collateral for loans would be rendered useless.'[17]

The National Assembly's proposals for deletion of the clauses were not adopted as they did not receive the margin of support required for adoption.[18] The Constitution of Kenya (Amendment) Act, 2008 required that any amendment to the Proposed Constitution should be supported by 65% of the Members of the National Assembly to be adopted. The proposed clause on privacy at the time read:

'Every person has the right to privacy and that this right includes the right to every person not to have –

(a) their person, home or property searched;
(b) their possessions seized;
(c) information relating to their family or private affairs unnecessarily required or revealed; or
(d) the privacy of their communications infringed.'

Were the Assembly's proposals to delete clauses (a) and (b) adopted, Kenya would have had a watered-down constitutional right to privacy. The National Assembly had no opposition to the right to privacy in general terms, perhaps since the right appeared in the independence constitutional text and the text repealed by the current Constitution. The current Constitution was promulgated on the 27 August 2010 after having been ratified through a referendum on 4 August 2010. 68.55% of the voters approved the constitutional text with the proposed provision on the right to privacy forming Article 31 of the current Constitution.

The constitutional right to privacy is however not absolute. The right is not listed in Article 25 that lists fundamental rights and freedoms that may not be limited. On limitations, Article 19(3) states that "the rights and fundamental freedoms in the Bill of Rights are subject only to the limitations contemplated" in the Constitution. Article 24(1) provides that a right or

[17] Final Report of the Committee of Experts on Constitutional Review (2010) 139.
[18] Ibid 137.

fundamental freedom "shall not be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom".

More recently, the Constitutional (Amendment) Bill 2020 sought to amend, among other constitutional provisions, Article 31 on the right to privacy. The Bill proposed to expand the right to privacy to include a provision stating that "every person has the right to privacy, which includes the right not to have their personal data infringed".[19] If the Constitutional (Amendment) Bill was ratified, personal data protection would have been an express constitutional right. However, the High Court[20] and the Court of Appeal[21] declared the Bill to be unconstitutional for not having been published following constitutional procedures, not having been subjected to comprehensive public participation, and generally for amending what the courts deemed as the basic structure of the Constitution. In the end, the Supreme Court declared the constitutional amendment process that resulted in promotion of the Bill to have been unconstitutional.[22]

In addition to constitutional provisions, legislation has provided basis for protection of the right to privacy. The Constitution forms the cardinal source of the right to privacy and as Woolman argues (albeit in relation to the South African Constitution), "the Constitution is a form of scaffolding".[23] Woolman reasons that the constitutional text is not enough by itself, even with a robust Bill of Rights.[24] A constitutional text, as per Woolman, ought to be supported by "a rule of law culture", "political accountability", and "effective

[19] Constitutional (Amendment) Bill 2020. <http://kenyalaw.org/kenyalawblog/wp-content/uploads/2020/10/Constitution-of-Kenya-Amendment-Bill-25-11-2020.pdf> last accessed on 10 March 2022.
[20] David Ndii & others v Attorney General & others [2021] eKLR.
[21] Independent Electoral and Boundaries Commission & 4 others v David Ndii & 82 others; Kenya Human Rights Commission & 4 others (Amicus Curiae) [2021] eKLR.
[22] *Attorney-General & 2 others v Ndii & 79 others; Prof. Rosalind Dixon & 7 others (Amici curiae)* (Petition 12, 11 & 13 of 2021 (Consolidated)) [2022] KESC 8 (KLR).
[23] S Woolman 'Understanding South Africa's Aspirational Constitution as Scaffolding' (2016) *New York Law School Law Review* 283 - 295. See also S Woolman 'South Africa's Aspirational Constitution and our Problems of Collective Action' (2016) *South African Journal on Human Rights* 156-183.
[24] Ibid 285.

bureaucracies".[25] The rule-of-law culture, according to Woolman, would ensure that any State action is sanctioned by the law, applies equally to the citizens and ruling elite, is reasonable, and draws power from the constitutional text.[26]

In addition to rule of law culture, political accountability, and effective bureaucracies, legislation to give effect to constitutional provisions is key.[27] Du Plessis adds that legislation "has a very special role to play in the fulfilment of crucial constitutional objectives. Legislation is therefore an indispensable ally of the Constitution".[28] Thus, statutes on privacy are critical.

Even where legislation gives effect to constitutional provisions, Du Plessis while interrogating the South African context argues that statutes ought to be construed "to promote the spirit, purport and objects of both the Bill of Rights, and the specific constitutional provision(s) to which more concrete effect is given".[29] As such, statutes should "not be allowed to decrease the protection that a constitutional right affords or to infringe any other constitutional right".[30]

Before delving into the statutes, in the next section, I highlight case law that has interrogated the application of the right to privacy as provided for under Article 31 of the Constitution. The court decisions while not exhaustive point to a continuous emphasis on the importance of respecting, protecting, and promoting the right to privacy in Kenya.

[25] Ibid 285.
[26] Ibid 291.
[27] L du Plessis 'The Status and Role of Legislation in South Africa as a Constitutional Democracy: Some Exploratory Observations' (2011) *Potchefstroom Electronic Law Journal* 92 - 99.
[28] Ibid 97.
[29] Ibid.
[30] Ibid.

2.3 Judicial interpretation of the constitutional right to privacy

2.3.1 Samura Engineering Limited v Kenya Revenue Authority

In *Samura Engineering Limited*,[31] the High Court, on warrantless searches and seizures, ruled that they violated the right to privacy protected under Article 31 of the Constitution.[32] The Court stated that the right to privacy is enshrined in the Constitution and included the right to not to have one's person or home searched, one's property searched, or possessions seized. As searches infringe on the right to privacy, they must be conducted in compliance with legislation which in turn must comply with the provisions of Article 24 of the Constitution. Such constitutional safeguards "regulate the way in which state officials enter the private domains of ordinary citizens is one of the features that distinguish a democracy from a police state".[33] The onus is on the State to prove that the conduct of their agents while making incursions into the privacy of an individual meets constitutional standards.[34]

The court recognised that the State power to collect taxes by law ought to be "balanced with that of the individual right to privacy and dignity and in balancing these rights, the State must justify its actions".[35] When society places the values of rule of law, good governance, transparency, and accountability at the centre of the Constitution, the culture should be one that provides justification for any infringement of fundamental rights and freedoms. Search and seizure without reasonable cause was a breach of the right to privacy.[36]

The court linked the right to privacy with other rights by stating that "the purpose of the right to privacy is to protect human dignity which is itself a right protected under Article 28".[37] A search and seizure that took personal documents that included a will, medical records, documents of children and other documents not related to tax affairs was "an attack on the

[31] *Samura Engineering Limited & 10 others v Kenya Revenue Authority* [2012] eKLR.
[32] Ibid 104.
[33] Ibid 66.
[34] Ibid 76.
[35] Ibid 77.
[36] Ibid 83.
[37] Ibid 100.

inner sanctum of a person".[38] The decision demonstrates that courts will question State actors when they make incursions into the right to privacy and data protection of individuals.

2.3.2 Kenya Plantation and Agricultural Workers Union v James Finlay (K) Limited

In *Kenya Plantation and Agricultural Workers Union,*[39] the issue in contention was the safety of patients' records once a medical facility ceased to exist. Arguments set out before the court were that even where a medical facility was shut down, patients' records were still regulated by doctor-patient confidentiality. The court in making a determination on the issues before it emphasised on the fact that under Article 31(c) of the Constitution, every person has the right to privacy which includes the right not to have information relating to their family or private affairs unnecessarily required or revealed. As per the court this right to privacy extended to "having information such as official records, photographs, correspondence, diaries and medical records kept private and confidential".[40] Thus, there was need for medical professionals to "take positive steps to prevent intrusions into the privacy of its hospital's patients".[41]

In this decision, the court identified official records, photographs, correspondence, diaries, and medical records as information that ought to enjoy protection within the ambit of the right to privacy. The court found that where a medical facility was shut down, patients' records were still regulated by doctor-patient confidentiality. This decision is instrumental in highlighting occasions where courts have identified information that requires protection.

[38] Ibid.
[39] *Kenya Plantation and Agricultural Workers Union V James Finlay (K) Limited* [2013] eKLR.
[40] Ibid.
[41] Ibid.

2.3.3 C.O.M. v Standard Group Limited & another

In *C.O.M.* the Petitioner's claim related to publication of his photos in the Respondents' newspaper without consent. He claimed that this was a violation of his right to privacy under Article 31.[42] The court asserted that "the Petitioner's written consent was not sought for his photograph and names to appear in the publication, I am also persuaded to find that the Respondent also violated the Petitioner's right to privacy as pleaded."[43] The court awarded general damages for pain and suffering to the Petitioner.[44] This decision looks into when consent was considered to have been crucial before the Petitioner's privacy could have been infringed.

The court awarded damages for pain and suffering. While the decision was made before the enactment of the KDPA, it indicates that the courts have had a disjointed approach in providing effective remedies considering similar damages were not awarded in *David Lawrence Kigera Gichuki v Aga Khan University Hospital*, which is discussed next.[45]

2.3.4 David Lawrence Kigera Gichuki v Aga Khan University Hospital

In *David Lawrence Kigera Gichuki,* the issue in contention was that the Respondent had released the Petitioner's medical information to a third party without consent in effect violating the Petitioner's right to privacy under Article 31.[46] The court noted that "the right to privacy is not absolute and must, in certain circumstances, give way to the greater public interest in disclosure".[47] The court emphasised that the right to privacy was not an absolute right and that the right was subject to limitations outlined under Article 24 of the Constitution.[48]

---

[42] *C.O.M. v Standard Group Limited & another* [2013] eKLR
[43] Ibid 25.
[44] Ibid 32.
[45] *David Lawrence Kigera Gichuki v Aga Khan University Hospital* [2014] eKLR.
[46] Ibid.
[47] Ibid 22.
[48] Ibid 18.

In its final decision the court was of the view that there was a breach of privacy as medical information had been released to a third party.[49] But, the court was "not satisfied that there was any loss occasioned to the petitioner, or that damages, are as a result of such disclosure, merited" hence no damages were awarded.[50] This decision informs the discussions on remedies for incursions made into the right to privacy and data protection. It is my view that the courts will need to revisit how they award damages in privacy and data protection related disputes.

2.3.5 J L N v Director of Children Services

In *J L N*, the petitioners' case was against a hospital which they claimed had violated their right to privacy by unnecessarily and without just cause disclosing confidential medical information to a third party in violation of their right to privacy protected under Article 31.[51] Their case was anchored on the fact that the Hospital breached the doctor/patient confidentiality in disclosing the details of a surrogacy arrangement. The court found that the Hospital was right to inform the Director of Children Services about the surrogacy arrangement between the Petitioners as Kenya at the time did not have a law regulating surrogacy. The court in making this finding stated:

> 'The right to privacy is not absolute. Implicit in the protection accorded is that information relating to family and private matters must not be "unnecessarily revealed." Indeed, counsel for the petitioner submitted that there are instances where the right to privacy in respect of the patient/client relationship may be abridged. He cited the case of *W v Edgell* [1990] 1 ALL ER 835 where Lord Bingham set out the principles under which a doctor may disclose the information held in confidence. The principles were as follows;
>
> I. A real and serious risk of danger to the public must be shown for the exception to apply.
> II. disclosure must be to a person who has legitimate interest to receive the information.
> III. disclosure must be confined to that which is strictly necessary (not necessarily all the details).'[52]

[49] Ibid 37.
[50] Ibid 39, 40.
[51] *J L N & 2 others v Director of Children Services & 4 others* [2014] eKLR.
[52] Ibid 22.

The focus here is on disclosure of medical information. Potential risk to the public could for example be during a public health emergency and the information disclosed would be specific to dealing with that public health emergency. This decision points to a nuanced approach for reasons to make incursions into the right to privacy. In this case the justification was that the activities of the petitioners were not regulated by statute and did not enjoy constitutional or statutory protection. What this means is that activities that may be considered unlawful would not enjoy privacy protection.

In my view, this decision demonstrates instances where the courts will allow for limitation of the right to privacy and confirms constitutional guidelines that the right is not an absolute one. This is especially significant when dealing with State surveillance which I discuss in this study.

2.3.6 Aids Law Project v Attorney General

In *Aids Law Project,* the Petitioner challenged statutory provisions that stated that persons living with HIV/AIDS were legally obligated to disclose their medical status to their sexual contacts and not to keep such information confidential.[53] The obligation was set out under section 24 of the HIV and AIDS Prevention and Control Act, 2006.

The Petitioner claimed that disclosure of such information would undermine Article 31. The court agreed that such disclosure was inconsistent with Article 31 and the confidentiality principle of medical information.[54] The court ruled that the provision on disclosure of health status was vague and too broad, and lacked certainty, especially when it comes to the term "sexual contact". Such vagueness created an undesired situation of maintaining a law that vaguely prescribes criminal offenses that leave the court's subjective judgment as to whether the defendant has been convicted or acquitted.[55]

[53] *Aids Law Project v Attorney General & 3 others* [2015] eKLR.
[54] Ibid 87.
[55] Ibid 88.

This case dealt with vagueness and lack of certainty in provisions that protect or detract from confidentiality and in effect, the right to privacy. Any vague, broad, and uncertain provisions in statute or subsidiary legislation used to justify an assault into an individual's right to privacy will lead to potential successful challenges in the courts. As I argue in this study, provisions that vaguely and broadly limit the right to privacy and data protection should be struck out by the courts.

2.3.7 Kenya Legal and Ethical Network on HIV & AIDS (KELIN) v Cabinet Secretary Ministry of Health

The High Court in *Kenya Legal and Ethical Network on HIV & AIDS (KELIN)* was asked to rule on a Presidential Directive to County Commissioners to work with County Directors of Education and County Directors of Medical Services to collect up-to-date data on all school-going children living with HIV as well as expectant and breastfeeding mothers.[56] The information required in the directive was to be collected in a prescribed data matrix that would have linked individual's names to their HIV status. The court ruled that Article 31(c) of the Constitution protected against the unnecessary revelation of information relating to family or private affairs of an individual.[57] The court on the matter stated that "… the right to privacy protects the very core of the personal sphere of an individual and basically envisages the right to live one's own life with minimum interference. The right also restricts the collection, use of and disclosure of private information."[58]

The court in determining whether there had been a violation of the right to privacy, adopted the test set out in the South African case of *Mistry v Interim National Medical and Dental Council of South Africa:*

> 'the Court ought to take into account the fact; (i) whether the information was obtained in an intrusive manner, (ii) whether it was about intimate aspects of an applicants' personal life; (iii) whether it involved

[56] *Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 Others v Cabinet Secretary Ministry of Health & 4 Others* [2016] EKLR.
[57] Ibid 112.
[58] Ibid 69.

> data provided by an applicant for one purpose which was then used for another purpose and (iv) whether it was disseminated to the press or the general public or persons from whom an applicant could reasonably expect that such private information would be withheld.'[59]

Citing South African jurisprudence on the right to privacy points to the influence the South African Constitution has had on developing Kenyan jurisprudence. Secondly, the decision highlights a pre-KDPA era where the courts cited the importance of regulating processing of personal information.

In making its decision against the collection of information, the court stated that the Respondents had not indicated how they would collect the information. The Respondents had not stated when the information would be collected or whether it was after consent had been obtained. The court ruled that the directive on collection of information "amounted to compulsory testing which would be a violation of the right to privacy".[60] I argue that this decision is key as it is an indication that courts will seek clarity in the way information is to be collected and justification for the collection. Such principles as I assert in this study are key to adequate data protection regulation.

2.3.8 Roshanara Ebrahim v Ashleys Kenya Limited

In *Roshanara Ebrahim* intimate images had been shared without consent.[61] The court posited that "the protection of privacy must serve a lawful purpose the preservation of the applicant's dignity in conduct that accords with the law".[62] The court stated that expectations of privacy was reasonable where one shared intimate photos in boy-girl relationship situation and that "although the photographs were not obtained in an intrusive manner, the purpose of the access by the by the friend did not include the publication thereof to third parties…".[63] In its finding the court proclaimed:

---

[59] Ibid 70; See also *Mistry v Interim National Medical and Dental Council of South Africa (1998) (4) SA 1127 (CC).*
[60] Ibid 78.
[61] *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others* [2016] eKLR
[62] Ibid 27.
[63] Ibid 29.

> 'Article 31 (c) of the Constitution provides for the right to informational privacy which includes privacy of private photographs of a person. In taking selfie nude pictures using a mobile phone or other communication gadget, a person does not thereby waive her right to privacy, she only exposes herself to the risk and danger of the photographs being transmitted to and viewed by other persons through the communication networks by unauthorised access and publication, or by authorised access but unauthorised publication.'[64]

This decision looks into where consent is key if the Petitioner's privacy is to be infringed; there ought to be justification in overrunning an individual's privacy. In this case, there was no justification to access and publish the Petitioner's photographs. The photographs were the personal information being protected.

This decision demonstrates that private actors will be taken to task for incursions they make into the right to privacy of other individuals. The decision also indicates that the actions need not be only for a commercial purpose to be questioned. Further, the decision points to the fact that consent granted on a specific issue does not equal blanket consent.

2.3.9 Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre

In *Jessicar Clarise Wanjiru,*[65] the petition involved personality rights which were defined as "the right of an individual to control the commercial use of his or her name, image, likeness, or other unequivocal aspects of one's identity."[66] Personality rights as per the court include "the right to privacy, or the right to be left alone and not have one's personality represented publicly without permission".[67]

The court asserted that photography and written articles may be used to encroach into personal life which in turn may be ground for an action for breach of privacy.[68] The court defined breach of privacy as "… when there is a disclosure of true facts to outsiders contrary

[64] Ibid 38.
[65] *Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre & 2 others* [2017] eKLR.
[66] Ibid 1.
[67] Ibid 2.
[68] Ibid 16.

to the determination and will of the person concerned. A right to privacy encompasses the competence to determine the destiny of private facts, and the individual concerned is entitled to dictate the ambit and method of disclosure of such facts."[69] The court ruled that privacy included an individual's right "to decide for themselves who should have access to their image and likeness – something that goes to the root of individual autonomy or privacy".[70]

This decision indicates that courts do recognise nuanced approaches to the right to privacy. In this case, my view is that the concept espoused by the court is control over personal information especially when the information is sought for commercial purposes in direct conflict with an individual's wishes.

2.3.10 N W R v Green Sports Africa Ltd

In *N W R,* the issue in contention was the use of minors' images to promote gambling on billboards. [71] The court in making an analysis of personality rights stated that they consist of "the right to privacy and the right of publicity". The court defined the right to privacy as "the right to keep one's image and likeness from exploitation without permission or compensation and generally applies to members of the general public".[72] One of the questions the court considered was whether there was reasonable expectation of privacy.

The court held that there was a "heightened protection afforded to the privacy rights of children".[73] Where the respondents did not seek the consent of parents when taking photos of children, they were in violation of the fundamental rights and freedoms of the children as protected under Articles 31 and 53 of the Constitution. The court in determining damages to award to the Petitioners stated:

[69] Ibid 20.
[70] Ibid 21.
[71] *N W R & another v Green Sports Africa Ltd & 4 others* [2017] eKLR.
[72] Ibid.
[73] Ibid.

> 'An award of compensation will go some distance towards vindicating the infringed constitutional right. How far it goes will depend on the circumstances, but in principle it may well not suffice. The fact that the right violated was a constitutional right adds an extra dimension to the wrong. An additional award, not necessarily of substantial size, may be needed to reflect the sense of public outrage, emphasise the importance of the constitutional right and the gravity of the breach, and deter further breaches. All these elements have a place in helping the court arrive at a reasonable award. The court must consider and have regard to all the circumstances of the case.'[74]

My argument is that this decision emphasises the need to take commercial entities into account for using personal information without justification. Courts will be keen to protect special interest groups such as children and legal justifications are fundamental in commercialisation of personal data.

2.3.11 EG v Attorney General

In EG,[75] a case that sought the decriminalisation of gay sex, the High Court had an extremely narrow view of privacy, arguing that gay sex did not fall within the purview of the right to privacy.[76] This case dealt with the privacy concepts of personhood and intimacy. The Petitioners had challenged the constitutionality of sections 162(a) (c) and 165 of the Penal Code. The provisions make it an offence to engage in same sex conduct. One of the constitutional provisions the Petitioner argued was being violated by section 162(a)(c) and 165 of the Penal Code is the right to privacy.

The court ruled that the Penal Code provisions challenged by the Petitioners did not violate the Constitution or the Petitioners' rights to dignity and privacy.[77] The justification rendered by the court was that Article 45 of the Constitution only allowed for marriage between a man and a woman and therefore the Constitution did not contemplate same sex relations.[78]

---

[74] Ibid
[75] *EG & 7 others v Attorney General; DKM & 9 others (Interested Parties); Katiba Institute & another (Amicus Curiae)* [2019] eKLR.
[76] Ibid 395.
[77] Ibid 405.
[78] Ibid 405.

How the court dealt with the *EG* case,[79] raises questions as to whether under certain circumstances the KDPA will elicit broad interpretation of the right to privacy by the courts or some courts will adopt a narrow interpretation of the right to privacy as was the case in this decision. I would argue that the court did not consider other rights that would be affected by having laws that criminalise gay sex, for example, the right to equality and freedom from discrimination enshrined set out by Article 27 of the Constitution. In addition, the right to human dignity under Article 28 of the Constitution and freedom and security of the person as protected by Article 29. Secondly, the court did not uphold the need to respect personal autonomy. Thirdly, the court did not consider the potential and actual harms in having laws that criminalise gay sex such as discrimination and emotional distress.

My submission is that the *EG* case was a decision that construed the right to privacy narrowly. The decision ought not inform future jurisprudence on the right to privacy. Courts ought to be persuaded by the jurisprudence reflected in the *Okiya Omtatah Okoiti* case discussed below that recognises interdependence of fundamental rights and freedoms and broadly interprets the right to privacy.

2.3.12 Communications Authority of Kenya v Okiya Omtatah Okoiti

The Court of Appeal in *Communications Authority of Kenya*,[80] overturned a High Court decision in *Okiya Omtatah Okoiti v Communication Authority of Kenya*.[81] The High Court petition had challenged the introduction of a Device Management System (DMS) into the networks of the telecommunication companies. The petition stated that the DMS had the capacity to access customers' information, which should only be accessed in a manner prescribed by law.

[79] *Ibid.*
[80] *Communications Authority of Kenya v Okiya Omtatah Okoiti & 8 others* [2020] eKLR.
[81] *Okiya Omtatah Okoiti V Communication Authority of Kenya & 8 Others* [2018] EKLR.

Because there was no lawful prescription regarding it, the DMS was said to be a violation of the right to privacy. The High Court agreed that the DMS violated constitutional provisions. The Court of Appeal rejected this argument asserting that the High Court did not identify the actual probable evidence that led to the conclusion that DMS would intrude on privacy and even if there were issues of concern, they were still being addressed.[82]

In my view, the Court of Appeal, while dismissing the High Court's decision, failed to articulate right to privacy principles that ought to be considered when implementing technology such as the DMS. Nonetheless, the Court of Appeal was right by finding that no evidence had been adduced to indicate breach of the right to privacy.

The High Court decision in *Okiya Omtatah Okoiti v Communication Authority of Kenya* sought to define privacy:

> 'Privacy is a fundamental human right, enshrined in numerous international human rights instruments. It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information, and association. The right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction, and liberty, a "private sphere" with or without interaction with others, free from arbitrary state intervention and from excessive unsolicited intervention by other uninvited individuals. Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.'[83]

The court argued that the individual right to privacy means that an individual needs to be able to manage their personal information and perform their personal work free from unwanted interference.[84] The right to privacy allows everyone to be alone, however, individual autonomy is conditioned by relationships with others in a society.

The High Court recognised that there were new challenges having an impact on the right to privacy. In this case, the discussion on data protection was analysed in the context of the

[82] (Note 80 above) 47.
[83] Ibid 63.
[84] Ibid 77.

global information society.[85] When information technology determines almost every aspect of individuals' lives, the court stated that it had a duty to give constitutional importance to the freedom of individuals in a networked world. According to the High Court, the Constitution protects privacy as a basic principle, but courts ought to be sensitive to the needs, opportunities, and dangers of freedom in the digital world.[86]

The High Court emphasised that data protection is one aspect of protecting an individual's right to privacy. When an individual's personal data is processed by another, there ought to be legal protection. The court identified processing of personal data as involving the collection, storage, use, and distribution of information. Data processing was a potential threat to an individual's privacy. The acquisition and disclosure of false or misleading information can lead to identity infringement.[87]

The High Court recognised emerging threats to the right to privacy and identified technology as driving the threats.[88] Due to the threats, the individual right to privacy requires that an individual ought to have control over their personal information.[89]

While the High Court decision is not binding, it is my view that it provides the more robust analysis and consideration of the right to privacy. The Court of Appeal was shallow in its consideration and analysis of the right to privacy and data protection. In the future, the Court of Appeal and perhaps the Supreme Court ought to adopt the analysis and conclusions of the High Court in relation to the right to privacy and data protection where the threat is State surveillance. Tying this to the discussions in this study on State surveillance, I would argue that potential harms caused by intrusions into privacy ought not be proven through concrete evidence as the Court of Appeal ruled. What ought to be considered is the possibility of threat of unwarranted intrusions into the right; the harms must not necessarily materialise. With privacy, once the intrusion is done, it cannot be undone.

[85] Ibid 64.
[86] Ibid.
[87] Ibid 65.
[88] Ibid 73.
[89] Ibid 74

2.3.13 PAK v Attorney General

The High Court in *PAK* proclaimed a wide view of the right to privacy.[90] One of the issues for determination before the court was whether the lack of access to safe abortion services was a violation of the right to privacy. The court in its determination stated that "forcing someone to carry an unwanted pregnancy to term, or forcing them to seek out an unsafe abortion, is a violation of their human rights, including the rights to privacy and bodily autonomy".[91] This is a progressive and purposeful interpretation of what may constitute the right to privacy as it recognises bodily autonomy. Such interpretation ought to have been adopted in *EG v Attorney General* discussed above.

2.3.14 Concluding thoughts on judicial interpretation

I find that the courts in Kenya have made progressive pronouncements to protect the right to privacy save for decisions such as *EG v The Attorney General* and the Court of Appeal in *Communications Authority of Kenya v Okiya Omtatah Okoiti*. The courts have aptly defined the boundaries of the right to privacy and embraced principles such as autonomy, consent, legitimate expectation, legitimate use of personal information, and potential harms to violation of the right to privacy. In this study I discuss these principles which are pillars to personal data protection regulation.

Privacy as defined by Kenyan courts includes several principles. First, the right to privacy is an individual right. Secondly, the right to privacy is linked to other rights such as the right to human dignity and the right to freedom from discrimination. Thirdly, the right to privacy may at times be balanced with other rights and interests such as public policy. Fourthly, limitations to the right to privacy must be justified through constitutional principles or statutory provisions. Fifthly, justifications for limiting the right to privacy do not apply in a blanket

[90] *PAK & another v Attorney General & 3 others* (Constitutional Petition E009 of 2020) [2022] KEHC 262 (KLR)
[91] Ibid 57.

manner. Sixthly, where an individual suffers harm due to incursions into their privacy, they ought to be awarded damages.

Having considered judicial interpretation of the constitutional right to privacy, in the next sections I highlight statutes that have to a certain degree provided for the protection of the right to privacy in defined contexts. This is notwithstanding the fact that the KDPA is the most comprehensive statute when it comes to the right to privacy.

2.4 Legislating privacy in Kenya

This section presents statutes that deal with an aspect of the right to privacy. The statutes are listed and described in chronological order. The statutes just like the constitutional provisions discussed above bear witness to the fact that Kenya has been experiencing continuous reinforcement of the right to privacy. The KDPA described under section 2.4.3 is the foundational statute when dealing with personal data protection.

2.4.1 HIV AIDS Prevention and Control Act

The HIV AIDS Prevention and Control Act (HAPCA) was enacted in 2006 years before promulgation of the current Constitution that provides for an individual right to privacy.[92] Section 20 of the Act provides for privacy guidelines:

(1) 'The Minister for the time being responsible for matters relating to health may, in regulations, prescribe privacy guidelines, including the use of an identifying code, relating to the recording, collecting, storing and security of information, records or forms used in respect of HIV tests and related medical assessments.

(2) No person shall record, collect, transmit or store records, information or forms in respect of HIV tests or related medical assessments of another person otherwise than in accordance with the privacy guidelines prescribed under this section.'

[92] Act No. 14 of 2006.

The privacy guidelines contemplated under section 20 of the Act are yet to be developed.[93] This is one of the first Kenyan statutes to regulate processing of specified personal information. Section 21 of the HAPCA provides for confidentiality of records while section 22 defines circumstances under which information may be disclosed. Section 22(1)(a) indicates that "no person shall disclose any information concerning the result of an HIV test or any related assessments to any other person except… with the written consent of that person".

HAPCA sets out lawful means for disclosure of information with consent being key. Section 22 provides for other reasons for disclosure of information including "for the purpose of an epidemiological study or research authorized by the Minister" and "to a court where the information contained in medical records is directly relevant to the proceedings before the court or tribunal". Section 23 provides for penalty for breach of confidentiality by stating that "a person who contravenes any of the provisions of this Part or of any guidelines prescribed hereunder commits an offence".

The HIV & AIDS Tribunal has considered the question of disclosure of information on an individual's HIV and AIDS status without consent. In *SKM v C. B. M*[94] the Tribunal stated that one ought to demonstrate how the disclosure of information was carried out.[95] The Tribunal found that there was disclosure without consent, and it awarded monetary damages to the Claimant.[96] The Tribunal also inquired into why there ought to be such protections. In *SKM v C. B. M* the tribunal stated that the "claimant suffered emotionally or psychologically as a result of the unauthorized disclosure, we find that there is sufficient evidence on record to prove that the Claimant has, directly and indirectly though her family, suffered emotionally and psychologically".[97] Similarly, in *JK v AAR Healthcare Kenya Ltd* the Tribunal considered the

[93] See A Akinyi *Laws, Policies and the Right to Privacy for People Living with HIV in Kenya* (2019) available at < Laws, Policies and the Right to Privacy for People living with HIV in Kenya (uonbi.ac.ke)> last accessed 9 March 2022 and N Sircar and A Maleche 'Assessing a Human Rights-Based Approach to HIV Testing and Partner Notification in Kenya: A Qualitative Study to Examine How Kenya's Policies and Practices Implement a Rights-Based Approach to Health' (2020) *Health and Human Rights Journal* 167 -176.
[94] *SKM v C. B. M & 3 others* [2021] eKLR.
[95] Ibid 56.
[96] Ibid 77.
[97] Ibid 78.

question of disclosure of HIV status to third parties.[98] The Tribunal was clear that a Claimant ought to prove that there has been unauthorised disclosure to third parties.[99]

HAPCA protects personal information relating to the HIV status of an individual. One may exercise their privacy rights under the Act and there is provision for the Tribunal to handle complaints on breach of confidentiality.

In my view, the HAPCA complements the provisions of the KDPA when dealing with privacy and data protection matters on an individual's HIV and AIDS status. Health status is defined as sensitive personal data under section 2 of the KDPA. Sensitive personal data requires a high level of protection as defined under Part V of the KDPA. What this means is that complaints related to the HIV status of an individual may be adjudicated under the HAPCA and the KDPA.

2.4.2 Computer Misuse and Cybercrimes Act

The Computer Misuse and Cybercrimes Act came into force in 2018; the Act provides for offences relating to computer systems.[100] The objects of the Act, under section 3, are to protect computer systems, programs, and data; prevent unauthorised use of computer systems; deal with cybercrimes; and protect the right to privacy, freedom of expression and access to information. Some of the offences created by the Act include unauthorised access, unauthorised interference, unauthorised interception, unauthorised disclosures, cyber espionage, child pornography, computer fraud, cyber harassment, identity theft, impersonation, and wrongful distribution of obscene or intimate images.

The offences cited under the Act influence the right to privacy and data protection. Section 14 of the Computer Misuse and Cybercrimes Act makes it an offence to access a computer system without authorisation. Section 16 makes it an offence to interfere with a computer

[98] *JK v AAR Healthcare Kenya Ltd* [2020] eKLR.
[99] Ibid 49.
[100] Act No 5 of 2018.

system without authorisation. Section 29 makes it a crime to engage in electronic identity theft and impersonation. Section 38 makes it an offence to fraudulently use electronic data.

Provisions of the Computer Misuse and Cybercrimes Act are key to the right privacy and data protection insofar as they relate to cybersecurity. Cybersecurity lapses may cause data breaches which may occasion loss or exposure of personal data, in effect contravening provisions of the KDPA. Section 43 of the KDPA provides for notification and communication of a personal data breach. KDPA does also have provisions for the crimes set out under the Computer Misuse and Cybercrimes Act. In my view, the Computer Misuse and Cybercrimes Act ought to be read together with the KDPA to ensure greater protection of personal data.

2.4.3 Data Protection Act

The KDPA came into force on 25 November 2019. The Act read together with Article 31 of the Constitution, forms the foundation for the right to privacy. Before its enactment, no statute comprehensively gave effect to Article 31 as legal principles on privacy could only be derived from a few provisions of select statutes and judicial decisions.

The KDPA is divided into eleven parts. Part 1 is the preliminary, Part 2 provides for the establishment of the Office of the Data Protection Commissioner, Part 3 regulates registration of data controllers and data processors, Part 4 sets out principles and obligations of personal data protection, Part 5 provides for grounds for processing sensitive personal data, Part 6 regulates transfer of personal data outside Kenya, Part 7 sets out exemptions, Part 8 provides the enforcement provisions, Part 9 is on financial provisions, Part 10 provides for enactment of regulations, and Part 11 sets out miscellaneous provisions.

Section 3 of the KDPA provides the object and purpose of the Act:

(a) 'to regulate the processing of personal data;
(b) to ensure that the processing of personal data of a data subject is guided by the principles set out in section 25;
(c) to protect the privacy of individuals;

(d) to establish the legal and institutional mechanism to protect personal data; and

(e) to provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with this Act.'

In relation to the first object and purpose, personal data under section 2 of the Act is defined as "any information relating to an identified or identifiable natural person". Section 2 further states that a data subject is "an identified or identifiable natural person who is the subject of personal data". Processing on the other hand under section 2 is defined as "any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means".

The Act identifies data controllers and data processes as engaging in personal data processing. Section 2 defines a data controller as a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data". A data processor is a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller". The import of these provisions is that the Act applies to public and private sector actors.

On the second object and purpose, section 25 of the Act outlines the principles of data protection:

'Every data controller or data processor shall ensure that personal data is—

(i) processed in accordance with the right to privacy of the data subject;

(ii) processed lawfully, fairly and in a transparent manner in relation to any data subject;

(iii) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(iv) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

(v) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;

(vi) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;

(vii) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and

(viii) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.'

Any public or private sector actor processing personal data may only do so in line with the outlined principles. Section 2.4.3.2 of this chapter delves deeper into an analysis of these principles plus lawful processing of personal data as listed under section 30 of the Act. Lawful processing relates to the circumstances under which a public or private sector actor may process personal data. Section 30 states:

(1) 'A data controller or data processor shall not process personal data, unless—
(a) the data subject consents to the processing for one or more specified purposes; or
(b) the processing is necessary—
(i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
(ii) or compliance with any legal obligation to which the controller is subject;
(iii) in order to protect the vital interests of the data subject or another natural person;
(iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(v) the performance of any task carried out by a public authority;
(vi) for the exercise, by any person in the public interest, of any other functions of a public nature;
(vii) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
(viii) for the purpose of historical, statistical, journalistic, literature and art or scientific research.'

On the third object and purpose relating to the protection of the right to privacy of individuals, section 26 of the Act expands the right to privacy by providing for the rights of data subjects:

'A data subject has a right—

(a) to be informed of the use to which their personal data is to be put;
(b) to access their personal data in custody of data controller or data processor;
(c) to object to the processing of all or part of their personal data;
(d) to correction of false or misleading data; and
(e) to deletion of false or misleading data about them.'

Section 2.4.3.1 of this chapter discusses these rights in greater detail.

In relation to the fourth object and purpose, section 5 of the Act establishes the Office of the Data Protection Commissioner as a body corporate. Section 8 lists the functions of the Office which generally are to ensure implementation and enforcement of the Act. Section 9 grants the Data Commissioner powers that include conduct of investigations, facilitation of alternative dispute resolution, and imposing administrative fines.

On the fifth object and purpose on remedies, section 56 enables an individual aggrieved by any decision made in relation to matters regulated under the Act to make a complaint to the Office of the Data Protection Commissioner. The Commissioner may issue enforcement notices as per section 58, issue administrative fines as per section 63, order for compensation of a data subject under section 65 or make other orders that would remedy the data subject's predicament. It cannot be gainsaid that there are statutory consequences for public and private sector actors who process personal data in violation of provisions of the KDPA.

To give effect to the Act, on 31 December 2021, the Cabinet Secretary, Ministry of Information, Communication, Technology, Innovation and Youth Affairs exercising powers granted under section 71 of the KDPA published three Regulations under the Act. These are the Data Protection (General) Regulations, 2021,[101] the Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021,[102] and the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.[103]

The Data Protection (General) Regulations, 2021 enable the rights of a data subject, provide for, restriction on the commercial use of data, obligations of data controllers and data processors, elements to implement data protection by design and by default, notification of personal data breaches, transfer of personal data outside Kenya, data protection impact assessment, and exemptions under the KDPA. The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021 outline the procedure for lodging, admission, and

[101] Legal Notice No. 263 of 2021.
[102] Legal Notice No. 264 of 2021.
[103] Legal Notice No. 265 of 2021.

response to complaints plus enforcement provisions. The Data Protection (Registration of Data Controllers and Data Processors) Regulations provide for registration of data controllers and data processors.

On application of the KDPA, the High Court in *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology* stated that the Act applies retrospectively, notwithstanding that the Act was enacted in November 2019.[104] On retrospective application, the court stated:

> 'Reading the preamble to the Act together with section 3 thereof on the Act's object and purpose, it is clear that the Act was intended to be retrospective to such an extent or to such a time as to cover any action taken by the state or any other entity or person that may be deemed to affect, in one way or the other, the right to privacy under Article 31(c) and (d) of the Constitution.[105]
>
> Needless to say, the need to protect the constitutional right to privacy did not arise with the enactment of the Data Protection Act; the right accrued from the moment the Constitution was promulgated.'[106]

Though an appeal lies in the Court of Appeal against the High Court decision, the reasoning of the High Court defines interpretation of the right to privacy post-promulgation of the Constitution. It is not the statutes enacted post-2010 that provide for the right, the right to privacy accrued "from the moment the Constitution was promulgated".

The KDPA amended several statutes. The Amendment to the Births and Deaths Act,[107] states that the Register of Births and Deaths in Kenya "shall be maintained in accordance with the principles of data protection set out in the Data Protection Act".[108] Section 25 of the Independent Electoral and Boundaries Commission was amended to state that "the principles of personal data protection set out in the Data Protection Act shall apply to the processing of personal data of voters…". Section 61 of the Employment Act was amended to provide the following on registers of children in employment: "where an employer maintains such a

[104] *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others Ex Parte Katiba Institute & another; Immaculate Kasait, Data Commissioner (Interested Party)* [2021] eKLR.
[105] Ibid 99.
[106] Ibid 100.
[107] Cap 149.
[108] Section 7 Births and Deaths Act, Cap 149.

register, the register shall be maintained in accordance with principles of data protection set out in the Data Protection Act".

I would argue that the KDPA amending twelve statutes to ensure conformity to data protection principles is curious. The Act would nonetheless apply to processing of personal data by individuals and entities in public and private sectors. It is not clear why Parliament sought to single out the twelve statutes. Be that as it may, the amendment provisions would be required in almost all existing statutes. Perhaps the drafters would have adopted the wording in section 7 of the Sixth Schedule of the Constitution. The wording would be to the effect that any statute in force before enactment of the KDPA would be construed in conformity with the KDPA where processing of personal data is concerned.

As the amendments to various statutes refer to principles under the KDPA and the High Court stated that the Act applies retrospectively, the sections below discuss five key aspects within the KDPA. These are data subject rights, data protection principles, lawful processing of personal data, oversight, and remedies.

2.4.3.1 Data subject rights

Section 26 of the KDPA sets out data subject rights which are an intrinsic part of Article 31 of the Constitution. Data subject rights must be taken into consideration when making incursions into an individual's right to privacy. Data subject rights under the KDPA expand the right to privacy as enshrined in the Constitution.

"One of the key objectives of data protection law is the effective and complete protection of the fundamental rights and freedoms of natural persons with respect to the processing of personal data" as was stated by the Court of Justice of the European Union in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González.*[109] To

[109] Judgment of 13. 5. 2014 — Case C-131/12, 53.

ensure effective protection, data protection laws empower data subjects to have a measure of control over how their personal data is processed; this is the essence of data subject rights.

The Council of Europe, when commenting on the Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data (Convention 108),[110] posited that the main purpose of the Convention was to enable individuals know, understand, and manage how others process their personal data. The Convention explicitly refers to the autonomy of an individual and the right to manage personal data, which derives from the dignity of the individual. Human dignity is a security measure when processing personal data so that the individual is not treated as a mere object.[111]

Despite the empowerment of an individual to manage their personal data, a paradox persists. Privacy paradox as defined by Solove is where individuals "say that they value privacy highly, yet they readily give away sensitive personal information for small discounts or tiny benefits—or sometimes for nothing at all".[112] According to Solove, individuals easily supply personal data when they perceive some measure of control, even if the control is illusory[113] but emphasises that "privacy's value involves the right to have choices and protections".[114] Due to privacy paradox, Solove argues that regulating privacy ought not just rely on individuals undertaking privacy self-management but that "privacy regulation should focus on regulating the architecture that structures the way information is used, maintained, and transferred".[115]

What Solove hints to is the fact that the focus on the right to privacy should be on the persons seeking to make incursions into the right. That is, their compliance with the constitutional right to privacy, respect of the rights of data subject, and adherence to data protection principles. Solove posits that "privacy cannot be solved at the individual level. Rights should

[110] Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, 28 January 1981, ETS 108.
[111] CETS "Explanatory Report of Convention 108 as modified by the amending Protocol. Council of Europe Treaty Series - No. 22" < CETS 223 - Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (coe.int)> 10.
[112] D Solove 'The Myth of the Privacy Paradox' (2021) *The George Washington Law Review* 2.
[113] Ibid 17.
[114] Ibid 24.
[115] Ibid 6.

certainly be part of privacy laws, but they can only play a small supportive role. Meaningful protection must be large-scale and structural in nature."[116] Simply, a balance between individual rights and constitutional obligations of those who wish to make incursions into the right to privacy.

As Solove argues, there is need for data subject rights that limit the power of government and companies,[117] ensure respect for individuals,[118] maintain appropriate social boundaries,[119] create trust,[120] allow the individual control over their life,[121] and offer protection of intimacy, bodies, and sexuality.[122] Data subject rights provide people with "notices, rights, and choices".[123] My view of Solove's reflections is that for data subject rights to be meaningful, the data subject ought to be informed of their rights, the effects of the rights, how to exercise the rights, and circumstances under which the rights might not operate. Empowerment of an individual in relation to their rights is critical. However, privacy self-management assumes that the individual can always self-manage.

With the KDPA being a fairly new statute and the fact that the Regulations under the Act were published at the end of December 2021, the rights of data subjects under the Act have not been subjected to robust litigation, adjudication by the Office of the Data Protection Commissioner, or interpretation by the Courts. In view of Solove's reflections, the personal data ecosystem ought to first create a culture of respecting, protecting, and promoting data subject rights. Data controllers and data processors must comply with Article 31 of the Constitution and the KDPA.

[116] D Solove 'The Limitations of Privacy Rights' (2021) *George Washington Law Review* 50.
[117] D Solove (note 112 above) 38.
[118] Ibid.
[119] Ibid 39.
[120] Ibid.
[121] Ibid.
[122] Ibid.
[123] Ibid 49.

Where it is argued that the rights of data subjects are not comprehensive enough, the Office of the Data Protection Commissioner and the Courts in interpreting the rights ought to be guided by Article 20(3) of the Kenyan Constitution:

> 'in applying a provision of the Bill of Rights, a court shall –
>
> (a) develop the law to the extent that it does not give effect to a right or fundamental freedom; and
> (b) adopt the interpretation that most favours the enforcement of a right or fundamental freedom.'

2.4.3.2 Data protection principles and lawful processing of personal data

Legitimate or lawful reasons for making incursions into an individual's right to privacy ought to be clearly set out in law. The statutory model ought to be that processing of personal data is permissible if it fits within identified legitimate or legal purposes. Data protection principles set the optimum standard that ought to be complied with where the right to privacy and data protection are at risk.[124] As per Hert, "principles can bridge differences in legal regimes and pave the way for common understanding of things (and eventually more common rules)".[125] Hert posits that "principles carry the data protection architecture. They are intended to be all-encompassing, abstract, and omnipresent throughout the text. They make data protection robust and time-resistant".[126]

Data protection principles are the guiding light in processing of personal data; they offer the vision of the right to privacy and the bare minimum that must be met by anyone processing personal data. On data protection principles, Scassa cites "control and consent; transparency, portability and interoperability; and strong enforcement and real accountability" as matters that should be provided for in a data protection statute.'[127] Scassa makes a link between privacy and other rights and freedoms, and argues that the individual right to privacy "must

---

[124] P De Hert 'Data Protection as Bundles of Principles, General Rights, Concrete Subjective Rights and Rules: Piercing the Veil of Stability Surrounding the Principles of Data Protection' (2017) *European Data Protection Law Review* 167, 168.
[125] Ibid 169.
[126] Ibid 175.
[127] T Scassa 'A Human Rights-Bases Approach to Data Protection in Canada' (2020) in E. Dubois and F Martin-Bariteau (eds.) *Citizenship in a Connected Canada: A Research and Policy* Agenda 2.

be supported by legislation that renders the right effective and realizable".[128] Scassa argues that "legitimate interest" as the basis for processing of personal data "must be weighed against the human rights of affected individuals and will only be justified where the impact on those human rights is not disproportionate to the goals sought to be obtained".[129]

The rights of a data subject, principles of data protection, and lawful processing are meant accord individuals privacy self-management. Scassa asserts that privacy self-management is achieved when individuals are granted express rights regarding their personal data. These rights include a right to opt out of data sharing, a right to notice, and a right to delete.[130] Self-management should not be illusory. Individuals ought to have statutory powers to act against natural and legal persons that wish to collect personal data.[131] As I have stated in the previous section, self-management ought to operate in a data processing ecosystem that respects, protects, and promotes data subject rights.

Roos, in analysing data protection laws from around the world before POPIA was enacted in South Africa, identified several data protection principles that must feature in a data protection statute.[132] These are fair and lawful processing,[133] purpose specification,[134] minimality,[135] quality,[136] openness and transparency,[137] data subject participation,[138] sensitivity,[139] security and confidentiality,[140] accountability,[141] plus exceptions and exemptions.[142] In discussing these principles, Roos is of the view that:

---

[128] Ibid 5.
[129] Ibid 6.
[130] Ibid 46.
[131] Ibid.
[132] A Roos 'Core principles of data protection law' (2006) *The Comparative and International Law Journal of Southern Africa* 103 -130.
[133] Ibid 108. See also A Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (2003) LLD Thesis.
[134] Ibid 111.
[135] Ibid 113.
[136] Ibid 114.
[137] Ibid 116.
[138] Ibid 119.
[139] Ibid 122.
[140] Ibid 124.
[141] Ibid 126.
[142] Ibid 127.

> 'despite differences in language, legal traditions and cultural and social values, there has been a broad measure of agreement on the basic principles that should be embodied in data protection legislation. These data protection principles should be reflected in a South African data protection law.'[143]

What Roos posits is that there is need for uniformity in the text of data protection laws, especially on the aspect of data protection principles. In Kenya, data protection principles are crystalised under section 25 of the KDPA.

The KDPA does not provide for security as an explicitly stated principle. Applying Roos'[144] essential data protection principles listed above, my conclusion is that the lack of "security" as a data protection principle in the KDPA is a regrettable omission. In practice, the lack of the security principle might be construed by data controllers, data processors, the Office of the Data Protection Commissioner, and the Courts to be of diminished importance, while in truth, it is a principle of global importance.

In addition to data subject rights and data protection principles, the right to privacy is enhanced by the KDPA providing for situations where lawful processing of personal data may take place. Section 30 of the Act sets out lawful processing of personal data.

Section 30(1)(b)(v) of the KDPA has a peculiar provision which states that "a data controller or data processor shall not process personal data, unless the processing is necessary the performance of any task carried out by a public authority". The use of the words "the performance of any task carried out by a public authority" is problematic in my view. The Act does not define what "any task" would entail, nor when processing would be "necessary". The Act does not define a "public authority".

I posit that broad and vague statutory provisions have the potential effect of unnecessarily limiting fundamental rights and freedoms. In section 3.5.2 below I discuss vagueness in statutory provisions in greater detail. The State seems to be given a tremendous amount of latitude in processing personal data of individuals by section 30(1)(b)(v) of the KDPA which

[143] Ibid 130.
[144] Ibid.

brings about aspects of ambiguity, vagueness, and broadness in statutes affecting fundamental rights and freedoms.

2.4.3.3 Oversight and remedies

In line with section 8 of the KDPA, oversight is undertaken by the Office of the Data Protection Commissioner. Ideally, the Office must be independent. Sajo argues that independence of independent authorities is tied to their "distance from constitutionally recognized branches of power". [145] Independence of these authorities speaks to the integrity of the service which the independent authority renders.[146] According to Sajo, "appointment, dismissal, qualification, fixed term, conflict of interest rules (*incompatibilite*) of commissioners and other independent authority leaders are considered fundamental guarantees of authority independence".[147] Independence is not absolute as the independent authorities ought to be subject to oversight from institutions such as Parliament and the courts.[148] Parliament and the courts may however, only undertake oversight within their constitutional mandates and powers.[149] Oversight does not mean receiving order or instructions from organs of the State or even private entities.[150]

There ought to be effective remedies for personal data protection violations. Article 8 of the Universal Declaration of Human Rights (UDHR) provides for a right to an effective remedy[151] and so does Article 2(3) of the International Covenant on Civil and Political Rights (ICCPR).[152] An effective remedy according to the UDHR and ICCPR has four components. First, there ought to be a violation of a fundamental right that is recognised by law. Secondly, there ought to be a remedy

[145] A Sajo, 'Independent Regulatory Authorities as Constitutional Actors: A Comparative Perspective' (2007) *Annales Universitatis Scientiarum Budapestinensis de Rolando Eotvos Nominatae* 14.
[146] Ibid.
[147] Ibid.
[148] Ibid 13, 24.
[149] Ibid 24. See also Case Law (note 31 above) 1822.
[150] Ibid.
[151] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).
[152] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.

for the violation. Thirdly, the determination of the remedy is to be undertaken by a competent authority. Fourthly, the remedy should be enforced by competent authorities once it is granted.

Varuhas and Moreham posit that "remedies make rights real in practice for plaintiffs. They can provide redress and solace, punish, and condemn outrageous violations, potentially deter future harmful conduct, and vindicate interests that are of importance to individuals and society as a whole".[153] Varuhas and Morenham argue that remedies ought to be tethered to the norms they relate to, that is remedies cannot be divorced from the rights they are tied to.[154]

In chapter 6 of this study, I interrogate the oversight role of the Office of the Data Protection Commissioner. I also discuss the need for availability of effective remedies under the KDPA.

2.4.4 Children Act

The recently enacted Children Act[155] is the latest statute to have provisions on the right to privacy. Section 19 of the repealed Children Act on the right to privacy stated that "every child shall have the right to privacy subject to parental guidance".[156] The recently enacted Children Act gives "effect to Article 53 of the Constitution", it makes provision for children rights, and parental responsibility. This Act was drafted over the backdrop of the KDPA. On data protection, section 33 in regulating the processing of personal data of children:

(1) 'Every data controller or data processor shall not process personal data relating to a child unless—
   (a) consent is given by the child's parent or guardian; and
   (b) the processing is in such a manner that protects and advances the rights and best interests of the child.
(2) A data controller or data processor shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child.
(3) Mechanisms contemplated under sub-section (2) shall be determined on the basis of—

[153] J Varuhas and N Moreham 'Remedies for Breach of Privacy' in J Varuhas and N Moreham(eds.) *Remedies for Breach of Privacy* (Kindle edn 2018) Ch 1.
[154] Ibid.
[155] Act No. 29 of 2022.
[156] Act No. 8 of 2001.

(a) available technology;

(b) volume of personal data processed;

(c) proportion of such personal data likely to be that of a child;

(d) possibility of harm to a child arising out of processing of personal data; and

(e) such other factors as may be specified by the Data Commissioner.

(4) A data controller or data processor that exclusively provides counselling or child protection services to a child may not be required to obtain parental consent as set out under sub-section (1). '

On the right to privacy of a child, section 27 of the Children Act:

(1) 'No person shall subject a child to arbitrary or unlawful interference with his or her privacy, family or private affairs, or correspondence, or to attacks upon his or her honour or reputation.
(2) Without prejudice to the generality of subsection (1), parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children.
(3) The personal data concerning a child shall be processed only in accordance with the provisions of the Data Protection Act.'

The Children Act makes other specific provisions on the privacy of a child. Section 16(3) on right to health care states that "in pursuance of the right to healthcare services under this section, every child has the right to privacy and a child-friendly environment". Section 26(6) on detention of children in conflict with the law provides that "the competent authorities shall take appropriate measures to facilitate humane treatment and respect for the privacy, legal capacity and inherent human dignity of children deprived of liberty, including children with disabilities". Section 94 indicates that proceedings relating to children should ensure privacy. Section 220(1) provides that a "child offender has the right to privacy during arrest, the investigation of the offence and at any other stage of the cause of the matter". Section 235(g) provides that "every child accused of having violated any rule of law shall— have his or her privacy respected at all stages of the proceedings".

What is apparent from the provisions of the Children Act in comparison to the KDPA is that the Children Act focuses on the general right to privacy of a child while the KDPA is specific to data protection for a child. Section 27(3) of the Children Act even states that personal data

relating to children shall be processed in accordance with the KDPA. There is a synergetic relationship between the two statutes. One issue that is common in the two statutes is the role of parents and legal guardians. A child's right to privacy is exercised subject to parental guidance.

Gligorijević, on parental consent and guidance, argues that "a child's human right to privacy should not be rendered conditional upon another's wishes and behaviour, or control and consent".[157] Gligorijević contends that while a parent may have control over a child's privacy, courts ought to consider the best interests of the child.[158] Secondly, Gligorijević argues that courts should specifically inquire into the harms that may be occasioned on a child if their right to privacy is violated whether or not parental control and consent has been exercised.[159] In the Kenyan context, Article 53(1)(e) of the Kenyan Constitution read together with the Children Act provide for parental care and protection unless such care and protection occasions harms on a child.

I associate myself with Gligorijević's proposals on how to deal with privacy questions relating to a child. Where a parent exercises parental control and consent, there is an assumption that the parent making decisions on behalf of the child understands the parameters within which the right to privacy may operate. On a child's right to privacy, the courts ought to inquire into whether the parent was empowered to make the right call. When considering a child's data protection rights, the Children Act ought to be read together with the KDPA.

2.4.5 Subsidiary legislation and guidelines

On subsidiary legislation and guidelines, Rule 7 of the Law Society of Kenya Code of Conduct and Ethics for Advocates:

[157] J Gligorijević 'Children's privacy: the role of parental control and consent' (2019) *Human Rights Law Review* 201-229.
[158] Ibid 210.
[159] Ibid 212.

> 'Communication between the Advocate and client is protected by the rule on confidentiality of Advocate-client communication. The Advocate has a duty to keep confidential the information received from and advice given to the client. Unauthorized disclosure of client confidential information is professional misconduct. At the same time the Advocate has a duty to safeguard against the abuse of Advocate-client confidentiality to perpetrate illegal activity.'[160]

Clause 4.2.5 of the Central Bank of Kenya Prudential Guidelines for Institutions Licensed Under the Banking Act[161] on confidentiality:

> 'Confidentiality of relations and dealings between the institution and its customers is paramount in maintaining the institution's reputation. Thus directors, chief executive officers and management must take precaution to protect the confidentiality of customer information and transactions. No member of staff or director should during, or upon and after termination of employment with the institution (except in the proper course of his duty and or with the institution's written consent) divulge or make use of any secrets, copyright material, or any correspondence, accounts of the institution or its customers. No employee or director shall in any way use information so obtained for financial gain.'

Clause 14 of the Code of Conduct for the Practice of Journalism under the Media Council Act[162] guides journalists when carrying out their journalistic duties:

(1) 'The public's right to know shall be weighed against the privacy rights of people in the news.
(2) Journalists shall stick to the issues.
(3) Intrusion and inquiries into an individual's private life without the person's consent are not generally acceptable unless public interest is involved. Public interest shall itself be legitimate and not merely prurient or morbid curiosity.
(4) Things concerning a person's home, family, religion, tribe, health, sexuality, personal life and private affairs are covered by the concept of privacy except where these impinge upon the public.'

The Law Society of Kenya Code of Conduct, Central Bank of Kenya guidelines, and the Code of Conduct for the Practice of Journalism just like the Children Act and HIV AIDS and Control Act again point to the fact that elements of the right to privacy have been practiced in Kenya

[160] Law Society of Kenya "Code of Standards of Professional Practice and Ethical Conduct (June 2016)" < https://lsk.or.ke/Downloads/LSK%20CODE%20OF%20STANDARDS%20OF%20PROFESSIONAL%20PRACTICE%20AND%20ETHICAL%20CONDUCT%20FINAL%20VERSION.pdf> last accessed 25th July 2021.
[161] Central Bank of Kenya Prudential Guidelines January 2013.
[162] Act No. 46 of 2013.

for a long period of time. Such subsidiary legislation and guidelines work to complement provisions of the KDPA.

As some statutes discussed above promote the right to privacy, some limit the right. I discuss statutes that limit privacy in the next section.

2.5 Legislation limiting the right to privacy

Article 24 of the Kenyan Constitution allows for limitation of fundamental rights and freedoms:

> 'A right or fundamental freedom in the Bill of Rights shall not be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including—
>
> (a) the nature of the right or fundamental freedom;
>
> (b) the importance of the purpose of the limitation;
>
> (c) the nature and extent of the limitation;
>
> (d) the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others; and
>
> (e) the relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose.'

Article 24(2) states that legislation limiting a fundamental right or freedom "is not valid unless the legislation specifically expresses the intention to limit that right or fundamental freedom, and the nature and extent of the limitation"; is not valid "unless the provision is clear and specific about the right or freedom to be limited and the nature and extent of the limitation"; and "shall not limit the right or fundamental freedom so far as to derogate from its core or essential content". Article 24(3) declares that "the State or a person seeking to justify a particular limitation shall demonstrate to the court, tribunal or other authority that the

requirements of this Article have been satisfied". The statutes I discuss below limit the right to privacy.

2.5.1 Registration of Persons Act

One of the statutory provisions limiting privacy is section 9A of the Registration of Persons Act which provides for the National Integrated Identity Management System (NIIMS).[163] The section provides for digital identity cards for all Kenyans and for sweeping changes to citizen registration; migrating it to a digital platform. The reason for section 9A is the creation of a national digital identity card. The digital identity programme was challenged in court.

Courts maintained that the State did not pay attention to the right to privacy, it did not comply with privacy and data protection principles and was not compliant with legal provisions for legitimate use of personal information. The High Court in *Nubian Rights Forum v Attorney General*, while examining issues raised by the petitioners, ruled that the State is at liberty to proceed with the implementation of NIIMS and to process and utilize the data collected in NIIMS, on condition that an appropriate and comprehensive regulatory framework on the implementation of NIIMS that is compliant with Article 31 of the Constitution was enacted.[164] The court identified the need for data protection laws in Kenya. The court also made a declaration that "the collection of DNA and GPS co-ordinates for purposes of identification is intrusive and unnecessary, and to the extent that it is not authorised and specifically anchored in empowering legislation, it is unconstitutional and a violation of Article 31 of the Constitution."[165]

The digital identity cards rollout was also challenged in *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology.*[166] In this case, the

[163] Cap 107 Laws of Kenya.
[164] *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (*Interested Parties) [2020] eKLR.
[165] Ibid 1047.
[166] (Note 104 above).

Petitioners had argued that before the digital identity cards rollout, the government ought to have carried out a data protection impact assessment. In making its decision, the court made two key pronouncements that have an impact on the promotion, protection, and respect of the right to privacy and personal data protection. First, the Court ruled that notwithstanding the fact that the KDPA was enacted in November 2019, it had retrospective application. Secondly, the court ruled that before the State could roll out the digital identity cards, it ought to have carried out a data protection impact assessment.

In conclusion, the court ordered the State to halt the roll out of the digital identity cards and conduct a data protection impact assessment. What is precedent setting in this decision is the pronouncement on the importance of the right to privacy. Secondly, that the KDPA has retrospective application which commences from the date of the promulgation of the Constitution. The government has since appealed this decision at the Court of Appeal; the court is yet to render its decision on the matter.

In my view, the decision by the High Court is a welcome one. It demonstrates that the courts may be persuaded to uphold the right to privacy. The decision points to the requirement that any incursions into the right to privacy where personal data is concerned should be undertaken within the framework of the KDPA. In the NIIMS case, while provision of digital identity cards may be necessary in incorporating technology with the right to an identity, the limitation to the right to privacy that allows this must be exercised cautiously bearing in mind data subject rights and data protection principles.

2.5.2 National Intelligence Service Act and National Police Service Act

On surveillance, the long title of the National Intelligence Service Act[167] provides that the National Intelligence Service is responsible for security intelligence and counterintelligence to enhance national security in accordance with the Constitution. The National Intelligence Service is to "gather, collect, analyse, and transmit or share with the relevant State agencies,

[167] Act No. 28 of 2012.

security intelligence and counterintelligence". The Service has the power to investigate, gather, collate, correlate, evaluate, interpret, disseminate, and store information, which is relevant in the performance of its functions, under the Act, whether within or outside Kenya.

The National Intelligence Service Act is one of the statutes that provides the State with powers to process personal data and carry out surveillance, in effect limiting the right to privacy and data protection. Specifically, section 36(1) of the National Intelligence Service Act states:

> 'the right to privacy set out in Article 31 of the Constitution, may be limited in respect of a person who is subject to investigation by the Service or suspected to have committed an offence to the extent that subject to section 42, the privacy of a person's communications may be investigated, monitored or otherwise interfered with.'

Further on State surveillance, the National Police Service Act, establishes the Police Service with one of its functions being collection of criminal intelligence.[168] Article 24(5) of the Constitution provides that "provision in legislation may limit the application of the rights or fundamental freedoms in the following provisions to persons serving in the Kenya Defence Forces or the National Police Service—(a) Article 31—Privacy". To this end, section 47(3) of the National Police Service Act provides that for persons subject to the Act, their right to privacy may be limited. The justification in the Act is pronounced under section 47(2):

> (a) 'the protection of classified information;
> (b) the maintenance and preservation of national security;
> (c) the security and safety of officers of the Service;
> (d) the independence and integrity of the Service; and
> (e) the enjoyment of the rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others.'

Section 48 of the Kenya Defence Forces Act also limits the right to privacy.[169] The justification as set out under section 43(2) of the Act is to ensure:

> (a) 'the defence and protection of the sovereignty and territorial integrity of the Republic of Kenya;

[168] Cap 84 Laws of Kenya.
[169] Act No. 25 of 2012.

(b) the protection of classified information;
(c) the maintenance and preservation of national security;
(d) the security and safety of members of the Defence Forces;
(e) that the enjoyment of the rights and fundamental freedoms by any individual member of the Defence Forces does not prejudice the rights and fundamental freedoms of any other individual member of the Defence Forces;
(f) good order and service discipline; and
(g) public health and safety.'

The National Police Service Act and the Kenya Defence Forces Act are the only statutes within Kenya's legal system that expressly provide for limitation of the right to privacy. The two statutes are instrumental in illustrating statutory provisions that provide justifications for incursions into fundamental rights and freedoms.

The functions of the National Intelligence Service and the National Police Service necessitate processing of personal data. The two institutions ought to respect the right to privacy and process personal data in compliance with the KDPA. The KDPA creates a link between the National Intelligence Service Act, the National Police Service Act, and the Office of the Data Protection Commissioner. Section 8(2) of the KDPA provides that the "Office of the Data Commissioner may, in performance of its functions collaborate with national security organs". Article 239 of the Constitution lists the national security organs as, the National Police Service, the National Intelligence Service, and the Kenya Defence Forces.

The KDPA does not define the nature of the collaboration that is to take place between the Office of the Data Commissioner and the national security organs. I would argue that without clarity, the provision is overly broad and vague and ought not be operationalised.

Section 51(2)(b) of the KDPA on national security states that processing of personal data is exempt from the provisions of the act "if it is necessary for national security". There is no definition of what amounts to national security under the KDPA. My submission is that there ought to be no room for ambiguous, vague, and broad legal provisions that allow for arbitrary incursions into the right to privacy and data protection.

Provisions of the National Intelligence Service Act, National Police Service Act, and the KDPA bring to question the adequacy of personal data regulation in Kenya especially where State surveillance is concerned. The adequacy will be discussed in depth in chapter four of this study.

2.5.3 Private Security Regulation Act

The Private Security Regulation Act's purpose is to regulate the private security industry and to provide for a framework for cooperation with the Kenya Defence Forces, the National Security Intelligence Service, and the National Police Service.[170] Section 47 of the Act provides for the power of search for private security providers:

(1) 'A private security service provider, a security guard or security officer manning a building or responsible for any property may search a person on entry or exit of that building or property without a warrant.
(2) In the exercise of the power to search under subsection (1), a private security service provider, a security guard or a security officer shall not infringe on any right or fundamental freedom of an individual under the Constitution.
(3) The power to search under subsection (1) shall be exercised responsibly and shall be subject to any other written law.
(4) A private security service provider, a security guard or security guard who violates an individual right or fundamental freedom in exercise of the right to search under this section commits an offence and shall in addition to cancellation of licence, be liable on conviction to the penalty prescribed under this Act or any other written law whichever is higher.
(5) The Cabinet Secretary shall, within three months of the commencement of this Act, make regulations generally to provide for the responsible exercise of the power of search granted under this section.'

Section 48 on the power to record and temporarily withhold identification documents:

(1) 'At the entry of any premises or property within the jurisdiction and care of a private security service provider, a security guard or a security officer, the private security service provider, security guard or officer may request a person to identify themselves, register the time of entrance and exit of the person and retain temporarily the identification document of such person.

[170] Act No. 13 of 2016.

(2) The identification document surrendered under subsection (1) shall—
    (a) be given back to the person at the point of exit;
    (b) not be used for any other purpose save for identification;
    (c) be kept in safe custody until given back to the owner.
(3) Subject to section 45, any information obtained in the registration of a person under subsection (1) shall not be used for any other purposes save for identification of the person.
(4) The Cabinet Secretary shall make regulations generally to give full effect to this section.
(5) A person who violates any provision of this section or any regulations made thereunder commits an offence and shall be liable on conviction to a penalty prescribed under this Act.'

This statue is problematic in that is give broad powers to private security providers to make incursions into an individual's right to privacy. Private security providers may use the personal data collected for commercial purposes, an abuse of data protection principles and data subject rights. Private security providers will seek to rely on section 30(1)(b)(ii) of the KDPA that states that "a data controller or data processor shall not process personal data unless the processing is necessary for compliance with any legal obligations to which the controller is subject".

As private security providers rely on section 30(1)(b)(ii) of the KDPA, they ought to pay attention to principles of data protection under section 25 of the Act, ensure rights of data subjects are respected and protected as per section 26, and if they are to use personal data collected for commercial purposes, they must comply with section 37 of the Act that requires express consent from data subjects.

2.5.4 Other statutes

The Health Act[171] mandates the national government to formulate policy promoting disease surveillance in connection with the prevention of environmental, food, water, and sanitation

[171] Act No. 21 of 2017.

related diseases.[172] The Kenya Citizenship and Immigration Act,[173] the Refugees Act,[174] and the Statistics Act[175] have provisions that require information from an individual and in effect allowing for intrusions into the privacy of persons and mass personal data collection. Statutory justifications ought to be within constitutional guidelines on limitation of fundamental rights and freedoms, data protection principles and data subject rights set out in the KDPA.

2.5.5 Concluding thoughts on statutes

The highlights of the statutes mentioned in this part indicate that there is a data protection regulation in Kenya. Court decisions have affirmed the KDPA as foundational statute in personal data processing by public and private sector actors. The discussion above has shown that the HIV and AIDS Prevention and Control Act, the Computer Misuse and Cybercrimes Act, and the Children Act have provisions that complement application of the KDPA.

On the other hand, the Registration of Persons Act, the National Intelligence Service Act, the National Police Service Act, and the Private Security Regulation Act have provisions that may limit the right to privacy and the application of the KDPA. The vague and overly broad provisions in the KDPA on national security and collaboration between the Office of the Data Protection Commissioner and national security organs are problematic. This is subject for discussion in later chapters of this study.

[172] Section 69, Health Act.
[173] Parts III, IV, V, VI, VII and VII, Kenya Citizenship and Immigration Act, Act No 12 of 2011.
[174] Section 26, Refugees Act, Act No. 13 of 2006.
[175] Part II, Statistics Act, Cap 112 Laws of Kenya.

2.6 Conclusion

My focus in this chapter was to describe how the right to privacy has been structured within the Kenyan legal system. The independence and post-independence constitutional text provided for the right to privacy on an individual's home and property. The texts indicated the need for consent, justification for violating the right, and situations where the right could be limited. However, the texts did not provide for an express individual right to privacy. It was not until the promulgation of the Constitution of Kenya, 2010 that the individual right to privacy was a right enshrined in the constitutional text.

On jurisprudence, the highlights I have submitted demonstrate that the courts have considerably ruled in favour of respect, protection, and promotion of the right to privacy. The jurisprudence also indicates that the courts will interrogate action by State and non-State actors. In relation to effective remedies, I argue that the jurisprudence reveals a disjointed approach by the courts in considering damages for breach of the right to privacy and data protection.

In addition to the constitutional texts, in this chapter, I have highlighted legislation that provides for privacy rights or elements of the rights. One of these is the KDPA enacted in November 2019, which the courts declared as having retrospective application from the date the Constitution was promulgated. The KDPA provides a framework to inquire into the adequacy of data protection regulations. The Act unpacks the right to privacy by providing for data subject rights, data protection principles, legitimate processing of personal data and oversight by the Office of the Data Protection Commissioner.

The major challenge is that the KDPA being a fairly new statute has not been subject to robust interpretation by the courts. I find that the KDPA has vague provisions that may undermine the right to privacy. To this extent and in consideration of jurisprudence from the Kenyan courts, vague and overly broad provisions of the KDPA ought not to apply. Two provisions that I identified to be vague and overly broad are the provision on tasks by a public authority

constituting legitimate personal data processing and the collaboration between the Office of the Data Protection Commissioner and national security organs.

In this chapter I highlighted provisions of the Children Act, the HIV and AIDS Control and Prevention Act that have express right to privacy and confidentiality elements. Provisions of the HIV and AIDS and Control Act have been subject to disputes considered by the HIV & AIDS Tribunal. The Tribunal often ruling in favour of confidentiality of HIV and AIDS status information and requiring complainants to prove breaches against their confidentiality rights and that they have suffered actual harm in the process. These Acts, read together with the KDPA ensure comprehensive protection of the right to privacy and data protection.

The Registration of Persons Act, the National Intelligence Service Act, the National Police Service Act, and the Private Security Regulation Act were featured as statutes that limit the right to privacy. The National Police Service Act and the Kenya Defence Forces Act expressly limit the right to privacy for individuals who are regulated under the two statutes. In this study, I use these Acts to interrogate State surveillance processing of personal data.

With the historical account in this chapter, I have painted a picture of the past and present status of the right to privacy and data protection. Borrowing from Boorstin, it is evident that past regulation of the right to privacy and data protection inform the status of the law today.[176] As this study is about the adequacy of data protection regulation in Kenya, this chapter lays the foundation from which adequacy may be determined.

Statutes and regulations I have highlighted will be interrogated in subsequent chapters of this study to determine whether they are adequate, and I shall propose law reforms in data protection regulation where the statutes fall short. To recall Dubber, the future is recalibrated using an understanding of the past and present.[177] Before interrogating adequacy and seeking a recalibration of the law, in the next chapter I propose the framework to be used in determining adequacy of data protection regulation in Kenya.

[176] Boorstin (note 5 above).
[177] Dubber (note 6 above).

CHAPTER THREE: A FRAMEWORK TO DETERMINE ADEQUACY

3.1 Introduction

In chapter two, I called attention to the evolution of the right to privacy and data protection in Kenya. I pointed out legislation that protects and limits the right to privacy and data protection. With the background set out in chapter two, the question that I pose in this study is whether the cited data protection framework provides adequate protection to a data subject. However, before determining the level of adequacy, the question that arises is, what framework may be used to determine adequacy of data protection regulation?

No robust study has been carried out to interrogate whether data protection regulation in Kenya is adequate. Were such a study to be carried out, the challenge is, what objective framework would be ideal to determine adequacy? In view of this dilemma, in this chapter I propose an objective framework which will first serve as a guide for introspection into Kenya's data protection regulation. Secondly, the framework may be used to assess adequacy of countries where Kenya exports personal data to. Thirdly, responses to the framework will provide the minimum standard for adequacy of personal data protection.

On adequacy, from the outset, it is key to note that the KDPA does not have provisions to guide determination of the adequacy of another country's data protection regulation. Section 48 of the KDPA provides:

> 'A data controller or data processor may transfer personal data to another country only where –
>
> (a) the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;
> (b) the data controller or data processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;
> (c) the transfer is necessary—

(i) for the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures taken at the data subject's request;

(ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

(iii) for any matter of public interest; for the establishment, exercise or defence of a legal claim;

(v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or

(vi) for the purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects.'

In view of the above provision, it is not clear what specific and objective criteria data controllers or data processors would adopt to determine whether jurisdictions they are transferring personal data to have data protection laws commensurate to the Kenyan law. Even so, and before delving into such determination, the issue I raise in this study is whether the Kenyan framework is itself adequate to be used as a benchmark to determine the adequacy of other countries.

Before proposing a determination-of-adequacy framework, in the section 3.2 below, I examine determination-of-adequacy under the GDPR. The GDPR offers means to determine adequacy which I argue is overly broad and does not provide a nuanced, more concrete, and practical approach to determining adequacy. It is for this reason I define my own determination-of-adequacy framework in section 3.3 of this chapter. In section 3.4, I identify natural and legal persons that should be regulated by law in relation to data protection. I delve into the concept of power asymmetry between the identified actors with a mention of State surveillance but with a focus on surveillance capitalism. In section 3.5, I emphasize the need for the law to have explicit and specified purposes for data protection and personal data processing. I indicate the importance of considering liberty principles and harms caused by personal data processing. In section 3.6, I discuss the kind of data that should be regulated by law. In section 3.7, I highlight instances where it is appropriate to process personal data. In section 3.8, I discuss jurisdictional issues in data protection regulation. In section 3.9, I discuss

how personal data is processed, how oversight might be undertaken, and how effective remedies may be accessed.

3.2 Adequacy determination under the GDPR

Article 45(2) of the GDPR provides pointers as to what should be considered when assessing the adequacy of the level of data protection for a country that imports personal data of persons within the European Union.[1] Article 45(2) states that the European Commission is to take account of:

> '(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
>
> (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.'

The European Commission has used the above parameters to recognise "Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey,

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, and Uruguay" as providing protection of personal data that is similar to the GDPR.[2]

Before the GDPR, the Working Party on the Protection of Individuals with regard to the Processing of Personal Data indicated that to determine adequacy, there was need to have "a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate".[3] The Working Party proposed content principles that included purpose limitation, data quality, proportionality, transparency, security, rights of access, rectification, opposition, restriction of onward transfers, direct marketing, and automated decision making.[4] The Working Party also proposed procedural and enforcement mechanisms that included good level of compliance, support to data subjects, and appropriate redress.[5]

In my view, the Working Party list and the GDPR provide a starting point when interrogating adequacy as a broad concept, not only limited to whether another jurisdiction provides adequate data protection regulation. Indeed, this starting point may be useful for countries interested in doing critical introspection about the adequacy of their own data protection laws. They point us in the right direction that, at the very least, when determining adequacy, one should examine international obligations, general and sectoral legislation, data protection principles, data subject rights, access to remedies, enforcement mechanisms, and existence of functioning independent regulatory authorities.

The challenge with the Working Party list is that, just like the GDPR, they are overly broad and do not provide a nuanced, more concrete, and practical approach to determining adequacy. My submission in this study is that a refined and structured determination-of-adequacy framework can be crafted; the Working Party list and the GDPR provide the backdrop.

---

[2] European Commission "Adequacy Decisions" Adequacy decisions | European Commission (europa.eu) last accessed 18 August 2022.

[3] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Working Document Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive Adopted by the Working Party on 24 July 1998 5.

[4] Ibid 5, 6.

[5] Ibid 7.

A refined and structured determination-of-adequacy framework is critical for States to conduct a critical self-assessment of their own data protection laws. As Roth points out, the determination-of-adequacy under the GDPR is not formulated with precision.[6] Adequacy decisions in the EU, according to Roth, have political undertones which indicates a fluidity in making determinations.[7] Lekubu asserts that the GDPR does not provide a "definitive checklist" that one may use to determine whether a country's data protection regulation measures up to the GDPR.[8] As such, the GDPR principles on adequacy are not particularly practically useful for states intending to assess the adequacy of their own data protection laws. Nonetheless, my view is that the GDPR offers political and doctrinal aspects of determining adequacy.

I submit that the determination-of-adequacy must be specific and concrete, providing a definitive checklist. It is also key to note that the determination-of-adequacy is a continuing process that requires continuous monitoring by the institution making the determination.[9] Hence, there is need for a nuanced framework like the one I propose in this study. The definitive checklist when applied, aids in determining the adequacy of data protection regulation within a country and for countries where personal data is transferred to. A country ought to first interrogate itself. Roth's reasoning which I agree with is that a country should not hold another to a standard higher than it itself is abiding by.[10]

The GDPR outlines factors to consider when determining adequacy, but the GDPR in my view is overly broad and does not provide a nuanced, more concrete, and practical approach to determining adequacy. I must emphasize that the GDPR framework is useful to the extent that it offers some guidance on what may be included when making a determination of adequacy. However, the GDPR lacks the fine points of making an adequacy determination and

[6] P Roth 'Adequate Level of Data Protection in Third Countries Post-Schrems and under the General Data Protection Regulation' (2017) *Journal of Law, Information and Science* 54.
[7] Ibid 60 – 63.
[8] D Lekubu 'Understanding 'Adequate Legal Protection' As A Requirement For Transborder Information Flows From South Africa' (2022) LLM Report.
[9] Ibid 59,60.
[10] Roth (note 6 above) 64, 65.

hence, as crafted is not useful for a State conducting a critical self-assessment of its own data protection laws.

The determination-of-adequacy framework that I propose in the next section will be instrumental in interrogating the issues set out under Article 45(2) of the GDPR. Secondly, my determination-of-adequacy framework while being definitive will inquire into constitutional and legislative pronouncements as they relate to data protection. Thirdly, my determination-of-adequacy framework provides the checklist that will investigate adequacy of sectoral laws that deal with State surveillance and surveillance capitalism. Fourthly, my framework will provide the template to inquire into case law, data subject rights, and data protection principles. Fifthly, my framework will assess access to effective remedies and existence of an effective and independent data protection authority.

3.3 Defining a determination of adequacy framework

Due to the gap in the KDPA on guidelines to determine adequacy of data protection regulation, this chapter proposes an objective framework to determine adequacy. The framework is party inspired by Kipling's poem "I Keep Six Honest Serving Men":

> 'I KEEP six honest serving-men
> (They taught me all I knew);
> Their names are What and Why and When
> And How and Where and Who.
> I send them over land and sea,
> I send them east and west;
> But after they have worked for me,
> *I* give them all a rest.
>
> *I* let them rest from nine till five,
> For I am busy then,
> As well as breakfast, lunch, and tea,
> For they are hungry men.
> But different folk have different views;
> I know a person small—
> She keeps ten million serving-men,
> Who get no rest at all!

She sends' em abroad on her own affairs,
From the second she opens her eyes—
One million Hows, two million Wheres,
And seven million Whys'[11]

The six honest men in Kipling's poem are "What and Why and When and How and Where and Who". Who, what, when, where, why, and how are regularly posed as questions by legal practitioners who seek to have a 360° view over legal issues they are interrogating.[12] Just like Kipling, the questions will teach us all we need to know about an issue. I adopt who, what, when, where, why, and how and turn them into questions to be used as the overarching framework to determine adequacy of data protection regulation in Kenya.

In this chapter, I take a deep dive into components of these questions with a view to propose a nuanced and objective framework that would provide a comprehensive dissection into data protection regulation in any jurisdiction. For each question, I set out the Kenyan data protection provision, I compare it with the GDPR and POPIA, and then discuss scholarly reflections on the provision.

The determination-of-adequacy framework I propose in this chapter sets the foundation for interrogation of adequacy in later chapters of this study. In chapters four, five, and six, I investigate Kenya's regulatory framework on data protection with a focus on State surveillance, surveillance capitalism, and availability of effective remedies by posing "who?", "why?", "what?", "when?", "where?", and "how?" questions. Responses to these questions in this chapter provide the bare minimum and general threshold of data protection regulation. In later chapters, dealing with more specific issues and provisions of the KDPA, I will add more substance to this general minimum threshold sketched in this chapter. The questions are interrelated and must all be answered for a comprehensive determination-of-adequacy to be realised.

[11] R Kipling *Just Do Stories* (1902).
[12] See A Gichuhi *Litigation: The Arts of Strategy and Practice* (2017); P Gaines *From Truth to Technique at Trial* (2016).

3.4 "Who?"

Responses to the "who?" question in the determination-of-adequacy at a minimum should first, identify persons who the prevailing data protection regulation accords legal protection. Secondly, the responses to the question pinpoint the persons whom the law grants powers to make incursions into the right to privacy as protection under the KDPA. Additionally, it is important to bear in mind the fact that a power asymmetry exists between the persons identified in the first and second responses to the "who?" question.

3.4.1 The data subject

Individuals have reasonable expectation of privacy. For data protection, reasonable expectation is derived from the KDPA that gives effect to Article 31(c) and (d) of the Constitution. Jurisprudence from the courts has put emphasis on the principle of reasonable expectation of privacy, for example, in *Roshanara Ebrahim v Ashleys Kenya Limited*[13] and *N W R v Green Sports Africa Ltd.*[14] The South African decision in *Mistry v Interim National Medical and Dental Council of South Africa* also recognised legitimate expectation of privacy.[15] But, who are these individuals with reasonable expectation of privacy?

The response to the "who?" question is set out in the KDPA which refers to a "data subject". Section 2 of the Act defines a data subject as "an identified or identifiable natural person who is the subject of personal data". The definition of a data subject under the KDPA word for word mirrors the definition under Article 4(1) of the GDPR.

South Africa's definition of a data subject includes a juristic person. Section 8(4) of the South Africa Constitution states that "a juristic person is entitled to the rights in the Bill of Rights to

[13] *Roshanara Ebrahim v Ashleys Kenya Limited & 3 others* [2016] eKLR.
[14] *N W R & another v Green Sports Africa Ltd & 4 others* [2017] eKLR.
[15] *Mistry v Interim National Medical and Dental Council of South Africa and Others* (CCT13/97) [1998] ZACC 10; 1998 (4) SA 1127; 1998 (7) BCLR 880 (29 May 1998) 27.

the extent required by the nature of the rights and the nature of that juristic person". In line with this provision, the Constitutional Court of South Africa in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* stated that juristic persons "do enjoy the right to privacy, although not to the same extent as natural persons. The level of justification for any particular limitation of the right will have to be judged in the light of the circumstances of each case".'[16]

Perhaps Kenyan Courts may in future consider arguments in the above South African decision since Article 260 of the Kenyan Constitution defines "person" to include a company, association, or other body of persons whether incorporated or unincorporated. Article 31 provides that "every person has the right to privacy". Section 2 of the KDPA states that "person" has the meaning assigned to it under Article 260 of the Constitution. The point of departure in Kenyan law is section 2 of the KDPA that states that "personal data" means any information relating to an identified or identifiable natural person. It does not include a legal or juristic person when defining "personal data" and "data subject". The Data Commissioner dealt with the definition of a data subject in *Allen Waiyaki Gichuhi v Florence Mathenge* where the data commissioner reiterated section 2 of the KDPA that defines a data subject to be a natural person only.[17]

I my view, data protection regulation must at the very least provide protection for the data of a natural person. However, should the courts pronounce that personal data includes data of a juristic person, then they should borrow principles found in the South African *Hyundai* case where determinations are to be made on a case-to-case basis.[18]

---

[16] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* (CCT1/00) [2000] ZACC 12; 2000 (10) BCLR 1079; 2001 (1) SA 545 (CC) (25 August 2000) 18.

[17] *Allen Waiyaki Gichuhi and Charles Wamae v Florence Mathenge and Ambrose Waigwa, complaint 677 of 2022.*

[18] For more discussions on the definition of a data subject, see also L Tosoni and L Bygrave 'Article 4. Definitions' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 100 – 115; Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (2018) 133 – 135; E De Stadler, E Hattingh , P Esselaar, and J Boast *Over-Thinking the Protection of Personal Information Act* (2021) 113 – 116.

3.4.2 Data controllers and data processors

Another response to the "who?" question identifies the natural or legal person who the law grants powers to process personal data. The KDPA refers to them as "data controller" and "data processor". Section 2 of the Act defines a data controller as "a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data". A data processor is "a natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller". Similar definitions for data controller and data processor are found in Articles 4(7) and 4(8) of the GDPR. POPIA uses the terms "responsible party" and "operator" in place of data controller and data processor respectively. However, the definitions are in substance similar to the definitions in the KDPA and GDPR.[19]

From these definitions, the list of "who" would wish to process personal data is limitless, ranging from natural to legal persons who may be public or private entities. In my view the law must regulate both public and private actors who make incursions into data protection rights. Identification of the "who" in processing personal data sets the scene for response to the other determination-of-adequacy framework questions. Specific response to the "who?" question provides basis for answers to the "why?", "when?", and "how?" questions. Responses to these questions for a public institution would be different compared to those of a private entity seeking to make incursions into an individual's privacy. It is for these reasons that I argue that responses to the "who?" question ought to be expressly set out in legislation.

After identifying the data subject, data controllers and data processors, it is instructive to note that a power asymmetry exists between these parties. This asymmetry impacts on the rights of the data subject. In the next section, I interrogate asymmetry of power between a data subject and a data controller or data processor.

[19] For more discussions on definitions of a data controller and data processor, see also L Tosoni and L Bygrave 'Article 4(7). Controller' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 145 – 156; L Tosoni and L Bygrave 'Article 4(8). Processor' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 157 – 162; Y Burns and A Burger-Smidt *A* (note 18 above) 149 – 154.

3.4.3 Power asymmetry

The relationship between a data subject and data controller or data processor presents one key challenge of asymmetry of power. In this section I discuss this troubled relationship and posit that the law must strike a balance in the interaction between a data subject and data controller or data processor. The law ought to establish guard rails to tame excesses by data controllers and data processors.

Constitutional principles easily seek to strike a balance on the power asymmetry between the State and an individual through vertical application of the Bill of Rights. For non-State actors, horizontal application of the Bill of rights applies. The Supreme Court of Kenya in *William Musembi v Moi Educational Centre Company Ltd*, emphasizing horizontal application of fundamental rights and freedoms, ruled that "private entities have the obligation, under Article 20(1) not to violate Article 43 rights as non-violation of all rights in the Bill of Rights applies both horizontally and vertically and binds both the State and all persons".[20] While power asymmetry exists vertically and horizontally, the focus of this section is power asymmetry as relates to commercial entities and data subjects. This section illustrates how power dynamics might play out in the relationship between data subjects and data controllers or data processors.

For commercial processing of personal data, Ghosh and Couldry argue that there is asymmetry of power between consumers and corporations fuelled by monopoly of power in the big data economy.[21] Zuboff asserts that individuals are in a "Faustian Pact"[22] with multinational technology companies.[23] Individuals wish away their right privacy to enjoy services, services provided by multinational corporations like Google, Facebook, Microsoft,

[20] *William Musembi and others v Moi Educational Centre Company Ltd and others* SC Petition No.2 of 2018 64.
[21] D Ghosh and N Couldry 'Digital Realignment Rebalancing Platform Economies from Corporation to Consumer' (2020) *M-RCBG Associate Working Paper Series* 6.
[22] Britannica "Faustian bargain, a pact whereby a person trades something of supreme moral or spiritual importance, such as personal values or the soul, for some worldly or material benefit, such as knowledge, power, or riches" < https://www.britannica.com/topic/Faustian-bargain> last accessed 18 August 2022.
[23] S Zuboff *In the Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Kindle Edn 2019) Ch. 5.6.

Apple, Amazon, Twitter, and Instagram are crafted within a business model that constantly extracts personal data for commercial purposes.[24] Individuals are the source of personal data that serves as raw material for surveillance capitalism and corporations often avoid accountability for their intrusive mass processing of personal data.

Zuboff posits that surveillance capitalists seem to have declared their right to use personal data processes without adherence to privacy and data protection principles.[25] The result is surveillance capitalism's mode of operation to modify human behaviour using personal data for profit by using methods that bypass human awareness, individual decision-making rights, and self-regulatory processes. Surveillance capitalism is about the control of certainty using personal data; like totalitarianism, surveillance capitalism seeks to control every aspect of society.[26]

Surveillance capitalism is anti-democratic. Corporations can determine and control their polices without consulting individuals from whom they extract personal data from. This creates an asymmetry of power between the corporations and individuals. No public participation takes place when corporations amend their terms of use and policies generally. The fact that they operate globally and in countries having different regulatory regimes for technology companies means that they can easily evade regulation.[27]

Surveillance capitalism is not only undertaken by multinational technology companies. The Centre for Intellectual Property and Information Technology Law (CIPIT) at Strathmore University published a report on privacy and data protection practices of digital lending apps in Kenya.[28] CIPIT found that the digital lending apps that it studied did not comply with privacy and data protection principles outlined in the KDPA. The apps shared data with third parties without the consent of data subjects and had embedded trackers that profiled user

[24] M Crain *Privacy Over Profit* (2021).
[25] Zuboff (note 23 above) Ch. 10.1.
[26] Ibid Ch. 13.2.
[27] Ibid Ch. 6.3; Ch. 6.5.
[28] CIPIT "Privacy and Data Protection Practices of Digital Lending Apps in Kenya" (2020) <https://cipit.strathmore.edu/privacy-and-data-protection-practices-of-digital-lending-apps-in-kenya-report/> last accessed 8 April 2021.

behaviour.[29] The practices of the digital lending apps led to amendments to the Central Bank of Kenya Act.[30] The amendments require registration of digital credit providers with the Central Bank of Kenya and secondly, led to enactment of data protection regulations specific to digital credit providers.

Martin points out that mobile money services especially in Africa are avenues of all forms of surveillance.[31] In 2021, Safaricom which is Kenya's largest mobile telecommunications company reported that it had 28.31 million mobile money subscribers.[32] The 2019 national census reports indicates that Kenya has a population of just over 47.5 million.[33] This means that Safaricom has almost 60% of the Kenyan population using its mobile money service.

Considering that Safaricom is Kenya's largest mobile telecommunications network and more than 60% of the population use Safaricom's mobile money, one who wishes to use mobile money in Kenya is resigned to the use Safaricom's services. Mobile money services are used to pay for most of the goods and services on offer in Kenya. One has no option but to use Safaricom mobile money services which creates an asymmetry of power between the consumer and Safaricom.

Draper and Turow explain the asymmetry of power by discussing what they call "digital resignation". [34] Draper and Turow argue that even though people are not happy with the monitoring that occurs in surveillance capitalism, they do not think that the surveillance can be avoided.[35] "Digital resignation" refers to "people's feeling that they are powerless to avoid the unwanted privacy violations that could occur as a result of any number of situations, from an online platform changing its privacy settings to a friend or family member sharing

[29] Ibid 31.
[30] The Central Bank of Kenya (Amendment) Act, 2021.
[31] A Martin 'Mobile Money Platform Surveillance' (2019) *Surveillance & Society* 214.
[32] Safaricom "Annual Report 2021" available at < Safaricom at a glance – Safaricom> last accessed 17 March 2022.
[33] Kenya National Bureau of Statistics.
[34] N Draper and J Turow 'The corporate cultivation of digital resignation' (2019) *New Media & Society* 1824 - 1839
[35] Ibid 1825

unwanted information".[36] In my view, an adequate legal regime should not disempower data subjects; people should not resign to their fate.

Draper and Turow acknowledge that there are advantages to information sharing such as "content personalization, improved service, and convenience". [37] However, requirements to provide personal information to enjoy these advantages "reduce participants' sense of control". [38] The power asymmetry brings about "feelings of resignation" that emanate from "a perception that privacy violations are unavoidable".[39] This is the reason I argue that adequate legal protections provide data subjects with a measure of control over their personal data.

Surveillance capitalism actors exploit the sense of "digital resignation". While individuals may be concerned with the amount personal data they give away, they find themselves dependent on platforms or services that rely on such data.[40] Draper and Turow argue that the "feelings of resignation are a rational emotional response in the face of undesirable situations that individuals believe they cannot combat".[41] They further argue that such resignation "supports capitalism by constructing corporate power as an inevitable and immovable feature of contemporary life".[42]

Ghosh and Couldry are of the view that the asymmetry of power and "digital resignation" may be countered through privacy regulation.[43] On my part, I argue in this study that data protection regulation must be adequate. The law ought to empower a data subject to act against data controllers and data processors. The power imbalance whether in State surveillance or surveillance capitalism must be addressed by law. Response to the "why?", "what?", "when?", "where?", and "how?" questions within the determination-of-adequacy

[36] Ibid 1826.
[37] Ibid.
[38] Ibid.
[39] Ibid.
[40] Ibid 1827.
[41] Ibid 1828.
[42] Ibid 1829.
[43] Ghosh and Couldry (note 21 above) 15.

framework reveal how the law strikes a balance between a data subject versus a data controller and a data processor.

3.5 "Why?"

Responses to the "Why?" question in the determination-of-adequacy framework should at the very least identify the explicit and specified purposes for processing personal data, protecting personal data, and limiting data subject rights. Responses to the "why?" question are distinguished from the "when?" question responses discussed below as the "when?" question responses focus on the legitimate circumstances under which explicit and specified purposes may be executed.

3.5.1 Explicit and specified purposes

On a practical level, section 25(c) of the KDPA stipulates that personal data is to be processed and "collected for explicit, specified … purposes". The explicit and specified purposes ought to be set out in law. "Why?" question responses outline reasons data controllers and data processors process personal data.

Hallborg asserts that "invasions of privacy have great utilitarian value in promoting the safety and security of the public. The utility of privacy can, at times, be fairly evenly matched by the utility of invasions of privacy".[44] Eberle on the utilitarian value of sharing of personal information contends that collecting and storing large amounts of data is required to collect taxes, distribute services, monitor public health, operate the military, and enforce criminal law.[45] In making a determination-of-adequacy I interrogate the laws that provide for what Eberle lists above and specifically on processing of personal data. I do concede that there is

[44] R Hallborg 'Principles of Liberty and the Right to Privacy' (1985) *Law and Philosophy* 181.
[45] E Eberle 'The Right to Information Self-Determination' (2001) *Utah Law Review* 965 – 966.

utility in invasions of privacy for public interest and commercial purposes but only in so far as those invasions are spelt out in the law and balanced through compliance with constitutional and statutory provisions.

Data is often referred to as the "the new oil" or "the new bacon". Andrus compares data processing to how automobiles need oil to function; crude oil must be exploited to ensure that automobiles have sufficient refined oil.[46] Likewise, personal data is extracted from individuals and processed into a commodity that may be used for research, direct marketing, predictive modelling, and other commercial purposes. Just like extraction of oil has its negative effects, processing of personal data occasions harms.

Data also has the moniker "the new bacon" label because, first, with the world increasingly using technology and services that require massive amounts of data to thrive, data has become a prime commodity.[47] Secondly, the world has an "unhealthy obsession with data".[48] The insatiable goal for both State and non-state actors is to amass as much data as possible. Thirdly, high value is derived from the ability to "analyse, store, and archive unstructured data delivers true bacon for companies".[49]

Richardson reiterates that the existence of a market for personal data is part of today's modern life, albeit publicly problematic.[50] The obsession with data has created an environment where data economy enables State and non-state actors to adopt illegal, immoral, and highly intrusive means to process as much personal data as possible without taking into consideration constitutional and statutory provisions. The difference between data and oil is that data may be processed, used, stored, analysed, and shared for one purpose

[46] M Andrus 'The New Oil: The Right to Control One's Identity in Light of the Commoditization of the Individual' (2017) *Business Law Today* 1-5.
[47] Quantum Bog "Top 3 Reasons Why Metadata Is "The New Bacon"" (2017) <https://blog.quantum.com/2017/08/15/top-3-reasons-why-metadata-is-the-new-bacon/> last accessed 29th July 2022.
[48] Ibid.
[49] Ibid.
[50] J Richardson *Law and the Philosophy of Privacy* (2016) 11.

while also being processed for another purpose. Essentially data may be used and reused unlike oil or bacon.

On the importance of personal data, Rule writes that personal data has become an essential raw material for many important social and economic activities.[51] Be it in the public or private sector, personal data is invaluable, for example, when applying for documents such as a national identity card, passport, birth certificate or seeking services such as health, education, banking, and insurance, processing of personal data is paramount. As per Rule, we live "in a world where the flow of information plays as basic a role as coal and steam did during the Industrial Revolution".[52] Big data and specifically personal data is the fuel and driver of the fourth industrial revolution.[53]

Personal data is crucial for government planning, hence, reason the government periodically carries out national census that includes collection of personal data. On need for data for public purpose, Eberle stresses that "release of personal information is a necessary part of participation in modem society and democratic governance".[54] Personal information is necessary to fashion and implement public policies.

Eberle further emphasises that "collection and assembly of information about us is a necessary part of participation in modem society".[55] To illustrate, the Kenyan Statistics Act[56] under its Statistics (Census of Population) Order, 2018 requires individuals to provide personal data which includes name, sex, age, ethnicity or nationality, religion, marital status, and place of birth, among others. The information is processed by the Kenya National Bureau of Statistics established under section 3 of the Statistics Act. The Bureau uses personal data for among other functions to maintain a comprehensive and reliable national socio-economic database which may be used by State and non-State actors for varied purposes.[57] What the

[51] J Rule 'Toward Strong Privacy: Values, Markets, Mechanisms, And Institutions' (2004) *University of Toronto Law Journal* 183.
[52] Ibid 184.
[53] K Schwab *The Fourth Industrial Revolution* (2016) 18.
[54] Eberle (note 45 above) 970.
[55] Ibid.
[56] Act No. 4 of 2006.
[57] Section 4(2) Statistics Act.

Statistics Act does is provide a response to the "why?" question in relation to processing personal data for public planning purposes. Such responses are what I seek from legislation that interacts with the right to privacy.

Fan in making the case for consumer data being available for public use argues that personal data used for commercial purposes such as for target advertising, expanding sales, and encouraging spending, can also be used productively for the public good to prevent the outbreak of illness and detect and fight the spread of false and dangerous claims.[58] The OECD in a report on *Data-Driven Innovation: Big Data for Growth and Well-Being*[59] in indicating the importance of big data states that big data is "driving knowledge and value creation across society...".[60] Secondly, big data "can increase the transparency and accountability of governments, thus boosting public sector efficiency and public trust in governments."[61] Thirdly, data and analytics may be used to "improve or foster new products, processes, organisational methods and markets".[62]

While interrogating responses to the "why?" question, my argument is that one ought to pay attention to the value of the right to privacy and data protection. Corlett quotes DeCew who outlines the value of privacy as follows:

> "Privacy shields us not only from interference and pressures preclude self-expression and the development of relationships, from intrusions and pressures arising from others' access on us and details about us. Threats of information leaks, as well as threats of control over our bodies, our activities, and our power to make our own choices, give rise to fears that we are being scrutinized, judged, ridiculed, pressured, coerced or otherwise taken advantage of by others. Protection of privacy enhances and ensures the freedom from such scrutiny, pressure to conform, and exploitation. We require this protection that privacy provides so that as self-conscious beings we can maintain our self-respect, develop our self-esteem, and increase our ability to form a coherent identity and set of values, as well as our ability to form varied and complex relationships with others".[63]

[58] M Fan 'The Public's Right to Benefit from Privately Held Consumer Big Data' (2021) *NYU Law Review* 35.
[59] OECD *Data-Driven Innovation: Big Data for Growth and Well-Being* (2015).
[60] Ibid 20.
[61] Ibid 21.
[62] Ibid 21.
[63] J Corlett 'The Nature and Value of the Moral Right to Privacy' (2002) *Public Affairs Quarterly* 334.

Explicit and specified purposes for processing personal data should not be a threat to the fundamental rights and freedoms of a data subject. Cohen argues that the value of privacy protects from commercial and government entities' ambitions to conjure up predictable persons and communities.[64] I argue in this study that respect, protection, and promotion of the right to privacy and data protection influence how other rights are enjoyed. Explicit and specified purposes for personal data processing should be regulated by law, otherwise, the incursions into the right to privacy and other fundamental rights and freedoms will be unbridled.

Bruin reflects on the sceptical approach towards the value of privacy.[65] In Bruin's analysis, sceptics to the value of the right to privacy would acknowledge that the revelation of private information might have negative consequences, but argue that these are outweighed by liberty and that most problems emerging from invasions should be left to individuals.[66] Sceptics of the value of privacy sees no harm in government surveillance or surveillance capitalism.

According to the sceptics, surveillance does not stop one from carrying out certain activities. Secondly, disclosure of intimate information from an intimate relationship does not necessarily stop future sharing of information between partners. Thirdly, that to prove invasion of privacy, one would have to prove that the invasion resulted in the decrease of their freedom.[67] However, Bruin insists on the need for balance; "subject's liberty interest in the protection of privacy balanced against the liberty interests the recipient's freedom of information".[68]

Away from the sceptics, Bruin agrees with the notion that disclosure of private information influences one's negative freedom.[69] Disclosure of private information may cause an act or omission or change in disposition regarding certain acts or omissions making one less free to

[64] J Cohen 'What Privacy is For' (2013) *Harvard Law Review* 1905.
[65] B Bruin 'The Liberal Value of Privacy' (2010) *Law and Philosophy* 505 -534.
[66] Ibid 506.
[67] Ibid 507 – 509.
[68] Ibid 527.
[69] Ibid 511.

act as they wish.[70] In my view, the sceptics are misguided in their arguments. As I shall demonstrate in this chapter, actual harms may be occasioned on data subjects and the law must provide adequate recourse to a data subject.

In this study I submit that there is utility in processing personal data for public and commercial purposes. But such processing ought to be in line with adequately crafted laws bearing in mind that a data subject is central to adequate data protection laws. In view of these arguments, in the next sections I indicate that in as much as there may be data for good or limitation of data subject rights for good, there are harms that may be occasioned upon individuals and societies if these rights are not respected, promoted, and protected. I also argue that principles of liberty must be taken into consideration when identifying explicit and specified purposes for processing personal data.

3.5.2 Liberty and privacy

In addition to power asymmetry, responses to the "why?" question should be interrogated taking into account principles of liberty as espoused by Mill.[71] The principles are that, first, all persons have political liberties or rights which the State should not infringe upon. Secondly, there ought to be checks on the powers of the State; powers which are to be exercised with the consent of the people. Individuals should be protected from the tyranny of the majority; protection against the tyranny of prevailing opinion and feeling. Individual independence should be protected against control of the majority. The law should not control individuals such as to do away with individual freedoms or impose the will of the State or the majority.

Compulsion and control by the law or the State must be exercised only where it is aimed at protecting the individual or to prevent harm to others. Otherwise, over oneself, over one owns body and mind, the individual is sovereign. The State ought to create an environment where the individual can exercise their autonomy without undue interference from the State

[70] Ibid 511 -516.
[71] J Mill *On Liberty* (Kindle Edn 1859).

or the majority. The space within which an individual can exercise their autonomy without interference by the state, other persons, or commercial entities partly relates to the privacy of that individual.

Veliz posits that we need liberalism where individuals live their lives as they deem fit and that rules should be in place to ensure that individuals are free from interference from surveillance by the State or corporations.[72] For a liberal democracy to thrive, ordinary citizens need to let each other be. In the preface to his book, Snowden pronounced this about liberty and privacy:

> "The freedom of a country can only be measured by its respect for the rights of its citizens, and it's my conviction that these rights are in fact limitations of state power that define exactly where and when a government may not infringe into that domain of personal or individual freedoms that during the American Revolution was called "liberty" and during the Internet Revolution is called "privacy.""[73]

Corlette makes the argument that what rights and freedoms have in common is the ability of right holders to freely choose and execute (move freely) from the many options accepted in their lives.[74] This is their right to freedom and it is the core of liberty.[75] It is a right that holds the individual against the machinations of the world at large.[76] It is about human autonomy which is at the core of personal liberty. According to Solove, providing notification, access, and control of data is increasing decision-making power related to processing personal data which is the key to enabling some degree of autonomy.[77]

Hallborg seeks to derive the right to privacy from fundamentals of liberty.[78] While doing this, Hallborg points out certain definitions of the right to privacy within liberty fundamentals which include the "right not to be observed when private", "right to not be listened to", "right to retire into seclusion", and "right to engage in private conduct".[79] Hallborg argues

[72] C Veliz *Privacy is Power* (Kindle Edn 2020) Ch 4.
[73] E Snowden *Permanent Record* (Kindle Edn 2019).
[74] Corlett (note 63 above) 331.
[75] Ibid.
[76] Ibid 332.
[77] D Solove 'Privacy Self-Management and the Consent Dilemma' (2013) *Harvard Law Review* 1880.
[78] Hallborg (note 44 above) 175 – 218.
[79] Ibid 177 – 180.

that these are from the fundamentals of liberty and two rights to privacy emerge, first, a constitutional right to privacy and secondly, a moral right to privacy.[80]

On the constitutional right to privacy, Hallborg argues that it is a right asserted against the government while the moral right to privacy is the right that one asserts against another individual.[81] Hallborg avers that he makes the distinction because, the principles of liberty that apply to disputes between individuals and governments are different, but similar to the principles of liberty that apply to disputes between individuals.[82]

In setting out the constitutional right to privacy as against the state, an individual ought to direct their lives as they so wish save for when the public good may require control of that conduct.[83] The state must have good reason to restrict an individual's right to privacy. And as I argue in this study, this reason must be spelt out in written law.

According to Hallborg, "the restriction must be for the public benefit, there must be rational grounds for believing that the restriction will, in fact, achieve the desired result, and there must be no more restriction of liberty than it is reasonable to believe will achieve the desired result".[84] With the right to privacy being derived from fundamentals of liberty, an individual would wish to act or operate in an environment where they are not being constantly observed. If one was to be observed against their wish without reasonable justification, then that would be against fundamentals of liberty and in effect the right to privacy.[85]

Individuals may wish to act in an environment where they are not being constantly observed, for example, when engaging in political activities. At times, how one may act within a political setting may be determined by whether they are being observed. The right to privacy "is a condition of action which has considerable bearing on how we might choose to act and, as it is not a morally reprehensible or oppressive condition of action, it presents at least a prima

[80] Ibid 180.
[81] Ibid 180.
[82] Ibid 180.
[83] Ibid 182.
[84] Ibid 183.
[85] Ibid 187.

facie valid claim to being a liberty right".[86] Hallborg on limiting the right states that "the greater the proposed destruction of liberty, the greater the burden of justification on the proponent of destruction - in this case, government".[87] The same principles apply to the right to privacy. Eberle on information data processing in a liberal democracy asserts:

> 'Democratic decision making means the power of citizens to participate in collective life, listening to and voicing ideas that contribute to the formation of community, its value structure, and society-wide policies. Here we must preserve the capacity for people to make choices about relevant concerns and policies. In respect of both individual self-determination and democratic decision making, we must guard against intimidation, coercion, and manipulation of people and society through the use of personal information in data processing.'[88]

Rouvroy and Poullet on privacy and democracy hold that privacy as a legal claim is essentially a means of promoting an individual's specific but changing autonomy needed at a particular time in a particular society to maintain vibrant democracy.[89] Rouvroy and Poullet go on to state that individual autonomy ought to be balanced through legislation against forces within the technological, economic, political, and social realms.[90] Human beings are fighting for their autonomy against the "intensification of observation and monitoring technologies such as CCTV, data mining and profiling, RFID and the 'internet of things', ubiquitous computing and 'ambient intelligence'".[91]

Cohen reiterates that privacy is an "indispensable structural feature of liberal democratic political systems"[92] and that liberal democracy and innovation "thrive in the interstitial spaces within information processing frameworks; privacy regulation must focus on maintaining those spaces".[93] In Cohen's analysis of a liberal democracy, such cannot be sustained without

---

[86] Ibid 188.
[87] Ibid 211.
[88] Eberle (note 45 above) 970.
[89] A Rouvroy and Y Poullet 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' S Gutwirth, Y Poullet, P Hert, C Terwangne, S Nouwt (eds) *Reinventing Data Protection?* (2009) 46.
[90] Ibid.
[91] Ibid.
[92] Cohen (note 64 above) 1905.
[93] Ibid 1906.

the autonomy of the individual to self-govern; Cohen is of the opinion that a society that permits unfettered surveillance on individuals, cannot possibly remain a liberal democracy.[94]

On liberty, Rouvroy and Poullet submit that "the right to self-development is not conceived as a liberty held in isolation by an individual living secluded from the rest of society but, on the contrary, as a right enjoyed as member of a free society".[95] It is for this reason, that the State exercises its negative and positive duties in relation to the right to privacy. Legislation for example, allows an individual to live in society while maintaining their autonomy by warding off unwelcome or unwarranted privacy intrusions.

In my analysis, what the above arguments indicate is that crafting a data protection regulatory framework is a race towards saving liberal democracy and autonomy of the individual. An autonomous individual is empowered to operate in society actively and objectively. Intrusions or limitations not only affect the individual but society at large.

As I will argue throughout this thesis, data protection regulation should have the individual at the centre. This individual requires robust legislation to thrive in society and to have their right to privacy respected, protected, and promoted. Promulgation of the Constitution was meant to usher a new constitutional dispensation that not only adheres to constitutionalism and the rule of law but also guarantees and promotes in practice the fundamental rights and freedoms of the individual including privacy and data protection.[96] The Constitution and principles of liberty therein are some of the pillars I use to interrogate adequacy of data protection regulation.

[94] Ibid 192.
[95] Rouvroy and Poullet (note 89 above) 57.
[96] M Mbondenyi and O Ambani *The New Constitutional Law of Kenya: Principles, Government and Human Rights* (2012); P Lumumba and M Mbondenyi *The Constitution of Kenya: Contemporary Readings* (2011).

3.5.3 Harms

While scrutinising the value of privacy and data protection it is critical to take note of the harms that may be occasioned by not protecting the right, not adhering to principles of data protection, or disregarding data subject rights. As I analyse responses to the "why?" question, I bear in mind the potential harms that may be caused by executing the responses. For example, Warren and Brandeis stated that invasions of privacy may subject an individual to "mental pain and distress, far greater than could be inflicted by mere bodily injury."[97]

Eberle argues that managing personal data is management of people which includes the ability to force and manipulate people to take predetermined actions.[98] Whether such ability is used for better or for worse is a challenge in the information age; it is one of the most pressing political issues.[99] When personal data is used by State or non-State actors to coerce or manipulate the data subject suffers harm or loss.

On data protection, Citron and Solove state that "many privacy violations involve broken promises or thwarted expectations about how people's data will be collected, used, and disclosed".[100] While the violation may be seen as minor as it affects just an individual, Citron and Solove go on to argue that "…these small harms are dispersed among millions (and sometimes billions) of people. Over time, as numerous people are each inundated by a swarm of small harms, the overall societal impact can be significant".[101] An example of societal impact is the Cambridge Analytica scandal mentioned below. There is no doubt that there are harms cause by privacy violations. Challenges that I address in this study include what the law should do about the harms and whether the law does indeed recognise the harms.[102]

---

[97] S. D. Warren & L. D. Brandeis 'The Right to Privacy' (1890) *Harvard Law Review* 193.
[98] Eberle (note 45 above) 966.
[99] Ibid.
[100] D Citron & D Solove 'Privacy Harms' (2011) *GW Law School Public Law and Legal Theory Paper No. 2021-1, GW Legal Studies Research Paper No. 2021-11* 3.
[101] Ibid 4.
[102] L Barrett 'Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries' (2019) *Seattle University Law Review* 1056 – 1112.

Section 65 of the KDPA recognises that harm may be occasioned upon a data subject and provides for remedies:

(1) "A person who suffers damage by reason of a contravention of a requirement of this Act is entitled to compensation for that damage from the data controller or the data processor.

(2) Subject to subsection (1) —

(a) a data controller involved in processing of personal data is liable for any damage caused by the processing; and

(b) a data processor involved in processing of personal data is liable for damage caused by the processing only if the processor—

(i) has not complied with an obligation under the Act specifically directed at data processors; or

(ii) has acted outside, or contrary to, the data controller's lawful instructions.

(3) A data controller or data processor is not liable in the manner specified in subsection (2) if the data controller or data processor proves that they are not in any way responsible for the event giving rise to the damage.

(4) In this section, "damage" includes financial loss and damage not involving financial loss, including distress."

What is the nature of "harm" or "damage" that may warrant compensation? Section 65(4) is vague when it defines "damage" to include "financial loss and damage not involving financial loss, including distress". Financial loss requires factual proof. Damage that's non-financial requires specific definition. To identify harms, section 31 of the KDPA provides for data protection impact assessments. As per section 31 data protection impact assessments are important tools in identifying where processing of personal data is "likely to result in high risk to the rights and freedoms of a data subject".

In comparison, on damages, Article 82 of the GDPR refers to "material and non-material damages" which may warrant compensation to the data subject. On the other hand, section 99 of POPIA provides that a data subject may institute an action for damages and courts may order an amount which may include:

(a) 'payment of damages as compensation for patrimonial and non-patrimonial loss suffered by a data subject as a result of breach of the provisions of this Act;

(b) aggravated damages, in a sum determined in the discretion of the Court;

(c) interest; and

(d) costs of suit on such scale as may be determined by the Court.'

The point I make here is that the KDPA, the GDPR and POPIA recognise that there are potential harms to processing of personal data. Lipton discusses harms and remedies in relation to privacy intrusions.[103] The harms aspect brings to the fore the dichotomy between monetary and non-monetary harms. While monetary damages are easy to quantify because they may result from "misappropriation of an individual's private persona, as with the misappropriation privacy tort, the right of publicity, or identity theft", non-monetary harms or damages pose a challenge to courts on how to quantify them.[104] Notwithstanding, an effective remedy is instrumental to the harm occasioned by the intrusion.[105] In chapter six I discuss the need to have access to effective remedies legislated, and the need to have damages for monetary and non-monetary harms alike.

Citron and Solove identify fourteen harms that may be occasioned by an intrusion of privacy, these are, physical, economic, reputational, emotional, relationship, chilling effect, discrimination, thwarted expectations, control, data quality, informed choice, vulnerability, disturbance, and autonomy harms.[106] In this section, I breakdown the elements of these harms are pronounced by Citron and Solove. Meanwhile, Kilovaty on the other hand identifies "doxing, cyberstalking, medical identity theft, disclosure of sensitive information, and manipulation and microtargeting" as some of the potential misuses of personal data.[107]

Physical harm may be occasioned where personal information is obtained used to physically injure a data subject;[108] economic harm as indicated earlier in this section is where a data

[103] J Lipton 'Mapping Online Privacy' (2009) Case Research Paper Series in Legal Studies: Working Paper 09-24
[104] Ibid 25 – 28.
[105] Ibid 28 – 29.
[106] Citron and Solove (note 100 above) 19 – 40.
[107] I Kilovaty 'Psychological Data Breach Harms' (2021) *North Carolina Journal of Law & Technology* 1. Merriam Webster Dictionary defines "doxing" to mean: "to publicly identify or publish private information about (someone) especially as a form of punishment or revenge" Available at < Doxing Definition & Meaning - Merriam-Webster> last accessed 22 September 2022.
[108] Citron and Solove (note 100 above) 19 – 20.

subject suffers financial loss.[109] Reputational harms points to harms similar to those caused by defamation and depending on what kind of personal information is publicised this may "impair a person's ability to maintain "personal esteem in the eyes of others" and can taint a person's image".[110]

Citron and Solove posit that "emotional distress encompasses a wide range of emotions, including annoyance, frustration, anger, and various degrees of anxiety".[111] Perhaps, these are the emotions drafters of the KDPA had in mind when they penned Section 65(4). Citron and Solove emphasize that "privacy violations can cause emotional distress that can impede someone's life as much as certain physical injuries".[112]

One of the concepts of privacy is maintaining relationships where information may be shared or concealed. When there is an intrusion into one's privacy, certain personal information may become available and in effect damage an intimate relationship.[113] One example is the lawyer-client relationship where confidentiality is paramount. Once the lawyer-client confidentiality is breached without due cause, the relationship breaks down. The same is true for confidentiality in medical settings. "The law of fiduciary relationships safeguards against relationship harms",[114] a duty of care is owed to a data subject.

Barrette argues for the placing of fiduciary duties on "data collectors" for personal information they process whether or not the processing is regulated by law.[115] Additionally, "applying duties of care, loyalty, and confidentiality to data collectors injects a moral valence to broadly uphold users' trust".[116] As Barrette posits, individuals deserve protection against invasion of privacy and the direct or indirect manipulation, exploitation, discrimination, and other damages that digital platforms make on their own.[117] Fiduciary relationships are created

[109] Ibid 20 – 22.
[110] Ibid 22.
[111] Ibid 23
[112] Ibid 23.
[113] Ibid 25.
[114] Ibid 26.
[115] L Barrett 'Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries' (2019) *Seattle University Law Review* 1061.
[116] Ibid 1062.
[117] Ibid 1088.

such that "fiduciaries are generally prohibited from benefitting from their clients' information in a way that could hurt the client: using client information to enrich themselves in a way that disadvantages the client would violate the duty of loyalty, and sharing it beyond prescribed limits would violate the duty of confidentiality".[118] My argument is that adequate data protection regulation is the guard rail for the fiduciary relationship between a data subject and data controllers or data processors.

Personal liberty allows an individual to act as they wish. An invasion of privacy impacts this where it inhibits "people from engaging in certain civil liberties such as free speech, political participation, religious activity, free association, freedom of belief, and freedom to explore ideas",[119] fearing negative consequences. This causes a chilling effect on how individuals act.

Discrimination as a harm relates to where personal information is used to prejudice individuals due to their "race, sex, pregnancy, marital status, health status, ethnic or social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth".[120] Article 27(5) of the Kenyan Constitution states that "a person shall not discriminate directly or indirectly against another person on any of the grounds specified or contemplated". Use of personal information to discriminate is a harm proscribed in the Constitution.

European Digital Rights in a report dubbed "How online ads discriminate: Unequal harms of online advertising in Europe"[121] reported that "discrimination can also occur in other areas of the broader online advertising ecosystem, such as in the many ways in which data is collected, processed and shared for advertising purposes, in the ways in which advertising supported platforms recommend content, or in decisions about which content and which content producers can rely on advertising to monetise their content online".[122] Discrimination in this regard "in the case of online job or housing ads that either exclude, or predominately target

[118] Ibid 1089.
[119] Citron and Solove (note 100 above) 27 – 28.
[120] Article 27(4) Constitution of Kenya, 2010.
[121] European Digital Rights "How online ads discriminate: Unequal harms of online advertising in Europe (2021)" <https://edri.org/wp-content/uploads/2021/06/EDRi_Discrimination_Online.pdf> las accessed 26th July 2021. 10.
[122] Ibid.

a specific demographic or otherwise defined group, discriminatory outcomes in online advertising mean that protected groups are excluded from opportunities".[123]

Thwarted expectations harm derives from the fact that when one allows intrusion into their privacy, the expectation is that the information derived from the intrusion shall only be used for a pre-defined purpose.[124] Where personal information is used for a purpose it was not intended, then, that may be termed as thwarted expectation. For example, where one's personal data is processed by consent for provision of a service by a service provider, but they use the personal data for direct marketing, then that is a thwarted expectation on the part of the data subject. On this, section 25 (c) and (d) of the KDPA states that "every data controller or data processor shall ensure that personal data is… collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes; adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed".

On control harms, Citron and Solove argue that losing control of personal information is a breach of our security and risk management capabilities.[125] Personal information can be used indefinitely for a variety of purposes. Hence, data protection legislation aims to regulate the flow of data to protect individuals from potential downstream use.

Data quality harm is about "keeping data accurate, complete, and up-to-date".[126] It is for this reason that section 25(f) of the KDPA provides that "every data controller or data processor shall ensure that personal data is— accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay".

Informed choice harms as posited by Citron and Solove are to the extent that a data subject ought to provide prior, free, and informed consent before their personal data is processed.[127]

---

[123] Ibid.
[124] Citron and Solove (note 100 above) 31 – 33.
[125] Ibid 35.
[126] Ibid 35.
[127] Ibid 37.

Citron and Solove state that if people aren't informed of their rights or receive important information, they can't claim their rights at the right time, answer questions about personal data effectively, or make meaningful decisions. They suffer because they lose the ability to do it. Laws that require people to be informed of their rights empower individuals.[128] An example of this under the KDPA is section 26(a) which states that "a data subject has a right… to be informed of the use to which their personal data is to be put". In comparison, Article 12 of the GDPR requires "transparent information, communication and modalities for the exercise of the rights of the data subject" while section 5(1)(a) of POPIA demands notification to the data subject.[129]

Vulnerability harms relate to not having sufficient security safeguards for processed personal data.[130] According to Citron and Solove, "disturbance harms involve unwanted communications that disturb tranquillity, interrupt activities, sap time, and otherwise serve as a nuisance".[131] Such include unwanted mail, emails, text messages, telephone calls, or direct messaging on social media. Autonomy harms on the other hand "involve the restriction, coercion, or manipulation of people's choices. People are either directly denied free will to decide or are tricked into thinking that they are freely making choices when they are not. In the consumer privacy context, the most prevalent form of autonomy harm is "manipulation"".[132]

On the effect of manipulation harms to society, Citron and Solove argue that "manipulation can affect not just individuals but also create societal harm, as people's decisions can affect not just themselves but society as well. The Cambridge Analytica incident involved the use of

[128] Ibid 38.
[129] On transparency under the GDPR see also R Polčák 'Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 398 - 412; on transparency under POPIA see also De Stadler (note 18 above) 308 – 320.
[130] Citron and Solove (note 100 above) 38,39.
[131] Ibid 39, 40.
[132] Ibid 40.

personal data on a mass scale to influence people's decisions in the 2016 U.S. presidential election and in the United Kingdom's vote for Brexit".[133]

A harm not centred on the individual relates to how corporations that are driven by mass processing of personal data have created monopolies and distorted markets. Companies such as Facebook, Amazon, Google, Apple, and Microsoft have business models that are focused on processing and commercialisation of their customer's data. A Wall Street Journal report indicated that the five largest U.S. technology companies, Apple, Microsoft, Amazon.com, Google-parent Alphabet, and Facebook had a "combined market capitalization soared by half over the past year (2020) to a staggering $8 trillion".[134]

In the USA, for example, the Federal Trade Commission (FTC) in 2020 authorised an investigation into Facebook's monopolistic practices. On its website, the FTC stated that "the Federal Trade Commission … sued Facebook, alleging that the company is illegally maintaining its personal social networking monopoly through a years-long course of anticompetitive conduct".[135] In 2019, the European Commission fined Google €1.49 billion for breaching EU antitrust rules. A statement by the European Commission stated: "Google has abused its market dominance by imposing a number of restrictive clauses in contracts with third-party websites which prevented Google's rivals from placing their search adverts on these websites".[136] In chapter five of this study I discuss the need to have adequate competition and consumer protection laws to tame monopolies whose business model is based on mass processing of personal data.

[133] Ibid 41.
[134] Wall Street Journal "How Big Tech Got Even Bigger: Technology giants such as Alphabet, Amazon and Apple are more dominant than a year ago thanks to a greater reliance on their services during the pandemic. The forces propelling them to new heights are expected to outlast Covid-19." (6th February 2021) < https://www.wsj.com/articles/how-big-tech-got-even-bigger-11612587632> last accessed 29th July 2022.
[135] Federal Trade Commission "FTC Sues Facebook for Illegal Monopolization Agency challenges Facebook's multi-year course of unlawful conduct" (2020) < https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization> last accessed 29th July 2022.
[136] European Commission "Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising" (2019) < https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770> last accessed 29th July 2022.

To deal with privacy and data protection harms Selinger and Hartzog advance the concept of "obscurity".[137] They define "obscurity" as "the idea that information is safe—at least to some degree—when it is hard to obtain or understand".[138] When information is hard-to-find, it protects an individual against harms, secures an individual's control over personal information, secrecy, intimacy, personhood, limited access to self, and the right to be let alone among others.[139]

According to Selinger and Hartzog, if information is difficult to obtain, it is only used by people who are motivated enough to make the necessary effort and resources.[140] The challenge with this argument is that companies such as Facebook, Amazon, Google, Apple, and Microsoft whose business model is based on personal data mining will constantly have the motivation to expend effort and resources to acquire troves of personal data; in fact through constant technological advances, they have been able to do so.[141] Essentially, Seliger and Hartzog argue that "contemporary privacy debates are probably better understand (sic) if reclassified as concern over losing obscurity".[142]

Selinger and Hartzog outline seven factors that undermine obscurity.[143] First, reduced accountability and transparency in public affairs.[144] Secondly, the increased pressure individuals face to share personal information especially over digital platforms.[145] Thirdly, the proliferation of surveillance technology in use by both state and non-state actors.[146] Fourthly, advances in big data mining.[147] Fifthly, need to provide identity details to access certain

[137] E Selinger and W Hartzog 'Obscurity and Privacy' in J Pitt and and A Shew (2018) *Spaces for the Future: A Companion to Philosophy of Technology* 119 – 129.
[138] Ibid 119.
[139] Ibid.
[140] Ibid.
[141] Ibid 122.
[142] Ibid 121.
[143] Ibid 122, 123.
[144] Ibid.
[145] Ibid.
[146] Ibid.
[147] Ibid.

services.[148] Sixthly, individuals not being aware of the consequences of sharing or exposing personal data.[149] Seventhly, increased automation in data processing operations.[150]

To maintain obscurity as Selinger and Hartzog posit, one key strategy is for the law to recognise data protection and provide remedies for intrusions.[151] Secondly, it is to have technology set in privacy by default or by design mode.[152] Section 41 of the KDPA does provide for data protection by design or default where data controllers and data processors ought to implement technical and organisational measures that are designed to implement data protection principles and integrate appropriate data protection safeguards.

According to Selinger and Hartzog, obscurity not only requires legal and policy pronouncements to protect the right privacy but also requires technological, technical, and organisational measures.[153] This way, personal information becomes harder to obtain and mitigates the potential of ensuing harms. This is what "protection" in data protection relates to and includes jurisprudence, constitutional, legislative and policy regulatory frameworks that guarantee, promote, and protect the right to privacy and data protection while offering effective remedies in cases of breach.

In conclusion, responses to the "why?" question within an adequate personal data protection regulation set up will first, identify the explicit and specified purposes for processing personal data. While carrying out a determination-of-adequacy of data protection regulation, one ought to bear in mind that an incursion into the right to privacy has an effect over other fundamental rights and freedoms. Secondly, it is key to determine the utility of intruding into data subject rights. This applies to public and commercial need for a limited right to privacy. Thirdly, one ought to lay bare the harms that may be caused by limiting protection of personal data. Fourthly, all these considerations ought to be specific and set out in law.

[148] Ibid.
[149] Ibid.
[150] Ibid.
[151] Ibid.
[152] Ibid 124, 125.
[153] Ibid.

3.6 "What?"

In interrogating the adequacy of data protection regulation, my position is that it is critical to identify "what" data is protected by law. The simple response to the "what?" question is "personal data". Section 2 of the KDPA defines "data" as "information which is processed by means of equipment operating automatically in response to instructions given for that purpose; is recorded with intention that it should be processed by means of such equipment; is recorded as part of a relevant filing system; and which forms part of an accessible record; or is recorded information which is held by a public entity". "Personal data" is defined as "any information relating to an identified or identifiable natural person." Hence, personal data of a data subject. Section 2 of the KDPA defines another category of data which is "sensitive personal data", defined as "data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject."

For the GDPR "data" is specifically limited to personal data which includes "any information relating to an identified or identifiable natural person, such information may include an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity."[154] Recital 30 of the GDPR Recitals goes further to state that "natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when

[154] Article 4 of European Union 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)). See also Tosoni and Bygrave (note 12 above).

combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."[155]

In South Africa, section 1 of POPIA has a broader definition on "personal information":

> 'information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—
>
> (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
> (b) information relating to the education or the medical, financial, criminal or employment history of the person;
> (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
> (d) the biometric information of the person;
> (e) the personal opinions, views or preferences of the person;
> (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
> (g) the views or opinions of another individual about the person; and
> (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.'

The common thread I note in the three definitions is the notion of information being of an identified or identifiable natural person.[156] My view is that the definition of personal data must be as broad as possible to capture any elements that may be used to identify a data subject. Schwartz and Solove make the argument that information refers to an identified person when it singles out an individual from others.[157] Information about an identified person ascertains their identity. Information or data refers to an identifiable individual when there is possibility

[155] Ibid.
[156] See also Burns and Burger-Smidt (note 18 above) 15 - 22 and De Stadler (note 18 above) 79 – 84.
[157] P Schwartz and D Solove 'Reconciling Personal Information in the United States and European Union' (2014) *California Law Review* 905.

of future identification which is made possible through a combination of data sets, de-anonymising or de-pseudonymising data.[158]

Technology informs the kind of personal data that is available for processing. Perninan affirms this thinking by stating:

> '… the emergence of new technologies of information and communication provides greater ease for the invasion of another's privacy. This represents an increase in possible aggressions and is surely a source of concern for citizens and lawyers. Nevertheless, it is not only a problem of quantity but also of quality if we consider the use of the information obtained by wrongdoers.'[159]

In my submissions in this study, I posit that responses to the "what?" question are critical in evaluating whether the personal data processed is adequate and relevant as per data protection principles outlined under section 25(d) of the KDPA. At a minimum, personal data ought to be defined in the law.

3.7 "When?"

Next in the adequacy determination framework is to identify the legitimate circumstances under which the law allows for personal data processing. Responses to the "why?" question set the explicit and specified purposes for processing personal data, protecting personal data, and limiting data subject rights. The legitimate circumstances under which data controllers and data processors may legitimately process personal data are defined by responses to the "when?" question. Responses include principles that data controllers and data processors must pay attention to while processing personal data. In this section I point to the overarching principles to bear in mind when responding to the "when?" question and I indicate what the general answers to the question are. I also note that the general responses are subject to

[158] Ibid 907.
[159] B Perninan, 'The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law' (2012) *American Journal of Legal History* 200.

constitutional principles on limitation of fundamental rights and freedoms and ought to be subjected to the proportionality test.

3.7.1 General responses

Reponses to the "when?" question point to legitimate reason to process personal data. Roos argues that an individual determines the destiny of their private facts.[160] An individual has a role to play in the respect, protection, and promotion of their right to privacy.[161] "When" data subject rights are violated or protected, consent while not paramount, is instrumental.

Austin, while analysing consent states that "privacy is often seen as the core interest protected and individual consent as the central vehicle through which this protection is accomplish".[162] Data protection centres itself within the right to privacy concept of control over personal information.[163] Austin qualifies the assertions by submitting that notice to a data subject and reasonableness in processing would also offer privacy protection like consent.[164] But, according to Solove's concept of control of personal information, consent is considered in line with other instruments for legally processing personal data.[165] Responses to the "when?" question must include statutory provision for consent and circumstances under which an individual may lose control over their personal information.

An individual's control in protection of their personal data may be qualified under certain circumstances. To illustrate, law enforcement or national security agencies may limit individual control over personal information in the investigation of a crime.[166] Section 51(2) of

[160] A Roos 'Privacy in the Facebook Era: A South African Legal Perspective' (2012) *The South African Law Journal* 396.
[161] A Roos 'Legal Protection of Personal Information' in J Neethling, J Potgieter and A Roos *Neethling on Personality Rights* (2019) 365 – 414.
[162] L Austin 'Is Consent the Foundation of Fair Information Practices? Canada's Experience under Pipeda' (2006) *The University of Toronto Law Journal* 181.
[163] Ibid 187.
[164] Ibid 183.
[165] D Solove 'Conceptualizing Privacy' (2002) *California Law Review*, 1087-1155.
[166] Austin (note 162 above) 193.

the KDPA provides that the processing of personal data is exempt from the provisions of the Act "if it is necessary for national security or public interest". Section 30(b) of the KDPA also presents other situations where consent is not be central to processing of personal data:

(1) 'A data controller or data processor shall not process personal data, unless—
  (a) the data subject consents to the processing for one or more specified purposes; or
  (b) the processing is necessary—
    (i) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
    (ii) for compliance with any legal obligation to which the controller is subject;
    (iii) in order to protect the vital interests of the data subject or another natural person;
    (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    (v) the performance of any task carried out by a public authority;
    (vi) for the exercise, by any person in the public interest, of any other functions of a public nature;
    (vii) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
    (viii) for the purpose of historical, statistical, journalistic, literature and art or scientific research.'

Section 30 of the KDPA provides the bulk of the responses to the "when?" question. In comparison, Article 6 of the GDPR stipulates similar provisions when processing of personal data may be lawful. On the other hand, section 4 of POPIA sets out the "conditions for the lawful processing of personal information by or for a responsible party".[167] The glaring difference that I identify between the KDPA, GDPR and POPIA is that it is only the KDPA that has provisions for "the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" and "the performance of any task

[167] For lawful processing in the GDPR, see also W Kotschy 'Article 6. Lawfulness of processing' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 321- 344; on lawful processing in POPIA, see also De Stadler (note 18 above) 185 – 203; Burns and Burger-Smidt (note 18 above) 25 -36.

carried out by a public authority". I interrogate these broad and vague provisions in chapter four of this study.

If the response to the "when?" question is consent, Borgesius discusses what is necessary for valid consent. [168] Valid consent is " (i) freely given, (ii) specific, (iii) informed (iv) indication of wishes, by which the data subject signifies agreement to his or her personal data being processed".[169] When processing personal data for commercial purposes, Borgesius is categorical that a data controller or data processor "must generally obtain the data subject's unambiguous consent for personal data processing for behavioural targeting.".[170] This principle is echoed by section 37(1)(a) of the KDPA which provides that "a person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person… has sought and obtained express consent from the data subject".

Section 30 of the KDPA cited above should be read contextually in line with changing circumstances that influence data protection. Kandeh, Botha, and Futcher assert that we are in the fourth era of information privacy compliance laws such as POPIA.[171] In this fourth era, the context within which privacy and data protection laws apply is one of big data, IoT, cloud computing, social media, and e-government. Advancement of technology creates new privacy concerns and there is need to contextualise data protection.[172] These assertions have been echoed by scholars such as Warren and Brandeis, Solove, and Roos. "When?" question responses should be aligned to emerging privacy concerns.

Makulilo's arguments are that data protection laws "organize and control the way personal data can only be legitimately processed if some conditions pertaining to the transparency of the processing, the participation of the data subject, and the accountability of the data

[168] F Borgesius 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) *International Data Privacy Law* 163 -176.
[169] Ibid 170. See also De Stadler (note 18 above) 197 – 199; E Kosta 'Article 7 Conditions for consent' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 345 – 354.
[170] Ibid 163.
[171] T Agbor, A Kandeh, and L Futcher 'Enforcement of the Protection of Personal Information (POPI) Act : perspective of data management professionals.' (2018) *South African Journal of Information Management* 1 – 9.
[172] *Ibid* 2.

controller are met".[173] "When?" question responses in determining adequacy should be provisions of the law that set out the legitimate conditions for processing personal data. The long title of the KDPA in addition to giving effect to Article 31(c) and (d) of the Constitution, states that the Act is "to make provision for the regulation of processing personal data".

Another essential component of the "when?" question responses is whether data controllers and data processors have paid attention to principles of personal data protection. Section 25 of the KDPA sets out the principles:

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

Article 5 of the GDPR on the other hand sets out the principles relating to data processing:

> 'Personal data shall be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

[173] A Makulilo 'Privacy and Data Protection in Africa: A State of the Art' (2012) *International Data Privacy Law* 164.

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').”[174]

Chapter Three of POPIA sets the “when” in terms of “conditions for lawful processing of personal information”. POPIA lays out conditions as accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation. Under the GDPR and POPIA, there is an emphasis of the principle of “accountability”.

My submission is that when answering the “when?” question, one must flesh out data protection principles and legitimate means through which to process personal data which are a bare minimum for adequate personal data protection regulation.

[174] See C Terwangne ‘Article 5. Principles relating to processing of personal data’ in in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 309 – 320.

3.7.2 Limitations to the right to privacy

Even with adherence to data protection principles and processing personal data through legitimate means, before processing personal data, a data controller or a data processor must be aware that the right to privacy may only be limited within the confines of the Constitution. Further, a data subject ought to know that their right to privacy is not an unlimited right. The right to privacy under Article 31 of the Constitution may be limited within the ambit of Article 24:

(1) 'A right or fundamental freedom in the Bill of Rights shall not be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including—
   (a) the nature of the right or fundamental freedom;
   (b) the importance of the purpose of the limitation;
   (c) the nature and extent of the limitation;
   (d) the need to ensure that the enjoyment of rights and fundamental freedoms by any individual does not prejudice the rights and fundamental freedoms of others; and
   (e) the relation between the limitation and its purpose and whether there are less restrictive means to achieve the purpose.

(2) Despite clause (1), a provision in legislation limiting a right or fundamental freedom—
   (a) in the case of a provision enacted or amended on or after the effective date, is not valid unless the legislation specifically expresses the intention to limit that right or fundamental freedom, and the nature and extent of the limitation;
   (b) shall not be construed as limiting the right or fundamental freedom unless the provision is clear and specific about the right or freedom to be limited and the nature and extent of the limitation; and
   (c) shall not limit the right or fundamental freedom so far as to derogate from its core or essential content.

(3) The State or a person seeking to justify a particular limitation shall demonstrate to the court, tribunal or other authority that the requirements of this Article have been satisfied.'

In the same light, Article 19(3)(c) stipulates that "the rights and fundamental freedoms in the Bill of Rights…are subject only to the limitations contemplated" in the Constitution. A

limitation to the right to privacy ought to be spelt out in written law which in effect should be justified and reasonable.

To determine the borders within which limitations to data protection may be confined, guidance may be sought from the *Special Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*.[175] In the report, the Special Rapporteur of the United Nations Human Right Council, writing on the right to freedom of expression under the International Covenant on Civil and Political Rights,[176] reiterated that limitations to the right to freedom of expression ought to pass a three-part test:

> " (a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); and (b) It must pursue one of the purposes set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals (principle of legitimacy); and (c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality)."[177]

A limitation to personal data protection ought to be predictable, transparent, legitimate, necessary, and proportional. Just like the purposes to limit the right to freedom of expression are articulated by the Special Rapporteur, purposes for limiting data protection should also be stated in law. Details of limitations to personal data protection manifest themselves when carrying out the determination-of-adequacy test.

For the State to meet its constitutional, statutory, and policy obligations, it must process reliable, and real time data, some of which is personal data. Data controllers and data processors process personal data, at times doing so while limiting rights of a data subject. While Article 24 of the Constitution provides for a framework for limitation of fundamental rights and freedoms one ought to bear in mind that rights and freedoms "work as a shield or

[175] UN Human Rights Council "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" 17 April 2013, A/HRC/23/40, available at: <https://www.refworld.org/docid/51a5ca5f4.html > last accessed 23 July 2022.
[176] UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171
[177] UN Human Rights Council (note 175 above).

bulwark" from unnecessary incursions.[178] Fundamental rights and freedoms as limited as some may be, draw "the limits and frontiers of power of the State and of State intervention".[179] Gutwirth and Hert argue:

> 'The constitutional recognition and implementation of the rule of law again tend to limit the power of government, but this time this happens no longer through setting a limit to the reach of the power, but through what one could call a system of 'internal' organisation of government and power. Nonetheless, the objective remains the same, namely the protection of individuals against excessive and arbitrary domination. The main idea of the rule of law is the subjection of government and other state powers to a set of restricting constitutional rules and mechanisms.'[180]

The State must be confined within constitutional principles and provisions especially when seeking to limit fundamental rights and freedoms. As I apply the determination-of-adequacy test, the guiding framework is the constitutional text. State power may only be exercised within a legal framework that binds all public authorities.[181] Exercise of State or public power outside the confines of the law ought to attract sanctions, and society must ensure that "the government is accountable and that its actions must be controllable, and thus transparent".[182]

Kulhari posits that data protection laws promote accountability and transparency when the State is exercising its powers.[183] Laws are not to prohibit State power but to promote meaningful public accountability and give data subjects a chance to challenge inaccuracies or abusive record-keeping practices.[184] The reason for data protection in the public sector is based on the understanding that authorities can easily infringe on data subject rights and that there is a strong desire to acquire, retain, and use data in all administrative systems.[185] Encroaching on fundamental rights and freedoms must have legal basis.[186] As Kulhari argues,

---

[178] S Gutwirth and P Hert 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E Claes, A Duff & S Gutwirth (eds..), *Privacy and the criminal law* (2006) 63,64.
[179] Ibid.
[180] Ibid.
[181] Ibid.
[182] Ibid 65.
[183] S Kulhari 'Data Protection, Privacy and Identity: A Complex Triad' in *Building-Blocks of a Data Protection Revolution* (2018) 75.
[184] Ibid.
[185] Ibid.
[186] Ibid 81.

written law exists to limit rights and freedoms but the law must also be justified in a democratic society.[187]

Where the law providing responses to any of the adequacy determination framework questions is ambiguous and uncertain, it ought not apply; particularly when limiting fundamental rights and freedoms. In *Association of Kenya Insurers (AKI) v Kenya Revenue Authority*[188] the court in considering uncertain, ambiguous, and absurd law, stated that the court "upon finding that the impugned Amendment creates uncertainty, ambiguity and absurdity is obligated to declare it as unconstitutional as the effect of the implementation would infringe a right already guaranteed under the Constitution, in particular, rights under Article 10(2)(a) and 10(2)(d) of the Constitution".[189] In *Katiba Institute vs. Attorney General*[190] the High Court on ambiguity and vagueness stated:

> 'ambiguity and or vagueness in a statutory provision? Do they affect constitutionality of those provisions? In our view, ambiguity or vagueness in statutory provision makes that provision void. A provision will be said to be void where when the average citizen is unable to know what is regulated and the manner of that regulation; or, where the provision is capable of eliciting different interpretations and different results. Such a provision would not meet constitutional quality."[191]

I associate myself with the pronouncements of the courts. Where legislative responses to any questions in the determination-of-adequacy framework are vague, they ought not apply. Specifically, where there is unreasonable limitation of data subject rights.

Balancing public purpose and public interest with a data subject's rights is a dicey affair as there are instances where the balance may tilt against the individual. Posner argues that "people hide from government, and government hides from the people, and people and government have both good and bad reasons for hiding from the other. Complete transparency paralyzes planning and action; complete opacity endangers both liberty and

---

[187] Ibid.
[188] *Association of Kenya Insurers (AKI) Suing through its Chairman Mr. Mathew Koech) v Kenya Revenue Authority & 2 others; Insurance Regulatory Authority (IRA) & another (Interested parties) (Petition 201 of 2020)* [2021] KEHC 402 (KLR).
[189] Ibid 48
[190] Katiba Institute & another vs. Attorney General & another [2017] eKLR.
[191] Ibid 71.

security".[192] But, State officials have the overarching obligation to carry out their functions in public interest, "they must perform their official functions and duties, and exercise any discretionary powers, in ways that promote the public interest that is applicable to their official functions."[193]

On data subjects' rights, it is the State's duty to ensure its actions respect the rights, subject to constitutional and statutory limitations. Often, due to power dynamics, an individual may not be able to ensure respect, protection, and promotion of their rights. In view of this, Solove argues that fundamental rights and freedoms are often expected to provide protections that they may not deliver.[194] Solove posits that for effective protection of the right to privacy, it is not just about granting individuals privacy and data protection rights, but also ensuring control over processing of personal data.[195] Control operates within set out legal limitations and according to Solove, "the more practical and effective aim is to bring the data ecosystem under better control".[196] In my view, control lies in responses to the "when?" question.

At the very least, there is constant need to rein on State public purpose and public interest use of personal data which must be within the confines of Article 24 of the Constitution. Article 24 limitations are similar to the limitations laid out under the Siracusa principles which I discuss in the next section.[197]

[192] R. Posner 'Privacy, Surveillance, and Law' (2008) *The University of Chicago Law Review* 246.
[193] C Wheeler "The Public Interest We Know It's Important, But Do We Know What It Means" AIAL FORUM No. 48. Available at < 2.pdf (austlii.edu.au)> last accessed 27 August 2022.
[194] D Solove 'The Limitations of Privacy Rights' (2022) *George Washington University Law School, Legal Studies Research Paper Series.*
[195] Ibid 5.
[196] Ibid 6.
[197] UN Commission on Human Rights "The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights" 28 September 1984, E/CN.4/1985/4, available at: <https://www.refworld.org/docid/4672bc122.html> last accessed 27 January 2022.

3.7.3 Derogations and the Siracusa Principles

The Siracusa Principles focus on derogations under Article 4(1) of the International Covenant on Civil and Political Rights (ICCPR):[198]

> 'In time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed, the States Parties to the present Covenant may take measures derogating from their obligations under the present Covenant to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin.'

The right to privacy is one of the rights a State may derogate from in "time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed". Austin argues that what constitutes a national emergency is debatable.[199] National emergencies as per Austin occur in such a manner that they are difficult to anticipate and react to.[200] When interrogating the legality of State public purpose and public interest use of personal data it is key to note that in many cases the State seeks to use its discretionary powers for actions that are not expressly set out in the law.[201] Kenya is yet to signal a need to derogate from the right to privacy as provided for under the ICCPR. While the derogations are for times of emergency, they offer guidelines on how the State should act when seeking to limit fundamental rights and freedoms.

Hafner-Burton, Heifer, and Fariss assert that derogations from fundamental rights and freedoms are key at times of crisis.[202] Derogations apply to State surveillance discussed in chapter four of this study. According to Hafner-Burton, Heifer, and Fariss derogations work

---

[198] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).
[199] L Austin 'Lawful Illegality: What Snowden Has taught Us about the Legal Infrastructure of the Surveillance State' (2015) *in* M Geist (ed) *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* 105.
[200] Ibid.
[201] Ibid 106.
[202] E Hafner-Burton, L Heifer, and C Fariss 'Emergency and Escape: Explaining Derogations from Human Rights Treaties' (2011) *International Organization* 674, 675.

as "safety valves" for the State to enable them deal with crises.[203] Hafner-Burton, Heifer, and Fariss submit that where a State derogates from a fundamental right and freedom, it is most likely to derogate again.[204] Secondly, States with weak democratic and judicial structures will not adhere to derogation guidelines. Thirdly, States with strong democratic and judicial structures will operate within the confines of the outlined derogations.[205]

Hafner-Burton, Heifer, and Fariss reason that derogations are rational and enable "governments to buy time and legal breathing space from voters, courts, and interest groups to combat crises by temporarily restricting civil and political liberties. A derogation sends a credible signal to these domestic actors—many of whom are predisposed to challenge or find fault with such restrictions—that suspending rights is necessary, temporary, and lawful".[206] The Siracusa Principles guide on how to strike a balance between State actions and an individual's fundamental rights and freedoms.

Though not binding, the Siracusa Principles provide direction to governments when they are limiting or derogating from ICCPR rights. Article 17(1) of the ICCPR provides for the right to privacy stating that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". The ICCPR allows for limitations when "prescribed by law", "in a democratic society", for "public order (*ordre public*)", for "public health", for "national security", and for "public safety".

On "prescribed by law" Principle 15 of the Siracusa Principles states that "no limitation on the exercise of human rights shall be made unless provided for by national law of general application which is consistent with the Covenant and is in force at the time the limitation is applied". My submission in this study is that any incursion into data protection must be expressly provided for in legislation and be for a reasonable purpose.

[203] Ibid.
[204] Ibid 675.
[205] Ibid.
[206] Ibid 680.

Principle 16 also provides that "laws imposing limitations on the exercise of human rights shall not be arbitrary or unreasonable". Gill and Jaiswal are of the view that a surveillance State that is not subjected to laws that check its intrusive nature "poses much greater harm to society with respect to individual privacy than what is saliently visible".[207] For the rule of law to prevail any government action must be subjected to the law.[208]

Principle 15 is echoed in the International Principles on the Application of Human Rights to Communications Surveillance written by privacy organisations and experts.[209] On legality, the International Principles on Application of Human Rights to Communications Surveillance state:

> 'Any limitation to human rights must be prescribed by law. The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technological changes, laws that limit human rights should be subject to periodic review by means of a participatory legislative or regulatory process.'[210]

Principle 17 indicates that "legal rules limiting the exercise of human rights shall be clear and accessible to everyone". Article 10 of the Kenyan Constitution cites "participation of the people" as one of the national values and principles of governance. Laws that limit the right to privacy must at first instance be subjected to public participation and secondly, once enacted, the laws should be accessible to all. On the aspect of transparency, the International Principles on Application of Human Rights to Communications Surveillance posit that "States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance".[211] This is

[207] A Gill and A Jaiswal 'Data Surveillance: Need for A Policy To Achieve Equilibrium Between State And Individual Interest' (2018) *Nirma University Law Journal* 61.
[208] Austin (note 190 above) 104.
[209] Necessary and Proportionate "International Principles on the Application of Human Rights to Communications Surveillance" (2014) < EN Princples (necessaryandproportionate.org)>.
[210] Ibid 7.
[211] Ibid 10.

in line with a data subject's right to be informed of data processing operations involving their personal data.

Principle 18 provides that "adequate safeguards and effective remedies shall be provided by law against illegal or abusive imposition or application of limitations on human rights". In chapter six of this study, I discuss access to effective remedies. Adequate safeguards and effective remedies include effective administrative and judicial protection that address violations. The International Principles on Application of Human Rights to Communications Surveillance provide that adequate safeguards and effective remedies necessitate the need to have due process.[212]

Due process under the International Principles is stated as the need for States to respect and ensure an individual's fundamental rights and freedoms are upheld.[213] This requires that authorized procedures governing any interference with human rights are correctly enumerated in law, consistently practiced, and accessible to the public.[214] Individuals are entitled to a fair and public hearing by an independent, competent, and impartial tribunal established by law in the assessment of their fundamental rights and freedoms, except in circumstances of emergency when there is an imminent risk of harm to human life.[215]

On limitations "in a democratic society", Principle 20 states that "the burden is upon a state imposing limitation so qualified to demonstrate that the limitations do not impair the democratic functioning of the society". In this chapter I have discussed the harms that may be occasioned upon a data subject through incursions into their privacy. Where incursions cause harm, then they are excessive and ought to be halted.

Principle 25 on "public order (*ordre public*)" stipulates that "state organs or agents responsible for the maintenance of public order (*ordre public*) shall be subject to controls in the exercise of their power through the parliament, courts, or other competent independent bodies". First, jurisprudence from the Kenyan courts has gone a long way to protect

[212] Ibid.
[213] Ibid 9.
[214] Ibid 9.
[215] Ibid 9

fundamental rights and freedoms including the right to privacy as was discussed in chapter two this study. Secondly, as discussed in chapter six of this study, the Office of the Data Protection Commissioner established under the KDPA should be competent and independent when providing oversight and addressing complaints by data subjects.

Principle 29 on "national security" provides that "national security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force". Further, Principle 30 indicates that "national security cannot be invoked as a reason for imposing limitations to prevent merely local or relatively isolated threats to law and order".

In chapter four of this study, I interrogate the adequacy of regulating State surveillance and I delve into the justification for limiting the right to privacy for national security purposes. As Principle 31 states, "national security cannot be used as a pretext for imposing vague or arbitrary limitations and may only be invoked when there exist adequate safeguards and effective remedies against abuse". This may be read together with Principle 33 on "public safety" stating that "public safety means protection against danger to the safety of persons, to their life or physical integrity, or serious damage to their property".

The derogation provisions and the Siracusa Principles emphasise that derogations and limitations must be proportional to their purpose. Does a State use the least restrictive means to apply a limitation or a derogation? In the next section I expound on the need to undertake a proportionality test when limiting data subject rights.

3.7.4 Proportionality test

In addition to Article 24 and the Siracusa Principles, when determining the constitutionality and legality of processing personal data, one must inquire into whether the processing is proportional to the protection and the limitation of the right to privacy. With Article 24(1)(e) as the reference point, the proportionality test is instrumental in evaluating whether the State

has adopted the least restrictive means to achieve its purpose when limiting data subject rights. This is due to the fact that there will always be conflict between an individual's rights and State's need for personal data.[216]

Macnish describes proportionality as an assessment that indicates that "the harms of a particular act not outweighing the benefits of that act".[217] Where harms caused by an act outweigh the benefits of the act, the act is considered disproportionate.[218] Macnish argues that for the call to be made whether an act is proportionate or disproportionate, the difference between the harms and benefits ought to be significant.[219] While it may not be possible to have a uniform harm versus benefits scale, acts may be balanced on a case-to-case basis.[220] Huscroft, Miller, and Webber proposed a proportionality test executed by asking four questions:

1. 'Does the legislation (or other government action) establishing the right's limitation pursue a legitimate objective of sufficient importance to warrant limiting a right?
2. Are the means in service of the objective rationally connected (suitable) to the objective?
3. Are the means in service of the objective necessary, that is, minimally impairing of the limited right, taking into account alternative means of achieving the same objective?
4. Do the beneficial effects of the limitation on the right outweigh the deleterious effects of the limitation; in short, is there a fair balance between the public interest and the private right?' [221]

The South African Constitutional Court in *S v Makwanyane*[222] while considering proportionality in limitation of rights stated that:

> 'In the balancing process, the relevant considerations will include the nature of the right that is limited, and its importance to an open and democratic society based on freedom and equality; the purpose for which the right is limited and the importance of that purpose to such a society; the extent of the

[216] A Gill and A Jaiswal (note 207 above) 61.
[217] K Macnish 'An Eye for an Eye: Proportionality and Surveillance' (2015) *Ethical Theory and Moral Practice* 532.
[218] Ibid.
[219] Ibid.
[220] Ibid 539.
[221] G Huscroft, B Miller, and G Webber 'Proportionality and the Rule of Law: Rights, Justification, Reasoning' (2014) *Cambridge University Press* 21.
[222] *S v Makwanyane and Another* (CCT3/94) [1995] ZACC 3; 1995 (6) BCLR 665; 1995 (3) SA 391; [1996] 2 CHRLD 164; 1995 (2) SACR 1 (6 June 1995).

limitation, its efficacy, and particularly where the limitation has to be necessary, whether the desired ends could reasonably be achieved through other means less damaging to the right in question.'[223]

In the Canadian case of *R. v Oakes*, the court held that the proportionality test is made up of three components, first, "the measures must be fair and not arbitrary, carefully designed to achieve the objective in question and rationally connected to that objective".[224] Secondly, "the means should impair the right in question as little as possible".[225] Thirdly, "there must be a proportionality between the effects of the limiting measure and the objective -- the more severe the deleterious effects of a measure, the more important the objective must be."[226]

The Kenyan High Court applied the proportionality test in *Jacqueline Okuta v Attorney General*.[227] The court expressed itself by arguing that the proportionality test is a "fluid test" that necessitates analysis and application of the law while having "regard to the surrounding circumstances, including recent developments in the law, current political and policy challenges and contemporary public interest considerations".[228] The court reasoned that a proportionality test "preserves rights, provides a framework for balancing competing rights and enables other important public concerns, such as national security and public order, to be duly taken into account".[229]

Where the test is being applied to an administrative action, the Kenyan High Court in *James Opiyo Wandayi v Kenya National Assembly*[230] citing *R (Daly) vs. Secretary of State for Home Department*[231] held:

1. 'Proportionality may require the reviewing Court to assess the balance which the decision maker has struck, not merely to see whether it is within the range of rational or reasonable decisions;

[223] Ibid 104.
[224] *R v Oakes* [1986] 1 SCR 103.
[225] Ibid.
[226] Ibid.
[227] *Jacqueline Okuta & another v Attorney General & 2 others* [2017] eKLR.
[228] Ibid.
[229] Ibid.
[230] *James Opiyo Wandayi v Kenya National Assembly & 2* others [2016] eKLR.
[231] *R (Daly) vs. Secretary of State for Home Department* (2001) 2 AC 532.

2. Proportionality test may go further than the traditional grounds of review in as much as it may require attention to be directed to the relative weight accorded to interests and considerations; and
3. Even the heightened scrutiny test is not necessarily appropriate to the protection of human rights.'[232]

The Court of Justice of the European Union when considering the legality and necessity of mass surveillance when limiting the right to privacy in *Digital Rights v. Ireland* was of the view that "it is necessary to verify the proportionality of the interference found to exist". [233] The court asserted that derogations and limitations that relate to personal data should be applicable in cases of actual necessity.[234]

My take is that responses to the "when?" question must be subjected to the "proportionality test". In relation to data protection, the "proportionality test" should have the following questions bearing in mind the prevailing circumstances at the time:

First, is the law or action limiting a data subject's rights of such importance to warrant the limitation? Secondly, is how the limitation is being carried out suitable in relation to the goal? Thirdly, are there other measures available that would ensure minimal interference with a data subject's rights? Fourthly, do the benefits of limiting a data subject's rights outweigh the need for protection of the right?

In conclusion, at the point of inquiring into "when?" question responses, one ought to pay attention to the whether they are exploiting limitations of the right to privacy as per constitutional principles. Secondly, the "when?" question responses ought to ensure that data protection rights of the individual are taken into consideration. Thirdly, the legitimate or lawful reasons for making incursions into an individual's right to privacy ought to be clearly set out in law, with no ambiguities.

[232] *James Opiyo Wandayi v Kenya National Assembly & 2 others* (note 230 above) 24.
[233] *Digital Rights v. Ireland* [2014] ECLI:EU:C:2014:238, para 45.
[234] Ibid 52.

3.8 "Where"?

The response to the "where?" question deals with jurisdiction; the territory within which data protection regulation applies.[235] Personal data protection regulation must at a minimum define its territorial boundaries. Section 4 of the KDPA on jurisdiction states that the Act applies to personal data processing:

> '(a) entered in a record, by or for a data controller or processor, by making use of automated or non-automated means:
>
> Provided that when the recorded personal data is processed by non-automated means, it forms a whole or part of a filing system;
>
> (b) by a data controller or data processor who—
>
> (i) is established or ordinarily resident in Kenya and processes personal data while in Kenya; or
>
> (ii) not established or ordinarily resident in Kenya but processing personal data of data subjects located in Kenya.'

In contrast, Article 3 of the GDPR refers to jurisdiction as "territorial scope".[236] As for POPIA, section 3(1) on application states that the Act applies to processing of personal information—

> 1. 'entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and
> 2. where the responsible party is—
>
> 1. domiciled in the Republic; or
>
> 2. not domiciled in the Republic but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.'[237]

[235] The Black's Law Dictionary (9th Edition) defines jurisdiction as "a government's general power to exercise authority over all persons and things within its territory".
[236] See D Svantesson 'Article 3. Territorial scope' in in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 74 – 99.
[237] See De Stadler (note 18 above) 85 – 88.

Provisions in the KDPA, the GDPR and POPIA point to extraterritorial application of the law. In Kenya, extraterritorial application comes into play where data controllers and data processors not established or resident in Kenya process personal data of "data subjects located in Kenya". In addition to such application, there are conditions for transfer of personal data outside Kenya. Section 48 of the KDPA lays out conditions for transfer of personal data outside Kenya while section 49 of the Act sets out safeguards required prior to transfer taking place, and section 50 indicates that there may be restrictions to personal data transfers. In juxtaposition, Chapter V of the GDPR regulates transfer of personal data to third countries and international organisations.[238] Similar provisions are found in section 72 of POPIA on "transfers of personal information outside Republic".[239]

I find the European Data Protection Board (EDPB) Guidelines on territorial application of the GDPR useful while seeking to interpret the territorial scope of the KDPA.[240] Section 3 of the KDPA refers to data controllers or data processors "established or ordinarily resident in Kenya". The EDPB Guidelines frown upon an overly formalistic determination of where a data controller or data processor is established.[241] The Guidelines note that "establishment extends to any real and effective activity… even a minimal one… exercised through stable arrangements".[242] Secondly, "the EDPB recommends that non-EU organisations undertake an assessment of their processing activities, first by determining whether personal data is being processed, and secondly by identifying potential links between the activity for which the data is being processed and the activities of any presence of the organisation in the Union".[243] Thirdly, the EDPB notes:

[238] See C Kuner 'Chapter V: Transfers of Personal Data to Third Countries or International Organisations (Articles 44–50)' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 755 – 856.
[239] See De Stadler (note 18 above) 421 - 440; Burns and Burger-Smidt (note 18 above) 121 – 132.
[240] European Data Protection Board Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) < edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf (europa.eu)> last accessed 21 December 2022.
[241] Ibid 5 – 7.
[242] Ibid.
[243] Ibid 8.

> 'It is the presence, through an establishment, of a data controller or processor in the EU and the fact that a processing takes place in the context of the activities of this establishment that trigger the application of the GDPR to its processing activities. The place of processing is therefore not relevant in determining whether or not the processing, carried out in the context of the activities of an EU establishment, falls within the scope of the GDPR.'[244]

The EDPB provides that the Guidelines in some circumstances are to be applied on a case-to-case basis. What I note from the EDPB Guidelines is that they shine a light on the statutory provisions. My hope is that the Kenyan Courts and the Office of the Data Protection Commissioner will adopt an interpretation similar to the EDPB Guidelines. The KDPA, the GDPR and POPIA provisions on territorial application have a similar theme. What is lacking is guidelines to unpack the application of the provisions. My conclusion is that for certain data protection provisions, adequate regulation will mean that the relevant authorities provide nuanced guidelines as the EDPB has done in this case. Interpretation of jurisdiction provisions must not be overly formalistic and rigid.

3.9 "How?"

The "how?" question response has three components which at a minimum must feature in personal data protection regulation, first, the laws that indicate the manner data processing is carried out, secondly, how oversight by independent data protection authorities may be exercised, and thirdly, how a data subject may access effective remedies.

3.9.1 General responses

When processing of personal data is taking place, Solove, defines privacy intruding conduct to involve "(a) information collection; (b) information processing; (c) information

[244] Ibid 9.

dissemination; and (d) invasion".[245] These four notions by Solove, in the Kenyan context refer to personal data processing defined under section 2 of the KDPA:

> '... any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as
>
> (a) collection, recording, organisation, structuring;
> (b) storage, adaptation or alteration;
> (c) retrieval, consultation or use;
> (d) disclosure by transmission, dissemination, or otherwise making available; or
> (e) alignment or combination, restriction, erasure or destruction.'

Section 2 above mirrors the provisions of Article 4(2) of the GDPR and section 1 of POPIA.[246] My take is that the definition is sufficient and that the first aspect of responding to the "how?" question examines whether the personal information sought is being subjected to at least one of the actions cited above. In section 3.9.1 below I delve deeper into aspects of processing personal data with a focus on profiling and use of technology for processing activities.

The second aspect of the "how?" question response relates to oversight by an independent authority. The Office of the Data Commissioner's is established under Part II of the KDPA with one of its core functions under section 8 being overseeing "the implementation of and be responsible for the enforcement" of the Act. Similarly, the GDPR provides for an independent authority under Article 51 and section 39 of POPIA establishes the Information Regulator and section 40 of POPIA lays down the powers, duties, and functions of the Regulator.[247] The difference I note between the KDPA, the GDPR and POPIA is that the regulator under the KDPA is not fully independent. As I explained in chapter one of this study, the Cabinet

[245] D Solove 'A Taxonomy of Privacy' (2006) *University of Pennsylvania Law Review* 489.
[246] See L Tosoni and L Bygrave 'Article 4(2). Processing' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 116 – 122; Burns and Burger-Smidt (note 18 above) 25 – 27.
[247] See H Hijmans 'Article 51. Supervisory authority' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 863 – 872; T Zerdick 'Article 52. Independence' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 873 – 883; Burns and Burger-Smidt (note 18 above) 201 – 218.

Secretary in charge of information, communication, and technology has a role to play in data protection regulation in Kenya. This is one of the areas I propose law reforms.

The third aspect of the "how?" question responses is access to effective remedies. Section 56(1) of the KDPA provides that "a data subject who is aggrieved by a decision of any person under this Act may lodge a complaint with the Data Commissioner". Section 64 of the KDPA states that "a person against whom any administrative action is taken by the Data Commissioner, including in enforcement and penalty notices, may appeal to the High Court". Section 65 provides for compensation for a data subject who suffers damage by reason of infractions by data controllers and data processors.

For the GDPR, Article 56(2) states that each supervisory authority is "competent to handle a complaint lodged with it".[248] POPIA on the other hand under section 74 provides that "any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject".[249] In relation to an effective remedy, Article 79 of the GDPR provides for a right to an effective remedy against a data controller or a data processor.[250] On compensation, Article 82 of the GDPR has provision for the right to compensation while section 99 of POPIA grants aggrieved parties powers to institute civil action for damages.[251] What I note here is that the KDPA, the GDPR and POPIA have provisions for making complaints and seeking remedies for damages. However, what is yet to be seen is how the Kenyan courts will compute damages provided for under section 65 of KDPA.

[248] See Hijaman (note 247 above).
[249] See Burns and Burger-Smidt (note 18 above) 144.
[250] See W Kotschy 'Article 79 Right to an effective judicial remedy against a controller or processor' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 1122 - 1141
[251] See G Zanfir-Fortuna 'Article 82 Right to compensation and liability' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 1160 – 1179; Burns and Burger-Smidt (note 18 above) 255 – 258.

3.9.2 Profiling and use of technology

As I discuss processing of personal data, it is crucial that I delve into profiling and use of technology that are at the centre of personal data processing. As part of the responses to the "how?" question, it is critical to examine whether the law adequately deals with profiling and use of technology. Section 2 of the KDPA defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behaviour, location or movements".

Profiling is at the centre of personal data processing. Section 35(1) of the KDPA stipulates that a "data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject". Section 35(3) goes further:

> 'Where a data controller or data processor takes a decision, which produces legal effects or significantly affects the data subject based solely on automated processing—
>
> (a) the data controller or data processor must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing; and
> (b) the data subject may, after a reasonable period of receipt of the notification, request the data controller or data processor to—
>
> (i) reconsider the decision; or
>
> (ii) take a new decision that is not based solely on automated processing.'

Articles 21 and 22 of the EU's GDPR and Section 71 of POPIA have provisions similar to section 35 of the KDPA on regulation of profiling and automated decision making.[252] The legal effects of profiling are identified through responses to the "how?" question and carrying out the

[252] See L Bygrave 'Article 4(4). Profiling' in in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 127 – 131; De Stadler (note 18 above) 443 – 468.

"proportionality test". Profiling as identified by section 35 of the KDPA produces legal effects to the data subject which may include limitation of the right to privacy and other fundamental rights and freedoms.

Kulhari notes that it is important to pay attention to profiling because of the legal effects it has towards an individual.[253] Any processing of personal data through profiling or otherwise ought to be for specified and acceptable societal reasons.[254] Evaluating profiling is a more nuanced approach towards carrying out the "proportionality test". Profiling is mostly executed through use of technology with some technology having capacity to make automated decisions without the need for human intervention.

Profiling facilitates data surveillance. Hu reiterates that in the digital era, there is proliferation of cybersurveillance and data surveillance that cut across public and private sectors.[255] Cybersurveillance and data surveillance is facilitated, first, by collection of large amounts of personal data which includes biometric data, biographic data, internet, and social media profiling.[256] Hartzog and Selinger remind us that application of applied technology to surveillance has made former manpower intensive activities easy.[257]

Public and private processing of personal data requires large volumes of data. Veliz argues that today's surveillance society was created through collaboration between public and private sectors.[258] States allow corporate mass collection of personal data so that they may have access to such data.[259] Profiling and surveillance by the State is facilitated by private actors.[260] It is critical that profiling operations be subjected to the "proportionality test".

There are harms that may be occasioned through automated processing and profiling. To avert harms that may result from technology such as Artificial Intelligence (AI), algorithmic

[253] S Kulhari 'Data Protection, Privacy and Identity: A Complex Triad' in *Building-Blocks of a Data Protection Revolution* (2018) 30.
[254] Ibid 72.
[255] M Hu 'Algorithmic Jim Crow' (2017) *Fordham Law Review* 639.
[256] Ibid 640, 641.
[257] W Hartzog and E Selinger 'Surveillance as Loss of Obscurity' (2015) *Washington and Lee Law Review* 1344.
[258] C Veliz *Privacy is Power* (Kindle Edn 2020) Ch 2.
[259] Ibid.
[260] Ibid.

transparency is necessary. The major fear of automated processing is algorithmic bias; algorithms designed for technologies such as AI have exhibited bias that may be attributed to their developers and the individuals from which large volumes of data are processed from. Bias has impact on AI decision making in areas such as health, housing, education, and political processes.[261]

Tschider recapitulates the fact that data is the foundation of AI and that AI requires exceptionally large volumes of data to carry out its operations.[262] The quality of these operations are determined by the quality and volumes of data which are stored in databases.[263] Decisions based on AI operations may be fair and free from bias depending on the diversity of data available for scrutiny.[264] Tschider makes the case that "AI does not simply require data, but it requires that data are available from a variety of data populations and collection contexts. Data must be quality, well-organized, appropriately labelled, and reliably sourced to ensure AI systems perform safely, efficaciously, and fairly".[265]

In the quest to ensure that AI is safe, fair, and free from bias, the Report of the Special Rapporteur on the right to privacy focusing on artificial intelligence, privacy, and children's privacy in addition to emphasis on the need for compliance with privacy and data protection principles, sets eight principles that are key in the planning, development, and implementation of AI solutions.[266] The principles are, jurisdiction, ethical and lawful basis, data fundamentals, responsibility and oversight, control, transparency and explainability, rights of the data subject, and safeguards.[267] Transparency and explainability demand that an individual using algorithms to reach certain decisions ought to be able to clarify about the process to decide and the decision made.

[261] S Russell *Human Compatible: AI and the Problem of Control* (Kindle Edn. 2019) Ch. 4.
[262] C Tschider 'AI's Legitimate Interest: Towards A Public Benefit Privacy Model' (2021) *Houston Journal of Health Law & Policy* 132.
[263] Ibid 133.
[264] Ibid 135, 136.
[265] Ibid 138.
[266] Artificial intelligence and privacy, and children's privacy: Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci A/HRC/46/37.
[267] Ibid 4, 5.

Felten identifies four challenges related to explainability.[268] First, is where individuals with knowledge about the decision-making process deliberately reject calls to reveal relevant information.[269] Secondly, is complexity of the algorithm that makes it a challenge to provide an explanation.[270] Thirdly, is where the result of the automated decision-making process does not make sense despite having the current data input and correct algorithm formula.[271] Fourthly, where the algorithm is inconsistent with basic constitutional and rule of law principles, most probably an explanation will not be forthcoming.[272]

Emerging technologies play a key role in facilitating State surveillance and surveillance capitalism. Technologies are designed to process personal data; they can carry out all the processing operations outlined in the definition of "processing" under section 2 of the KDPA. The technologies can also undertake automated individual decision making which is regulated under Section 35 of the KDPA and Regulation 22 of the Data Protection (General) Regulations, 2021.[273]

Russell points out that smart technology, that is the IOT, require a substantial amount of data to be effective; this data includes personal data of the users.[274] IOT include digital assistants, home intelligent systems, self-driving cars among other technologies.[275] While AI technology is invaluable, Russel argues that users of the technology need not give away their privacy to enjoy the benefits.[276] The key question is whether AI technology developers would adhere to data protection principles without concrete regulation.[277]

[268] E Felten "What does it mean to ask for an "explainable" algorithm?" (2017) < What does it mean to ask for an "explainable" algorithm? (freedom-to-tinker.com)> last accessed 10 July 2022.
[269] Ibid.
[270] Ibid.
[271] Ibid.
[272] Ibid
[273] Legal Notice No. 263 of 2021.
[274] Russell (note 261 above).
[275] Ibid Ch. 3.
[276] Ibid Ch. 3.
[277] Ibid Ch. 3.

AI is a constantly evolving technology that makes incursions into data protection. Article 3 of the proposed EU Artificial Intelligence Act describes AI as a software that is developed with one or more of the following techniques and approaches:

(a) 'Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
(c) Statistical approaches, Bayesian estimation, search and optimization methods.'[278]

The above techniques and approaches as per Article 3 are "for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".[279] AI is critical for provision of health care services, banking, insurance, transportation, and education among others. Cath indicates that AI enhances "economic, social welfare and the exercise of human rights".[280] Cath also points to the fact that more and more, societies are seeking to delegate high risk processes such as "granting parole, diagnosing patients and managing financial transactions" to AI systems.[281]

Emerging technologies such as AI operate within the framework of profiling. Section 35 of the KDPA provides that a "data subject has a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject". The major fear of automated processing is algorithmic bias; algorithms designed for technologies such as AI have exhibited bias that may be attributed to their developers. Bias has impact on AI decision making in areas such as health, housing, education, and political processes.[282]

[278] EU "Artificial Intelligence Act", Brussels, 21.4.2021, COM(2021) 206 final. 2021/0106(COD) available at < EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)> last accessed 17 August 2022.
[279] Ibid.
[280] C Cath 'Governing artificial intelligence: ethical, legal and technical opportunities and challenges (2018) *Philosophical Transactions of the Royal Society* 2.
[281] Ibid.
[282] Russell (note 261 above) Ch. 4.

Mhlambi identifies five challenges facing AI, first, is "exclusion of marginalized communities in the design".[283] Mhlambi points to the fact that in the design of AI, in most cases, the designers do not include engineers from racial, ethnic, and gender minorities.[284] This in turn brings about the next challenge which is "bias in procedure and data".[285] These are sentiments echoed by Birhane who states that in the case of AI, it is built "with values, norms, and interests of Western societies" which at times are not the same as African values, norms, and interests.[286] Development and use of AI tends to forget that data required actually comes from human beings and as Birhane states, processing of data potentially entails "monitoring, tracking, and surveilling people" without consideration of values, norms and interests.[287] This as per Birhane is the same modus operandi of colonialism that violently appropriated natural resources throughout the African continent to the detriment of the Africans.[288]

Secondly, according to Mhlambi, the selection of data to be used in AI is biased and that the AI system embeds the bias of its creators.[289] Thirdly, Mhlambi discuses "the failure to recognize the interconnectedness of society".[290] Here, Mhlambi highlights the social, economic, and political effects AI may have on society while the AI itself is built with individuals in mind.[291] This causes disruptions and inequities in the social, economic, and political spheres of society.[292] Fourthly, "the commodification of our digital selves".[293] On this Mhlambi states:

> 'The commodification resulting from designing one-sided objectives—objectives ultimately designed to increase a company's profits, sometimes through the capture of a user's attention—results in a diminished digital representation of ourselves and treats people as a means rather than an end. The

[283] M Mhlambi 'From Rationality to Relationality: Ubuntu as an Ethical & Human Rights Framework for Artificial Intelligence Governance' (2020) *Carr Center Discussion Paper* 20.
[284] Ibid.
[285] Ibid 21.
[286] A Birhane 'Algorithmic Colonization of Africa' (2020) *SCRIPTed* 395.
[287] Ibid 397.
[288] Ibid.
[289] Mhlambi (note 283 above) 21.
[290] Ibid.
[291] Ibid.
[292] Ibid.
[293] Ibid 22.

> extraction of our data reduces a holistic view of a person and leads to models designed to maximize profit.
>
> Algorithmic personalization and individualization, void of the consent and cooperation of those who will be affected by such algorithms, may also lead to processes of dehumanization that reduce individuals to mere commodifiable metrics.'[294]

Fifthly, Mhlambi talks about "the centralization of data and resources", that is "power is centralized among a few companies, countries, and continents through the centralization of data, capital, capabilities, and infrastructure that is required when producing artificial intelligence systems."[295]

Cath identifies challenges emanating from AI such as "role of the law, ethics and technology in governing AI systems".[296] AI systems raise questions relating to fairness, transparency, privacy, algorithmic fairness, transparency, accountability, and interpretability.[297] Slaughter, Kopec, and Batal also raise challenges relating to AI similar to those highlighted by Cath.[298] Slaughter, Kopec, and Batal explain the origins of algorithmic harms, first, they are caused by faulty input of data.[299] Where data is of low quality and a reflection of human bias and prejudices, Slaughter, Kopec, and Batal indicate that "these faulty inputs can create biased algorithms that exacerbate injustice".[300] The second origin of algorithmic harms is faulty conclusions which are caused by the input of faulty data.[301] The technology is also imperfect and just like human error in decision making, AI is also prone to errors.[302] The third origin is failure to test:

[294] Ibid.
[295] Ibid 23.
[296] Cath (note 280 above).
[297] Ibid.
[298] R Slaughter, J Kopec, and M Batal 'Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission (2021) *ISP Digital Future Whitepaper & Yale Journal of Law and Technology Special Publication*.
[299] Ibid 7.
[300] Ibid 7,8.
[301] Ibid 10.
[302] Ibid 13, 14.

> 'even if an algorithm is designed with care and good intentions, it can still produce biased or harmful outcomes that are unanticipated. Too often, algorithms are deployed without adequate testing that could uncover these unwelcome outcomes before they harm people in the real world'.[303]

There is need to not only input quality data but to also test the algorithm using different data sets continuously before deploying it to possibly avert any potential harms.[304] The harms caused as Slaughter, Kopec, and Batal indicate include discrimination, surveillance capitalism, and threats to competition.[305]

To maximise profitability from AI, AI architects design AI algorithms using what are termed as "dark patterns" which Brignull defines as "tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something".[306] Dark patterns are for the benefits of the designer and in the case of this study for the benefits of State surveillance and surveillance capitalists that wish that the data subject act or behave in a defined manner for a profit.[307] Dark patterns are frowned upon "because they mislead users into making choices that are not in their interest, and deprive them of their agency. This is particularly problematic given the power imbalances and information asymmetries that already exist between many service providers and their users."[308] It is my view that for personal data protection regulation to be adequate, the regulation must have provisions for AI.

Section 74 of the KDPA empowers the Data Commissioner to "offer data protection certification standards, data protection seals, and marks to encourage compliance of processing operations with the Act and require certification or adherence to code of practice

---

[303] Ibid 15, 16.
[304] Ibid 17.
[305] Ibid 20 – 37. See also F Raso, H Hilligoss, V Krishnamurthy, C Bavitz, and L Kim 'Artificial Intelligence & Human Rights Opportunities & Risks' (2018) *The Berkman Klein Center for Internet & Society Research Publication Series* available at <https://cyber.harvard.edu/publication/2018/artificial-intelligence-human-rights> last accessed 18 March 2022.
[306] H Brignull "What are dark patterns?" Available at < Dark Patterns> last accessed 22 March 2022.
[307] See J King and A Stephan 'Regulating Privacy Dark Patterns In Practice—Drawing Inspiration From California Privacy Rights Act' (2021) Georgetown Law Technology Review 26.
[308] Forbrukerradet "Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy" (2018) available at < 2018-06-27-deceived-by-design-final.pdf (forbrukerradet.no)> 7 last accessed 23 March 2022.

by a third party". I argue that where legal reforms are not effected, this is Kenya's entry point to regulating AI technology.

The Panel for the Future of Science and Technology of the European Parliament proposed a "A governance framework for algorithmic accountability and transparency".[309] Some of the proposals include the need for awareness raising on algorithmic accountability, accountability in public sector use of algorithmic decision-making, regulatory oversight and legal liability of the private sector, and the global dimension of algorithmic governance.[310]

To deal with the challenges brought about by AI, the EU proposed the "Artificial Intelligence Act".[311] The EU recognises that AI "is a fast-evolving family of technologies that can bring a wide array of economic and societal benefits across the entire spectrum of industries and social activities" but "can also bring about new risks or negative consequences for individuals or the society".[312] Hence, the need for the proposed EU Artificial Intelligence Act whose objectives are to:

a) 'ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
b) ensure legal certainty to facilitate investment and innovation in AI;
c) enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
d) facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.'[313]

Highlights of the EU Artificial Intelligence Act include Article 5 that prohibits certain uses of AI, Article 6 sets out rules for classification of high-risk AI. Article 9 requires the adoption of AI risk management systems to ensure mitigation of risks associated with AI. Article 10 mandates that any data sets used in AI be subject to EU data governance and management policies. Article 43 requires conformity assessments to be carried out on AI systems. Article 52

[309] The Panel for the Future of Science and Technology of the European Parliament 'A governance framework for algorithmic accountability and transparency' (2019).
[310] Ibid.
[311] EU Artificial Intelligence Act (note 278 above).
[312] Ibid 1.
[313] Ibid 3.

calls for transparency in use of AI systems such that individuals are informed beforehand that they are interacting with AI systems. Article 59 provides for establishment or designation of AI oversight authorities. Article 71 provides for penalties for non-compliance with the Act.

My conclusion on these matters is that any personal data protection regulation that is not specific on AI and technology in general is inadequate. In my view, any proposed law reforms on regulation of AI in Kenya should use the EU's Artificial Intelligence Act as a point of reference. This would bolster data protection regulation on profiling, automated decision making, and use of technology generally. Closely related to AI and technology is digital and algorithmic colonialism that I discuss in the next section.

3.9.3 Digital and algorithmic colonialism

In addition to profiling, AI, and use of technology generally, "digital colonialism" impacts negatively on personal data processing. Coleman defines "digital colonialism" to mean "the decentralized extraction and control of data from citizens with or without their explicit consent through communication networks developed and owned by Western tech companies."[314]

Coleman argues that there are four actors in the "digital colonialism" ecosystem; first, "Western tech companies who create and provide the technology and infrastructure that harvest the data for ad targeting and ad distribution".[315] Secondly, "advertising and consulting firms who use the technology provided by (Western tech companies) to target various groups with highly personalized ads and messages aimed at increasing profits".[316] Thirdly, "local companies, parties, and organizations who pay (advertising and consulting firms) to help them impose their different agendas for the respective countries".[317] Fourthly,

[314] D Coleman 'Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws' (2019) *Michigan Journal of Race & Law* 422.
[315] Ibid 423.
[316] Ibid.
[317] Ibid.

"citizens who knowingly and unknowingly act as data sources for (Western tech companies) and as target groups for (advertising and consulting firms) and (local companies, parties, and organizations)".[318]

Coleman explains that "digital colonialism" is made possible by the fact that African countries have "limited infrastructure, limited data protection laws, and limited competition, combined with social, political, and economic power imbalances and decades of resource pillaging is what gives the above consequences true power".[319] In the Kenyan context, it could be argued that Kenya is a net importer of technology from "Western tech companies" described by Coleman.

Birhane discusses another form of colonialism dubbed "algorithmic colonialism".[320] Birhane argues that instead of use of unilateral and brute force and domination over a colonised people, "algorithmic colonialism" occurs "through invisible and nuanced mechanisms such as control of digital ecosystems and infrastructure".[321] Birhane posits that "'algorithmic colonialism is the desire to dominate, monitor, and influence social, political, and cultural discourse through the control of core communication and infrastructure mediums".[322]

Algorithmic colonialism is driven by technology monopolies who consider humans as data producing resources.[323] Humans who are sources from which data is extracted have no control or power over the extractive actions. Like in Warren and Brandeis's time, technology has a role to play on how an individual's right to privacy is respected, protected, and promoted and more so "how" the technology is being deployed. In making a determination-of-adequacy of data protection regulation, it is instructive to inquire into whether there are legal provisions that provide guidance on the "how?" question responses.

[318] Ibid.
[319] Ibid 424.
[320] A Birhane 'Algorithmic Colonization of Africa' (2020) *SCRIPTed* 391. See also N Couldry and U Mejias, (2018) 'Data colonialism: rethinking big data's relation to the contemporary subject' *Television and New Media* 336 – 349.
[321] Ibid.
[322] Ibid.
[323] Ibid.

In this section I have revealed the point of disadvantage which Kenya finds itself. First, emerging technologies are mostly not developed in Kenya. Secondly, Kenya does not have laws in place for these technologies akin to the EU Artificial Intelligence Act. This brings about the question as to the extent the right to privacy may be respected, protected, and promoted in Kenya *vis a vis* technologies and in effect State surveillance and surveillance capitalism.

Having dealt with the first responses to the "how?" question, in the next sections I deal with the second and third aspects of the "how?" question responses. In the next sections I discuss oversight and access to remedies under the KDPA.

3.9.4 Oversight

Oversight by the Office of the Data Protection Commissioner is tied to its independence. My argument is that adequate data protection regulation must provide for independence of the regulatory authority. Section 8(3) of the KDPA states that "the Data Commissioner shall act independently in exercise of powers and carrying functions". However, as I explained in chapter one of this study, independence is watered down by the KDPA providing the Cabinet Secretary in charge of information, communication, and technology with roles under the Act.

Section 70 of the KDPA stipulates that the Data Commissioner is to submit reports to the Cabinet Secretary who in turn submits the report to the National Assembly. In sharp contrast section 31(1)(d) of POPIA states that the Information Regulator "is accountable to the National Assembly". Evidently, as I argue in this study there are numerous provisions of the KDPA that water down the independence of the Office of the Data Protection Commissioner.

Sajo contends that independence of independent authorities is tied to their "distance from constitutionally recognized branches of power". [324] Independence of these authorities speaks to the integrity of the service which the independent authority renders.[325] According to Sajo,

[324] A Sajo, 'Independent Regulatory Authorities as Constitutional Actors: A Comparative Perspective' (2007) *Annales Universitatis Scientiarum Budapestinensis de Rolando Eotvos Nominatae* 14.
[325] Ibid.

"appointment, dismissal, qualification, fixed term, conflict of interest rules (*incompatibilite*) of commissioners and other independent authority leaders are considered fundamental guarantees of authority independence".[326]

Independence is not absolute as the independent authorities ought to be subject to oversight from institutions such as Parliament and the courts.[327] Parliament and the courts may only undertake oversight within their constitutional mandates and powers.[328] Oversight does not mean receiving order or instructions from organs of the State or even private entities.[329]

As I respond to the "how?" questions in subsequent chapters of this study, I make proposals for law reforms. The proposals are to ensure statutory independence of the Office of the Data Protection Commissioner as it executes its mandate.

3.9.5 Access to effective remedies

Adequate data protection regulation must provide for effective remedies. International instruments, constitutional provisions, and case law offer guidance on what constitutes an effective remedy. Article 8 of the Universal Declaration of Human Rights (UDHR) states that "everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law."[330] Similarly, Article 2(3) of the International Covenant on Civil and Political Rights (ICCPR) provides:

> (d) 'To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;
> (e) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy;

[326] Ibid.
[327] Ibid 13, 24.
[328] Ibid 24.
[329] Ibid.
[330] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).

(f) To ensure that the competent authorities shall enforce such remedies when granted.'[331]

In European Union, Article 47 of the Charter of Fundamental Rights of the European Union provides that "everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal".[332] An effective remedy as per the UDHR and ICCPR has four components, first, there ought to be a violation of a fundamental right recognised by law. Secondly, there ought to be a remedy for the violation. Thirdly, the determination of a remedy is to be undertaken by a competent authority. Fourthly, the remedy should be enforced by competent authorities once it is granted.

The right to privacy and data protection are recognised by law. Where a violation occurs, the next question is whether competent authorities are available to provide effective remedies. The courts are one avenue that may ensure the availability of effective remedies. Article 22(1) of the Kenyan Constitution provides that "every person has the right to institute court proceedings claiming that a right or fundamental freedom in the Bill of Rights has been denied, violated or infringed, or is threatened".

Where a remedy requires administrative action, Article 47 of the Kenyan Constitution provides:

(3) 'Every person has the right to administrative action that is expeditious, efficient, lawful, reasonable and procedurally fair.

(4) If a right or fundamental freedom of a person has been or is likely to be adversely affected by administrative action, the person has the right to be given written reasons for the action.'

Section 63 of the KDPA provides that "in relation to an infringement of a provision of the Act, the maximum amount of the penalty that may be imposed by the Data Commissioner in a penalty notice is up to five million shillings (around USD 46 000, or ZAR 671 000) or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, whichever is lower". Owing to the scope and scale of use of personal data, the statutory fines

[331] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171

[332] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

under the Act may end up not being punitive or deterrent enough for any legal or natural person going against data protection principles set out in the Act.

3.10 Conclusion

In this chapter I have set out an objective framework to determine the adequacy of data protection regulation whether a country is carrying out introspection of its laws or determining adequacy of data protection regulation of another State. The determination-of-adequacy framework provides responses to the "who?", "why?", "what?", "when?", "where?", and "how?" questions. Comprehensive responses to these questions reveal whether a country's data protection regulation is adequate. In this chapter, the general responses provide the bare minimum of personal data protection regulation.

The "who?" question responses identify individuals whose activities or information is subject to regulation by law in relation to personal data. First, on the "who?" question, an adequate legal framework would identify the natural or legal persons whose personal data is subject to regulation. Secondly, the law ought to identify the natural or legal persons whether in public or private sector who seek to process personal data or information of persons identified in the first response to the "who?" question.

While responding to the "who?" question it is instructive to note that a power asymmetry will exist between the natural or legal persons identified. Regulation of data protection that is adequate strikes a balance in the power symmetry.

The "why?" question responses identify whether the law provides justification for personal data protection and personal data processing; the explicit and specified purposes. In responding to the "why?" question, attention must be paid to the value of personal data protection. The law ought to provide for checks and balances against those who wish to make incursions into personal data protection. The responses to the "why?" question are made

while recognising that harms may be caused by incursions into data subject rights, hence, it is critical that the law provides remedies to data subjects for the harms they are subjected to.

On the "what?" question responses, the law ought to indicate the kind of personal data or personal information that is regulated. This may include what may be termed as normal personal data and special or sensitive data. There must be no ambiguity on the nature of data regulated or protected by law.

"When?" question responses identify the legitimate circumstances under which the law allows for processing of personal data. The legitimate reasons that ought to be provided for by law, include consent, contractual obligations, statutory obligations, and public purpose or interest. These legitimate reasons are to be read together with principles of personal data protection set out in law. In responding to the "when?" question, one must pay attention to the fact that the Constitution provides for the limitation of the right to privacy.

"Where?" question responses relate to jurisdictional issues in data protection. The law must answer the question of the territorial scope of the law. Where the law has extra-territorial application, the law ought to be clear and specific on the boundaries of the application.

The "how?" question responses indicate what kind of data processing operations are regulated by law. Does the law regulate the collection, storage, disclosure, transmission, dissemination, destruction, and analysis of personal data? Does the law identify and regulate technology as where personal data is processed? This is bearing in mind that technology has an impact on effecting personal data protection. Technology might bring about bias and may be affected by digital and algorithmic colonialism. It is critical that the law provides a clear framework to minimise the negative effects technology may have on personal data protection.

Secondly, responses to the "how?" question should outline how the law deals with oversight of data protection regulation. Is there an independent oversight authority and what the powers and functions of that authority? Thirdly, the "how?" question responses should identify how the law deals with access to effective remedies for data subjects.

I believe that responses to these questions will flag out the strengths and weaknesses of data protection regulation in any country. The responses will inform law reform as they do in this study as I interrogate State surveillance in chapter four, surveillance capitalism in chapter five, and access to effective remedies in chapter six.

CHAPTER FOUR: ADEQUACY IN STATE SURVEILLANCE

4.1 Introduction

This chapter focuses on the question: To what extent is the legal framework on State surveillance adequate?

In chapter one of this study, I outlined the challenges of having vague statutory exemptions that facilitate unbridled and unregulated State surveillance. I also pointed out instances where the State carried out extrajudicial surveillance to the detriment of those put under surveillance and society at large. In chapter three I highlighted what generally, at the very least must be contained in personal data protection regulation for it to be considered adequate.

It is over the backdrop of chapters one, two and three, that this chapter applies the determination-of-adequacy framework set out in chapter three with the "who?", "why?", "what?", "when?", "where?", and "how?" questions posed on State surveillance. For each question, I outline the Kenyan data protection provision which I compare with the GDPR and POPIA, and then offer my reflections. In responding to the questions, I indicate whether the responses point to adequate personal data protection regulation in Kenya, and I propose law reforms where the regulation falls short. This provides a refined approach to determination-of-adequacy that is specific to State surveillance as opposed to the general responses set out in chapter three of this study.

I adopt the dictionary meaning of surveillance which is "observation and collection of data to provide evidence for a purpose"; "the careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected";[1] and "close watch kept

[1] Cambridge English Dictionary. Available at <SURVEILLANCE | meaning in the Cambridge English Dictionary> last accessed 22 September 2022

over someone or something".[2] Black's Law Dictionary defines surveillance as "close observation or listening of a person or place in the hope of gathering evidence".[3] Close observation includes processing of personal data.

Macnish defines surveillance as "the monitoring of a competent adult or adults over a period of time without their consent. Surveillance can be carried out on other parties (e.g. children) and it may be carried out with consent".[4] Where the State is involved in surveillance, State surveillance is the close monitoring or watching of individuals by institutions or organs of the State over time.

Where the State is monitoring an individual, their home, property, and communication it directly conflicts with the individual's right to privacy. Due to the tension that exists between State surveillance and privacy, it is critical to interrogate the adequacy of personal data protection regulation in State surveillance. Marx posits that surveillance works towards neutralising privacy and that as individuals work towards protecting their privacy, there are those such as State agents working through the barriers to carryout surveillance.[5] Marx argues that new technologies to collect personal information are constantly being developed to advance surveillance capabilities.[6] These arguments point to the need for adequate personal data protection regulation to ensure State surveillance does not overstep constitutional and legislative boundaries.

Data protection laws on State surveillance as advanced by Gutwirth and De Hert, protect individuals, require good data management practices, and "ensure that personal data are processed in ways that make it unlikely that personal integrity and privacy will be infringed or invaded".[7] Gutwirth and De Hert emphasise that data protection laws should recognise the

[2] Merriam Webster Dictionary. Available at < Surveillance Definition & Meaning - Merriam-Webster> last accessed 22 September 2022.
[3] Black's Law Dictionary 9th Edition.
[4] K Macnish 'An Eye for an Eye: Proportionality and Surveillance' (2015) *Ethical Theory and Moral Practice* 530.
[5] G Marx 'A Tack in the Shoe: Neutralizing and Resisting the New Surveillance' (2003) *Journal of Social Issues* 369, 370.
[6] Ibid 370.
[7] P De Hert and S Gutwirth 'Privacy, data protection and law enforcement: Opacity of the individual and transparency of power' (2006) *Privacy and the criminal law* 61-104.

need for public actors to use personal data but within set parameters.[8] Gutwirth and De Hert note that "the rationale behind data protection in the public sector is the knowledge that authorities can easily infringe privacy and that in all administrative systems there is an urge to collect, store and use data, an urge which must be curtailed by legal regulation."[9] In the next sections, starting with responses to the "who?" question, I outline the law that governs State surveillance *vis a vis* personal data protection to interrogate its adequacy.

4.2 Who?

I first need to identify who or what exactly the "State" is. Section 2 of the KDPA points to a data controller and a data processor who includes a "public authority". The provision does not define what or who a "public authority" is. Nonetheless, Article 260 of the Kenyan Constitution defines "State", "when used as a noun, to mean the collectivity of offices, organs and other entities comprising the government of the Republic". Consequently, a public authority may be interpreted as a "State" authority.

Just like the KDPA, the GDPR is silent on what constitutes a "public authority". POPIA on the other hand is specific in its definition. Section 1 of POPIA defines a "public body":

> '(a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
>
> (b) any other functionary or institution when—
>
> (i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
>
> (ii) exercising a public power or performing a public function in terms of any legislation;'

Looking at POPIA's definition that identifies the different levels of government in South Africa and noting that the government of Kenya is comprised of the national and county governments, responses to the "who?" question in Kenya include State organs at both levels

[8] Ibid.
[9] Ibid.

of government. Borrowing from section 1 of POPIA which provides the better definition in comparison, I submit that any person, organ, or institution performing a public function in terms of any legislation is considered as being part of the "State".

With the above definition of the State, for this chapter I focus on the national security organs which are part of the State and engage in State surveillance. I focus on these organs due to the fact that the general exemptions set out under section 51(2)(b) of the KDPA refer to national security. In Kenya, there are three main actors defined as national security organs by Article 239 of the Constitution. These are the National Police Service, the National Intelligence Service, and the Kenya Defence Forces established under the National Police Service Act,[10] National Intelligence Service Act,[11] and the Kenya Defence Forces Act[12] respectively. For purposes of applying the determination-of-adequacy framework in this chapter, the first response to the "who?" question is the National Police Service, the National Intelligence Service, and the Kenya Defence Forces.

The second aspect of the response to the "who?" question is the individual who is subjected to State surveillance. This is the individual whose right to privacy is protected under Article 31 of the Constitution and the KDPA. Article 31 refers to "every person" having the right to privacy. Article 260 defines "person" to include a company, association, or other body of persons whether incorporated or unincorporated.

Section 2 of the KDPA however reads that "person" has the meaning assigned to it under Article 260 of the Constitution. The provision then states that a "data subject" is "an identifiable natural person who is subject of personal data". Section 2 also states that "personal data" means any information relating to an identified or identifiable natural person. This specifically excludes legal persons. The Act protects processing of personal data of data subjects who are natural persons.

[10] Cap 84 Laws of Kenya.
[11] Act No. 28 of 2012.
[12] Act No. 25 of 2012.

The GDPR has the same definition of a data subject as the KDPA which only includes natural persons. Directive (Eu) 2016/680 of the European Parliament and of The Council distinguishes between different categories of data subjects.[13] The Directive is specific to "the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties". Article 6 of the Directive sets out the categories of data subject who may be put under surveillance:

(a) 'persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
(b) persons convicted of a criminal offence;
(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and
(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).'

In my view, the nuanced approach to defining data subjects in the Directive 2016/680 provides clarity on who at first instance may be subject to State surveillance. In comparison, the Constitutional Court of South Africa decision in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors*[14] recognised the right to privacy of juristic persons. The court had a caveat to the extent that the level of protection for a juristic person was to be determined on a case-to-case basis.

Burns and Burger-Smidt in their commentary on POPIA report that juristic persons are protected in POPIA because information of officials of companies or business partnerships

[13] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
[14] *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* (CCT1/00) [2000] ZACC 12; 2000 (10) BCLR 1079; 2001 (1) SA 545 (CC) (25 August 2000).

falls within POPIA.[15] Also that in South Africa juristic persons need protection when their information is being processed by credit reference agencies, telecommunication companies, and direct marketers among other institutions.[16] Kenya has not extended personal data protection to juristic persons.

Kenyan law adequately identifies the data subject who is the focus of personal data protection regulation. Perhaps in future there might be consideration for juristic persons as the case is under POPIA. This said, from the above responses to the "who?" question, it is apparent that the law does not adequately define data controllers and data processors that are constitutionally and legislatively mandated to carryout State surveillance; the KDPA does not spell out what or who a "public authority" is. This brings me to my first recommendation that borrows from Directive (Eu) 2016/680 and POPIA:

Recommendation 1:

Amend section 2 of the KDPA as follows:

Insert a new definition –

"public authority" means

(a) an organ, department, or institution in the national or a county government; or

(b) any other organ, department, or institution when—

(i) exercising a power or performing a duty in terms of the Constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation

Amend the Data Protection (General) Regulations as follows:

Insert a new Regulation 54A –

Data subjects for purposes of personal data processing for national security shall include -

(a) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
(b) persons convicted of a criminal offence;

[15] Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (2018) 19.
[16] Ibid.

(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and

(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).

4.3 Why?

This section responds to the "why?" question; explicit and specified purposes for carrying out State surveillance must be articulated in written law. This section, first, discusses the general exemptions under the KDPA that touch on national security and public interest. Secondly, the section identifies and discusses the constitutional and statutory provisions that allow for State surveillance, and thirdly, highlights the harms that may be occasioned by State surveillance.

As I argued in chapter three of this study, adequate data protection regulation in the case of State action ought to ensure that State activities are carried out only where they are aimed at protecting the individual and society at large. Individuals must be afforded the space to direct their lives as they so wish, and adequate protections ensure that individual are free from unwarranted State interference; human autonomy must be maintained. The State must have compelling and legitimate reasons to interfere with the individual.

4.3.1 General exemptions under the KDPA

When responding to the "why?" question, bear in mind that State surveillance may fall under the general exemptions outlined under section 51 of the KDPA. Section 51(2)(b) states that "the processing of personal data is exempt from the provisions of this Act if… it is necessary for national security and public interest". The Act does not define "national security" or

"public interest". Notwithstanding, Article 238(1) of the Kenyan Constitution defines national security as "the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests". The KDPA to ensure clarity ought to have referred to Article 238(1) of the Constitution while providing more information on what may constitute national security or public interest under the Act.

On national security, Regulation 54 of the Data Protection (General) Regulations provides:

(1) 'For the purposes of section 51(2) (b) of the Act, the processing of personal data by a national security organ referred to in Article 239 (1) of the Constitution in furtherance of their mandate constitutes a processing for national security.
(2) Despite sub-regulation (1), a data controller or data processor who processes personal data for national security and wishes to be exempt on that ground shall apply to the Cabinet Secretary for an exemption.
(3) The Cabinet Secretary shall, upon being satisfied that the grounds supporting the application are sufficient, issue a certificate of exemption.
(4) The Cabinet Secretary may revoke a certificate of exemption issued, at any time, where the grounds on which the certificate was issued no longer apply.'[17]

Regulation 54 refers to national security organs which under Article 239(1) of the Constitution are, the Kenya Defence Forces, the National Intelligence Service, and the National Police Services as they process personal data in furtherance of their mandate which includes national security. The mandate referred to in Regulation 54 is not defined. Is it the mandate under the Constitution, under statute, regulations, policies, or administrative orders made outside the confines of the law? The Regulation is inadequate for not being specific on where the mandate is derived from.

Regulation 54 does not define what criteria the Cabinet Secretary will adopt in deciding on exemption on the ground of national security. One absurd interpretation of this Regulation is that it assumes that national security organs will be under direction of the Cabinet Secretary in charge of information, communication, and technology for purposes of processing personal data to fulfil their mandate. Secondly, the question arises as to whether and how a

[17] Legal Notice No. 263 of 2021.

data controller or data processor who is not a national security organ would be processing personal data for national security purposes. The Regulation is inadequate to the extent that it does not provide clarity on these issues.

On non-State organs being part of State surveillance, Snowden narrates how private companies such as Microsoft, Google, Oracle, HP, Dell, Google, Facebook, and Amazon became sources of data for the United States government to carry out mass surveillance.[18] Snowden reports that "PRISM enables the NSA to routinely collect data from Microsoft, Yahoo!' Google, Facebook, Paltalk, YouTube, Skype, AOL, and Apple, including email, photos, video and audio chats, web-browsing content, search engine queries, and all other data stored on their clouds".[19] Though such mass surveillance was carried out covertly, only being made public after Snowden's revelations, it indicates the role that entities that are not national security organs can play in facilitating State surveillance.[20] Would these companies be exempt under Regulation 54? The Regulation is not clear.

Issue at hand in the Kenyan situation, is whether the Cabinet Secretary will be providing national security exemptions to private sector entities that aid State surveillance and whether such exemptions would be made public. As I argued earlier, the KDPA and the Regulations do not spell out the modalities for making national security exemptions for entities that are not national security organs. To this extent, these provisions on national security exemptions are vague, broad, and ambiguous. In my second recommendation for law reform below, I propose to do away with exemptions for non-State actors on national security matters.

In the European Union, Article 2(2)(d) of the GDPR states that the GDPR "does not apply to the processing of personal data…by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security". Directive 2016/680 defines a "competent authority" in Article 3(7):

[18] E Snowden *Permanent Record* (Kindle Edn 2019) Ch. 16.
[19] Ibid Ch. 20.
[20] Ibid.

(a) 'any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or

(b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;' [21]

What is key to note from the Directive's definition is that it is limited to public authorities that prevent, investigate, detect, or prosecute criminal offences plus execute criminal penalties. The Directive specifies what the exemptions to the GDPR entail. Article 13(3) of the Directive states that "information to be made available or given to the data subject" may be limited by law. Article 15 provides for limitation to accessing personal data by a data subject. Article 16(4) provides for denial of the "right to rectification or erasure of personal data and restriction of processing". Such specificity is not evident in the Regulation 54 of the Data Protection (General) Regulations with my conclusion being that the regulations are inadequate.

Moving to public interest, Regulation 55 of the General Regulations provides:

'For the purposes of section 51(2) (b) of the Act, the processing of personal data is exempted from the Act on the grounds of public interest where such processing exists as a—

(a) permitted general situation; or

(b) permitted health situation.'

A permitted general situation under Regulation 56 includes:

(a) 'lessening or preventing a serious threat to the life, health or safety of any data subject, or to public health or safety;

(b) taking appropriate action in relation to suspected unlawful activity or serious misconduct;

(c) locating a person reported as missing;

(d) asserting a legal or equitable claim;

(e) conducting an alternative dispute resolution process; or

(f) performing diplomatic or consular duties.'

[21] Directive (note 13 above).

State surveillance could fall under Regulation 56(b), "taking appropriate action in relation to suspected unlawful activity or serious misconduct". In comparison, the GDPR under Article 2(d) outlines the following exemptions:

> 'This Regulation does not apply to the processing of personal data:
>
> > (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'[22]

Even exemptions ought to be specified in the law as Article 8 of Directive 2016/680 on lawfulness of processing personal data stipulates:

1. 'Member States shall provide for processing to be lawful only if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law.
2. Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing.'

The aim of Article 8 of the Directive is to demand that Member State law be specific on statutory reasons for processing of personal data by competent authorities. In my analysis Kenya has not been specific. In contrast, POPIA provides clarity on exemptions, in section 6(1)(c):

> 'This Act does not apply to the processing of personal information—
>
> (c) by or on behalf of a public body—
>
> (i) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or
> (ii) the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of

[22] EU the 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.

sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information;'[23]

De Stadler argues that it is not easy to define national security but states that national security interest applies when the State is obligated to "protect the public order and safety of its citizens and persons resident within the country".[24] De Stadler provides a caveat on the exemptions under POPIA by arguing that the exclusions should be applicable where adequate safeguards are put in place to protect personal information processed through cited activities.[25] In my analysis, the GDPR and POPIA provide clarity on what activities may be regarded as "national security". Directive 2016/680 indicates that exemptions are not to be blanket in nature. To ensure adequacy in Kenya, data protection regulation should provide clarity on the "mandate" of the national security organs when processing personal data and define the boundaries of exemptions. This brings me to my second recommendation:

Recommendation 2:

Amend section 2 of the KDPA as follows:

Insert a new definition –
"national security" means national security as defined under Article 238(1) of the Constitution and includes prevention, investigation, detection or prosecution of criminal offences, and the execution of criminal penalties.

Amend Regulation 54 of the Data Protection (General) Regulations as follows:

- Insert a new paragraph immediately after sub-Regulation 54(1) – "for purposes of this Regulation, mandate means the mandate set out under the Constitution and relevant statutory provisions".
- Delete sub-Regulations 54(2), 54(3), and 54(3) and insert a new sub-Regulation 54(2) – "exemptions shall be limited to a data subject's right:
  (a) to information;
  (b) of access;

[23] Act 4 of 2013.
[24] E De Stadler, E Hattingh , P Esselaar, and J Boast *Over-Thinking the Protection of Personal Information Act* (2021) 111, 112.
[25] Ibid 94.

(c) to rectification or erasure of personal data; and

(d) to restriction of processing.

Another provision that may be used as an excuse for State surveillance and a response to the "why?" question is section 30(1)(b)(v) of the KDPA which provides that "a data controller or data processor shall not process personal data, unless… the processing is necessary (for) the performance of any task carried out by a public authority". This provision sets out a vague, broad, and ambiguous principle on lawful processing of personal data; "any task" could mean anything.

On ambiguity, vagueness, and broadness in statutes, in *Geoffrey Andare v Attorney*[26] the challenge was on the constitutionality of section 29 of the Kenya Information and Communication Act.[27] The section provided for the offence of misuse of a licensed telecommunication device which the court found to be vague, broad, and uncertain such that one could not know the parameters within which the provision operated.[28] Due to the vague, broad, and uncertain nature of section 29 of the Kenya Information and Communication Act, the court declared the provision to be unconstitutional.

Judicial pronouncements on vague provisions were also made *in Cyprian Andama v Director of Public Prosecution.*[29] The petition challenged the constitutional validity of section 84D of the Kenya Information and Communication Act on the basis that it created an offence of criminalizing the publishing of obscene information in electronic form. It was argued that this provision was couched in vague and broad terms, and that in turn, the chilling effect produced by the offence limited the constitutionally guaranteed freedom of expression. The court declared the provision to be unconstitutional due to one, being broad and vague.

The two decisions emphasize the need to have clear statutory provisions where limitation of a fundamental right or freedom is concerned. The broad, vague, and ambiguous provisions

[26] *Geoffrey Andare v Attorney General & 2 others* [2016] eKLR.
[27] Cap 411A of the Laws of Kenya.
[28] *Geoffrey Andare v Attorney General* (note 26 above) 78.
[29] *Cyprian Andama v Director of Public Prosecution & another; Article 19 East Africa (Interested Party)* [2019] eKLR.

on national security and public interest in the KDPA ought not apply; the provisions are inadequate.

Aaronson argues that inadequate regulation of personal data in State surveillance has negative effects.[30] First, it is a violation of the right to privacy.[31] Secondly, exposure of personal data by national security agents may also expose critical national security data.[32] Thirdly, data sets could be used for nefarious reasons by those with access to the data.[33] Aaronson makes the point that how data is governed determines how a country regulates the personal data of its citizens, government data, and is key to policy and decision making.[34]

Lack of adequate regulation leads to the State arbitrarily expanding the meaning of concepts such as national security. Abdulrauf argues that the scope of national security and State surveillance is evolving and expanding.[35] This calls for rule of law that curbs the arbitrariness of State surveillance.[36] The challenge is that the rule of law also provides for exceptions which work towards negating the protection of fundamental rights and freedoms.[37] Exceptions if not well articulated, lead to lack of transparency in State actions, restrict the intervention of judicial or oversight bodies, and could lead to massive abuses by the State.[38]

Basimanyane summarises these arguments by stating that "surveillance cannot be conducted in an indiscriminate manner, it must be conducted legitimately, be lawful and used only where necessary".[39] Hence, it is instructive that the rule of law is clear on regulating State surveillance and providing for limited and specific exceptions that are not vague, broad, or ambiguous, thus, my third recommendation:

---

[30] S Aaronson "Inadequate data protection: A threat to economic and national security" (2020) available at < Inadequate data protection: A threat to economic and national security | CEPR> last accessed 4 October 2022.
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Ibid.
[35] L Abdulrauf 'The Challenges for the Rule of Law Posed by the Increasing Use of Electronic Surveillance in Sub-Saharan Africa' (2018) African Human Rights Law Journal 365-391.
[36] Ibid 376.
[37] Ibid 378.
[38] Ibid 380, 381, 383.
[39] D Basimanyane 'The Regulatory Dilemma on Mass Communications Surveillance and the Digital Right to Privacy in Africa: The Case of South Africa' (2022) African Journal of International and Comparative Law 376.

Recommendation 3:

Amend the KDPA by deleting section 30(1)(b)(v).

4.3.2 Statutory provisions

Another response to the "why?" question is derived from statutes that regulate the national security organs; perhaps, the statutes are the mandate Regulation 54 of the Data Protection (General) Regulations refers to. The National Police Service, the National Intelligence Service, and the Kenya Defence Forces have the mandate to ensure national security. For the Kenya Defence Forces, Article 241(3) of the Kenyan Constitution provides that the Forces:

> 'are responsible for the defence and protection of the sovereignty and territorial integrity of the Republic; … assist and cooperate with other authorities in situations of emergency or disaster, and report to the National Assembly whenever deployed in such circumstances; and may be deployed to restore peace in any part of Kenya affected by unrest or instability only with the approval of the National Assembly'.

The Kenya Defence Forces Act,[40] reiterates the functions outlined under Article 241(3) of the Constitution. For the National Intelligence Service, Article 242(2)(a) of the Constitution, states that the Service is "responsible for security intelligence and counterintelligence to enhance national security". Section 5(1) of the National Intelligence Service Act,[41] sets out the functions of the National Intelligence Service, which include to:

(a) 'gather, collect, analyse and transmit or share with the relevant State agencies, security intelligence and counter intelligence;
(b) detect and identify threats or potential threats to national security;
(c) advise the President and Government of any threat or potential threat to national security;
(d) safeguard and promote national security and national interests within and outside Kenya;
(e) gather, evaluate and transmit departmental intelligence at the request of any State department or organ, agency or public entity;

[40] Act No. 25 of 2012.
[41] Act No. 28 of 2012.

(f) regulate, in co-operation with any State department or agency, the flow of security intelligence between the Service and that State department or agency;

(g) undertake security vetting—

i. for persons seeking to hold a vettable position.

ii. for persons seeking to be registered as a citizen of Kenya;

iii. for foreign institutions seeking documents or seeking to undertake any activity in the Republic which may have a bearing on national security; or

iv. as may be required under any written law;

(h) carry out protective and preventive security functions within State departments, agencies, facilities and diplomatic missions;

(i) safeguard information systems and processes within State departments or agencies;

(j) support and aid law enforcement agencies in detecting and preventing serious crimes and other threats to national security;'

For the Police Service, section 24 of the National Police Service Act lists the functions of the Kenya Police Service:

i. 'provision of assistance to the public when in need;

ii. maintenance of law and order;

iii. preservation of peace;

iv. protection of life and property;

v. investigation of crimes;

vi. collection of criminal intelligence;

vii. prevention and detection of crime;

viii. apprehension of offenders;

ix. enforcement of all laws and regulations with which it is charged;'[42]

In addition to the above, the Prevention of Terrorism Act provides for the detection and prevention of terrorist activities.[43] Section 35 of the Prevention of Terrorism Act provides for limitation of certain rights with section 35(3) specific to the right to privacy:

'The limitation of a fundamental right and freedom under this section shall relate to—

(a) 'the right to privacy to the extent of allowing—

i. a person, home or property to be searched;

[42] No. 11A of 2011.

[43] Act No. 30 2012.

ii. possessions to be seized;
iii. the privacy of a person's communication to be investigated, intercepted or otherwise interfered with.'

Section 36A(1) of the Prevention of Terrorism Act states that "the National Security Organs may intercept communication for the purposes of detecting, deterring and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary". Section 36A(3) states that "the right to privacy under Article 31 of the Constitution shall be limited under this section for the purpose of intercepting communication directly relevant in the detecting, deterring and disrupting terrorism". These provisions grant powers to the State through national security organs to carry out surveillance. The question that arises is whether there are constitutional and statutory provisions that define how these State surveillance functions and powers may be exercised and what the boundaries of State surveillance are.

The constitutional provision that sets out the boundaries of State surveillance include Article 24 of the Constitution that provides for "limitation of rights and fundamental freedoms". The Constitution is adequate in spelling out the boundaries of State surveillance that encroaches on the constitutional right to privacy. Article 24 is discussed extensively in chapter three of this study.

While interrogating the extent of these functions and powers from constitutional and statutory provisions, consideration should be made for the "proportionality test" discussed in chapter three of this study. Application of the proportionality test will determine whether action by a national security organ is warranted *vis a vis* personal data protection. As Macnish notes, for a call to be made whether an act is proportionate or disproportionate, the difference between the harms and benefits ought to be significant.[44]

Mavedzenge discusses the "proportionality test" in communication surveillance.[45] Mavedzenge proposes a two-step inquiry to determine the proportionality of communication

[44] Macnish (note 4 above) 532.
[45] J Mavedzenge' The Right to Privacy v National Security in Africa: Towards a Legislative Framework which Guarantees Proportionality in Communications Surveillance' (2020) *African Journal of Legal Studies* 360-390.

surveillance.[46] Taking into consideration the circumstances of the surveillance being carried out, the first step of the inquiry is to determine whether there exists a pressing need to conduct surveillance to "protect a legitimate interest or purpose".[47] If there is a pressing need and a legitimate interest or purpose, then one would inquire into "the appropriate terms and conditions of the surveillance".[48]

Mavedzenge's exposition focuses on the activities that constitute surveillance. As I have indicated in chapter three of this study, the proportionality test is carried out to statutory provisions and personal data processing activities around State surveillance. Surveillance activities ought to be limited to express statutory provisions while the statutory provisions may only limit personal data protection to the extent within which limitations are allowed by the constitutional text. My conclusion on this is that constitutional and statutory provisions plus jurisprudence from the courts in Kenya are adequate in delineating the boundaries within which the State may carryout surveillance. As the next section notes, there are harms to carrying out State surveillance.

4.3.3 State surveillance harms

While responding to the "why?" question, potential State surveillance harms should be identified. Some harms emanate from individual State surveillance action and others from systematic mass State surveillance. On systematic mass State surveillance, Foucault discusses Bentham's concept of the panopticon which was described as a structure that would facilitate surveillance on a population whether in a prison, school, hospital, or factory setting.[49] Foucault recounts Bentham's panopticon as a mechanism that "arranges special unities that make it possible to see constantly and to recognize immediately".[50] Foucault goes on to

[46] Ibid
[47] Ibid 367
[48] Ibid.
[49] M Foucault *Discipline and Punish: The Birth of the Prison* (1975) 195 – 230.
[50] Ibid 200.

explain that "the major effect of the panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power".[51] The panopticon is a device of permanent surveillance upon a population or a group within a population; the individual subject to the surveillance may not be aware that they are being constantly watched.[52] Permanent surveillance may place an individual in a constant state of anxiety.[53]

Foucault argues that "the panopticon was also a laboratory; it could be used as a machine to carry put experiments, to alter behaviour, to train, or correct individuals".[54] As Marx asserts, people's behaviour changes depending on whether they are under surveillance.[55] Foucault chronicles the panopticon as a laboratory of power and restates Bentham's view that it helped reform morals, preserve health, invigorate industry, diffuse instruction, and tighten public burdens.[56] Surveillance power is linked to knowledge and on this, Foucault avers:

> "Knowledge linked to power, not only assumes the authority of 'the truth' but has the power to make itself true. All knowledge, once applied in the real world, has effects, and in that sense at least, 'becomes true.' Knowledge, once used to regulate the conduct of others, entails constraint, regulation, and the disciplining of practice. Thus, 'there is no power relation without the correlative constitution of a field of knowledge, nor any knowledge that does not presuppose and constitute at the same time, power relations".[57]

Foucault's exposition of surveillance using Bentham's panopticon metaphor aptly describes the effects mass surveillance may have on an individual and society. Challenges to surveillance include the opacity of the surveillance tools, the effect surveillance has on the behaviour of individuals, and the societal impact of surveillance.

Foucault's arguments may be compared to those of Orwell in his book 1984.[58] Orwell narrates a dystopian world where the State referred to as "Big Brother" carries out constant mass

[51] Ibid 201.
[52] Ibid.
[53] Ibid 202.
[54] Ibid 203.
[55] Marx (note 5 above) 374, 375.
[56] Foucault (note 49 above) 204, 207.
[57] Ibid 27.
[58] G Orwell *1984* (1949).

surveillance on its population using devices such as the telescreen which was a two-way surveillance device.[59] The State ("Big Brother") is able to use this mass surveillance tool to monitor and ensure absolute loyalty to the State. Death was a consequence for any perceived show of disloyalty. Mass surveillance as described by Orwell created a "zombified" society and individuals had no say over how the State exercised its powers.[60]

Surveillance carried out in the manner narrated by Foucault and Orwell runs afoul of liberty. As I discussed in chapter three of this study, principles of liberty espoused by Mill recognise that that all persons have political liberties and rights which the State should not infringe upon.[61] Any action by the State ought to be subject to checks and balances and undertaken with the consent of the people. The law and actions of the State should not control individuals with the effect of doing away with individual freedoms or impose the will of the State or the majority. These sentiments are echoed by Veliz who argues that liberalism is key for individuals to enable them to go about their lives as they please and that rules ought to be in place to ensure that individuals are free from interference from surveillance by the State. [62]

On being free from interference that comes with surveillance, Richards argues for the need to have "intellectual privacy".[63] Richards makes the point that "guarantee of privacy, protection from interference is necessary to promote … intellectual freedom".[64] Richard goes on to enumerate three harms that may be occasioned by surveillance, "blackmail, discrimination, and persuasion".[65]

On blackmail, Richard contends that "information collected surreptitiously can be used to blackmail or discredit opponents by revealing embarrassing secrets".[66] With regards to persuasion, Richard makes the claim that "surveillance also gives the watcher increased power to persuade" and that "persuasion is a more subtle exercise of the power differential

[59] Ibid.
[60] Ibid.
[61] J Mill *On Liberty* (Kindle Edn 1859).
[62] C Veliz *Privacy is Power* (Kindle Edn 2020) Ch 4.
[63] N Richards 'The Dangers of Surveillance' (2013) *Harvard Law Review* 1945, 1946.
[64] Ibid 1946.
[65] Ibid 1953.
[66] Ibid.

that be used to blackmail, but it can be even more effective."[67] On discrimination, Richard rightly contends that surveillance and the collection of personal data allows for categorisation of individuals.[68] The categories may be used to profile and discriminate on individuals.[69] To mitigate these harms, Richard proposes the prohibition of secret surveillance, prohibition of mass surveillance, and recognition of the harms caused by surveillance.[70] Prohibitions are best dealt with through concrete State surveillance regulatory frameworks.

On harms, CIPESA reports that State surveillance jeopardizes communication privacy and the right to anonymity, leading to self-censorship and the exclusion of some individuals and groups from the online public sphere.[71] CIPESA further reports that State Surveillance undermines freedom of expression, access to information, right to privacy of communications, and freedom of movement.[72] Harms related to privacy include those discussed by Citron and Solove such as physical, economic, reputational, emotional, relationship, chilling effect, discrimination, thwarted expectations, control, data quality, informed choice, vulnerability, disturbance, and autonomy harms.[73]

Considering that it is not practical to regulate every State surveillance action, Théodore Christakis and Katia Bouslimani argue on the importance of derogation principles and carrying out the "proportionality test".[74] When State surveillance is carried out in a proportional manner it minimises harm, maximises on benefits, and reduces the suspicion the population has on the aims of State surveillance activities.[75]

What the foregoing means is that the law ought to set out principles for the proportionality test. Chapter three of this study discusses the proportionality test indicating that the courts

[67] Ibid 1955.
[68] Ibid 1956.
[69] Ibid 1958.
[70] Ibid 1959 – 1964.
[71] CIPESA "State of Internet Freedom in Africa 2021: Effects of State Surveillance on Democratic Participation in Africa" 4 available at <SIFA 21 copy (cipesa.org)> last accessed 31st January 2022.
[72] Ibid.
[73] D Citron & D Solove 'Privacy Harms' (2011) *GW Law School Public Law and Legal Theory Paper No. 2021-1, GW Legal Studies Research Paper No. 2021-11* 19 – 40.
[74] T Christakis and K Bouslimani 'National Security, Surveillance and Human Rights' in R. Geiss, N. Melzer (Eds), *Oxford Handbook on the International Law of Global Security* (2021) 1,2.
[75] Ibid 3.

have in the past articulated how the proportionality test applies. The proportionality test identifies harms and determines whether the action by the State is warranted. The High Court of Kenya in *James Opiyo Wandayi v Kenya National Assembly*[76] citing *R (Daly) vs. Secretary of State for Home Department*[77] stated that:

1. 'Proportionality may require the reviewing Court to assess the balance which the decision maker has struck, not merely to see whether it is within the range of rational or reasonable decisions;
2. Proportionality test may go further than the traditional grounds of review in as much as it may require attention to be directed to the relative weight accorded to interests and considerations; and
3. Even the heightened scrutiny test is not necessarily appropriate to the protection of human rights.'[78]

In *Jacqueline Okuta v Attorney General* the High Court posited that the proportionality test "is appropriate as it preserves rights, provides a framework for balancing competing rights and enables other important public concerns, such as national security and public order, to be duly taken into account".[79] My conclusion on identification of harms is that the law may not specify the potential harms that may be caused by State surveillance. But the law must provide for the proportionality test that may identify harms. Kenyan jurisprudence has aptly articulated the proportionality test which points to adequacy in regulating actual and potential harms.

4.4 What?

In responding to the "what?" question, adequate personal data protection regulation must spell out what information or personal data is subject to State surveillance. There is no limit

[76] *James Opiyo Wandayi v Kenya National Assembly* & 2 others [2016] eKLR.
[77] *R (Daly) vs. Secretary of State for Home Department* (2001) 2 AC 532.
[78] *James Opiyo Wandayi v Kenya National Assembly* (note 76 above) 24.
[79] *Jacqueline Okuta & another v Attorney General & 2 others* [2017] eKLR. See also *Kenya National Commission on Human Rights & another v Attorney General & 3 others* [2017] eKLR and *Cyprian Andama v Director of Public Prosecutions & 2 others; Article 19 East Africa (Interested Party)* [2021] eKLR.

as to the specific information relating to an identified or identifiable person that is relevant to State surveillance. So long as data identifies an individual, it is personal data.

Section 2 of the KDPA just states that personal data is "any information relating to an identified or identifiable natural person" and the GDPR provides similar provision.[80] Article 3 of the Directive 2016/680 defines personal data to mean "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, physiological, genetic, mental, economic, cultural or social identity of that natural person".[81] The definition in the Directive is tied to the mandate of "competent authorities" whose definition I have highlighted above.

Section 1 of POPIA offers a broader and better definition (I have cited the full text of section 1 of POPIA in chapter three of this study). In my view, when interrogating the "what?" question responses, the key point to consider is whether the information or data, first, identifies an individual or secondly, could be used to identify an individual. Having a list of data points as under POPIA may be advisable but not sufficient as personal data points are constantly emerging as technology advances.[82]

In another response to the "what?" question, there is information that requires a higher degree of protection. Section 2 of the KDPA singles out "sensitive personal data" which is described as "data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject". Article 9 of the GDPR extends the definition of special

[80] see L Tosoni and L Bygrave 'Article 4. Definitions' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 100 – 115.
[81] Directive (note 13 above).
[82] See Burns and Burger-Smidt (note 15 above) 15 - 22 and De Stadler (note 24 above) 79 – 84.

categories (sensitive) of personal data to include "political opinions" and "trade union membership".[83] Section 26 of South Africa's POPIA regarding special personal information:

1. 'A responsible party may, subject to section 27, not process personal information concerning—
   (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
   (b) the criminal behaviour of a data subject to the extent that such information relates to—
      i. the alleged commission by a data subject of any offence; or
      ii. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.'

To process the special personal information section 27 of POPIA requires pre-authorisation from the Information Regulator.[84] The processing is done either with the consent of the data subject, for an obligation of the law, for historical, research and statistical reasons, and where the data subject makes the information public. Under Article 9 of the GDPR, sensitive personal data may be processed where there is consent, where the data controller and data processors are obligated to do so under the law, to protect the vital interests of the data subject, where the data is made public by the data subject, for judicial processes, and for public interest.

Section 44 of the KDPA requires that sensitive data be processed in accordance with data protection principles laid out under section 25 of the Act. Section 45 on permitted grounds for processing sensitive data mirrors Article 9 of the GDPR outlined above. In my view, the KDPA is adequate in providing scenarios where sensitive data may be processed. I think it is an overstretch for POPIA to require pre-authorisation for processing special information. That said, the KDPA ought to expand its definition of sensitive personal data to include "political opinions" and "trade union membership". In my view, there was no justification for omitting the two in the definition. In conclusion to the "what?" question responses, I submit my fourth recommendation:

[83] See L Georgieva and C Kuner 'Article 9. Processing of special categories of personal data' C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 365 – 384.
[84] On pre-authorisation, see De Stadler (note 24 above) 240 – 251.

Recommendation 4:

Amend section 2 of the KDPA as follows:

The definition of "sensitive personal data" is amended to insert the words "political opinions" and "trade union membership" immediately after the phrase "sexual orientation of the data subject".

4.5 When?

While responding the "when? question it is important to note that State surveillance processing of personal data may only occur when the State takes into account principles that allow for incursions into privacy and applies the "proportionality test". Guiding principles must be well articulated in the law and as Hartzog and Selinger posit, the aim is not to stop the State from carryout surveillance but to make it harder for the State to do so.[85] Hartzog and Selinger argue in favour of the concept of obscurity which states that when information is hard to obtain or understand, then it may be considered safe to a certain degree.[86] State surveillance according to Hartzog and Selinger is a loss of obscurity.[87]

State surveillance should be limited through obscurity strategies spelt out in the law. As Hartzog and Selinger put it "democratically accountable government should find it appropriately difficult to violate the privacy rights of its citizens".[88] The State ought to ensure that the incursions are in line with Article 24 of the Kenyan Constitution's guidelines on limitation of rights and data protection principles outlined under section 25 of the KDPA (I have cited the full text of section 25 in chapter three of this study).

Article 5 of the GDPR on the other hand sets out the principles relating to data processing (I have cited the full text of Article 5 in chapter three of this study). Article 4 of Directive

[85] W Hartzog and E Selinger 'Surveillance as Loss of Obscurity' (2015) *Washington and Lee Law Review* 1355.
[86] Ibid 1338.
[87] Ibid 1369.
[88] Ibid 1386.

2016/680 provides for "principles relating to processing of personal data" which mirror provisions of the GDPR. Chapter Three of POPIA sets the "when" in terms of "conditions for lawful processing of personal information". POPIA lays out these conditions as accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, and data subject participation.[89]

As I compare the KDPA, the GDPR, and POPIA, I note that the KDPA does not provide for the data protection principles of "accountability" and "security safeguards". When answering the "when?" question, data controllers and data processors must demonstrate that they are compliant with data protection principles and that they are processing personal data through lawful and legitimate means. KPDA not having "accountability" and "security safeguards" as data protection principles is a gap that needs to be remedied. This brings me to my fifth recommendation:

Recommendation 5:

Amend section 25 of the KDPA as follows:

Section 25 is amended by inserting the following new sub-section –

Section 25(i) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Section 25 is amended by inserting the following new paragraph immediately after section 25(i):

The controller shall be responsible for and be able to demonstrate compliance with this section.

[89] See De Stadler (note 24 above) 185 – 203; Burns and Burger-Smidt (note 15 above) 25 -36.

In addition to Article 24 of the Constitution and section 25 of the KDPA, the Constitution, and other statutory pronouncements guide national security organs on the "when?" question responses. One of the provisions is Article 238(2) of the Constitution:

> 'The national security of Kenya shall be promoted and guaranteed in accordance with the following principles—
>
> (a) national security is subject to the authority of this Constitution and Parliament;
>
> (b) national security shall be pursued in compliance with the law and with the utmost respect for the rule of law, democracy, human rights and fundamental freedoms;'

Additionally, section 3 Kenya Defence Forces Act sets out guiding principles:

> 'The Defence Forces shall, in fulfilling its mandate, observe and uphold the Bill of Rights, values and principles under Articles 10(2), 232(1) and 238(2) of the Constitution and shall—
>
> (a) strive for the highest standards of professionalism and discipline amongst its members;
> (b) prevent corruption and promote and practice transparency and accountability;
> (c) comply with constitutional standards of human rights and fundamental freedoms;
> (d) train staff to the highest possible standards of competence and integrity and to respect human rights and fundamental freedoms and dignity;'

Section 3 of the National Intelligence Service Act contains similar provisions. The National Police Service Act does not enumerate corresponding guiding principles. What is key to note in response to the "when?" question is that national security organs are to ensure compliance with the law, respect "the rule of law, democracy, human rights and fundamental freedoms". I find that the Constitution and relevant national security organ statutes are adequate to the extent that they spell out these principles.

4.6 Where?

In addition to the general responses in chapter three of this study on the "where?" question, in response to the "where?" question in this chapter, there is nuanced application of the

KDPA. Section 50 of the KDPA provides that the Cabinet Secretary may prescribe that certain processing of personal data must only be done through a server or data centre located in Kenya. Regulation 26 of the Data Protection (General) Regulations list where a data controller or data processor must "process such personal data through a server and data centre located in Kenya; or store at least one serving copy of the concerned personal data in a data centre located in Kenya". This is to be done when:

(a) 'administering of the civil registration and legal identity management systems;
(b) facilitating the conduct of elections for the representation of the people under the Constitution;
(c) overseeing any system for administering public finances by any state organ;
(d) running any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018;
(e) offering any form of early childhood education and basic education under the Basic Education Act, 2013; or
(f) provision of primary or secondary health care for a data subject in the country.'

Provisions similar to section 50 of the KDPA and Regulation 26 of the Data Protection (General) Regulations are not present in the GDPR or POPIA. Curious is why the list in Regulation 26 does not include prevention, investigation, detection or prosecution of criminal offences, and the execution of criminal penalties. This drives me to my sixth recommendation:

Recommendation 6:

Amend Regulation 26(2) of the Data Protection (General) Regulations as follows:

- Insert a new sub-Regulations -
  26(2)(g) – prevention, investigation, detection, or prosecution of criminal offences.
  26(2)(h) – execution of criminal penalties.

4.7 How?

In responding to the "how?" question, section 2 of the KDPA outlines that processing personal data includes collection, recording, storage, use, disclosure, dissemination, erasure, and destruction. For State surveillance, these operations may be undertaken in a physical or digital environment. Physical surveillance may entail creating or going through physical records that contain personal data, or physically trailing an individual. Digital Surveillance includes monitoring of internet traffic, social media, communications interception, and use of closed-circuit television networks.

Ünver lists bulk data interception as a means of digital surveillance and secondly, ICT monitoring which Ünver describes:

> 'Internet Communication Technology (ICT) surveillance focuses on human activity on both social media platforms such as Twitter, Facebook or Instagram, but also peer-to-peer communication tools such as Whatsapp, Telegram, Signal or simple SMS tools. ICT surveillance concerns both content (i.e. text of the message concerned), metadata (date, time, location of the message) and network (follow/friends, retweet, 'like' patterns) of a single individual or a group.' [90]

Thirdly, Ünver lists geo-location and remote sensing.[91] Fourthly, biometrics.[92] Fifthly, IOT which is described as "consumer-facing devices that are structured on automated communications between machines".[93] With these digital surveillance means, Ünver argues that governments while carrying out surveillance must win support from the public.[94] There ought to be accountability mechanisms and processes to check State surveillance; Ünver posits that "legislative and legal oversight has to be sufficiently strong".[95]

[90] H Ünver 'Politics of Digital Surveillance, National Security and Privacy' (2018) *Centre for Economics and Foreign Policy Studies* 5.
[91] Ibid 6.
[92] Ibid.
[93] Ibid.
[94] Ibid 16.
[95] Ibid 17.

Watt reiterates that recently, intelligence agencies "have developed sophisticated methods of accumulating vast amounts of data transmitted over the Internet, the analysis of which became possible by technological advancements in algorithmic and related computer analysis".[96] Watt argues that mass surveillance by the State is facilitated through "increased capacity to store information, coupled with the decreased costs of such retention, transformed methods of data acquisition, examination and sharing".[97] What Watt alludes to is that the State has increasing capacity and power to carry out surveillance.

Bearing in mind the increased capacity of the State to carry out surveillance, in determining the adequacy of personal data protection regulation, this section deals with three responses to the "how?" question, creating databases, communications surveillance, and options available to individuals who are subjected to State surveillance. Databases that the State uses to carryout surveillance include those mandated by law.

4.7.1. Creating databases

Databases are central to State surveillance. The State creates databases formally and informally.[98] Databases provide the State with a trove of data that is accessible and centralised. Watt identifies "the collection and storage of personal information, including in government databases" as one of the ways intrusions into privacy is carried out.[99] The KDPA, the GDPR, and POPIA do not have provisions that provide for the creation and management of databases.

CIPESA reports that States embark on creating databases that contain inordinate amounts of personal data which include "biometric data, which tend to be linked to National Identity cards, voters' cards and SIM card registration details".[100] States interlink databases containing

[96] E Watt *State Sponsored Cyber Surveillance* (2021) 2, 3.
[97] Ibid.
[98] Ibid 6.
[99] Ibid 211.
[100] CIPESA (note 71 above) 10.

personal information to ensure a high level of accuracy in identification of individuals, to facilitate communication surveillance, and to track individuals.[101] Communication surveillance creates refined data points as it may reveal an individual's "medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications".[102]

Some statutes provide for the creation of databases that contain personal data. Section 22(1)(g) of the Kenya Citizenship and Immigration Act,[103] spells out the following:

> 'Every citizen is entitled to the rights, privileges and benefits and is subject to the limitations provided for or permitted by the Constitution or any other written law including—
>
> the entitlement to any document of registration or identification issued by the State to citizens including—
>
> i) a birth certificate;
> ii) a certificate of registration;
> iii) a passport;
> iv) a national identification card; and
> v) a voter's card, where applicable.'

For each document, the State has created a database that is accessible to State agencies. Section 3 of the Births and Deaths Registration Act,[104] provides for a principal register of births and deaths. Section 5 of the Registration of Persons Act also provides for a register. A national population register is maintained by the Kenya Citizens and Foreign Nationals Management Service, which is established under the Kenya Citizens and Foreign Nationals Management Service Act.[105] Section 2 of the Act states that the national population register is for "capturing registration information on all Kenyans and Foreign Nationals resident in Kenya". Section

[101] Ibid.
[102] Necessary and Proportionate "International Principles on the Application of Human Rights to Communications Surveillance" (2014) < EN Princples (necessaryandproportionate.org)> 3.
[103] Act No. 12 of 2011.
[104] Cap 149 Laws of Kenya.
[105] Act No. 31 of 2011.

4(2)(a) of the Kenya Citizens and Foreign Nationals Management Service Act states that the Kenya Citizens and Foreign Nationals Management Service:

> 'in relation to the national population register and for the purpose of collecting and compiling information concerning the distribution and composition of the population in Kenya, the scope and direction of migration, labour resource utilization, and other connected purposes have the following functions—
>
> (i) receiving, storing and updating information from primary registration agencies;
>
> (ii) generating of appropriate unique identifier for individuals and groups in accordance with this Act;
>
> (iii) subject to the Constitution and in consultation with other relevant institutions, regulating the sharing of information by the various registration agencies and other users;'

On the voter's card, section 4 of the Elections Act,[106] mandates the Independent Electoral and Boundaries Commission to keep a register of voters:

> '(1) There shall be a register to be known as the Register of Voters which shall comprise of—
>
> (a) a poll register in respect of every polling station;
>
> (b) a ward register in respect of every ward;
>
> (c) a constituency register in respect of every constituency;
>
> (d) a county register in respect of every county; and
>
> (e) a register of voters residing outside Kenya.
>
> (2) The Commission shall compile and maintain the Register of Voters referred to in subsection (1).'

Section 6 of the Elections Act states that the register is to be open to the public for inspection. The register contains biometric data of voters. The Elections (Registration of Voters) Regulations, 2012 provide in Regulation 13 that biometric data shall be collected from a voter during registration plus name, location, sex, age, identity card/passport number, contact telephone, email, postal address, disability, and constituency details of a voter.[107]

Another database stems from the requirement for mandatory mobile network subscriber identification. Regulation 4 of the Kenya Information and Communications Act (Registration

[106] No. 4 of 2011.
[107] L.N. 126/2012, L.N. 73/2017.

of SIM cards) Regulations, 2015 requires all mobile network providers to register all SIM card subscribers. Regulation 5 lists the information required for SIM card registration to include:

> 'full names; identity card, service card, passport or alien card number; date of birth; gender; physical address; postal address, where available; any other registered subscriber number associated with the subscriber; an original and a copy of the national identity card, service card, passport or alien card; an original and a copy of the birth certificate, in respect of registration of minors; subscriber number in respect to existing subscribers; an original and true copy of the certificate of registration, where relevant; a letter duly sealed by the chief executive officer or the person responsible for the day to day management of the statutory body.'

The above information is also required under the Kenya Information and Communications (Registration of Subscribers of Telecommunications Services) Regulations, 2014. The records of subscriber information are submitted to the Communication Authority of Kenya. The onus is on a telecommunications provider to ensure confidentiality of the records. Regulation 16 of the Kenya Information and Communications Act (Registration of SIM cards) Regulations, 2015 states:

(1) 'A telecommunications operator shall take all reasonable steps to ensure the security and confidentiality of its subscribers' registration particulars.
(2) A telecommunications operator shall notify the Authority of the steps taken and processes introduced to ensure the security and confidentiality of its subscribers' registration particulars within thirty days of the commencement of these Regulations.'

Regulation 10 of the Kenya Information and Communications (Registration of Subscribers of Telecommunications Services) Regulations, 2014 provides:

(1) 'A licensee or an agent shall not disclose the registration particulars of a subscriber to any person without the written consent of that subscriber.
(2) Notwithstanding paragraph (1), a licensee or an agent may disclose the registration particulars of a subscriber—
    (a) for the purpose of facilitating the performance of any statutory functions of the Commission;
    (b) in connection with the investigation of any criminal offence;
    (c) for the purpose of any criminal proceedings; or
    (d) for the purpose of any civil proceedings under the Act.

(3) A licensee shall ensure that the registration particulars of a subscriber are kept in a secure and confidential manner.

(4) A licensee shall notify the Commission of the steps taken and processes introduced to ensure the security and confidentiality of its subscribers' registration particulars within thirty days of the commencement of these Regulations.

(5) A licensee or an agent who contravenes this regulation commits an offence.'

Databases controlled by private sector actors are also available to the State; an example of this is Passenger Name Record (PNR) databases used by airlines for air travel.[108] There is regulation for some of the databases highlighted above. The Data Protection (Civil Registration) Regulations, 2020,[109] apply to civil registrations entities "involved in the processing of personal data relating to (a) registration of births; (b) registration of adoptions; (c) registration of persons; (d) issuance of passport; (e) registration of marriages; (f) registration of deaths; or (g) issuance of any document of identity".[110] Regulation 4 states:

> 'The processing of personal data is lawful, if undertaken pursuant to the Act and in accordance to the provisions of the following laws—
>
> (a) the Registration of Persons Act;
>
> (b) the Births and Deaths Registration Act;
>
> (c) the Kenya Citizenship and Immigration Act;
>
> (d) the Marriage Act;
>
> (e) the Children Act;
>
> (f) the Refugee Act; or
>
> (g) any other law relating to the issuance of identity document.'

The Data Protection (Civil Registration) Regulations, 2020 provide for data protection principles, rights of a data subject, obligations of civil registration entities, security safeguards, and oversight by the Office of the Data Protection Commission. The Data Protection (Civil Registration) Regulations, 2020 are critical in managing civil registration databases that

[108] See G Robinson 'Data protection reform, passenger name record and telecommunications data retention: - Mass Surveillance Measures in the E. U. and the Need for a Comprehensive Legal Framework' (2012) *Critical Quarterly for Legislation and Law* 394-416; H Farrell and A Newman *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security* (2019).

[109] Legal Notice No. 196 Of 2020.

[110] Ibid Regulation 3.

process personal data. However, there is a gap in the statutory regulation of databases not tied to civil registration such as the electoral register and the SIM-Cards register.

For databases that are not tied to civil registration, the law is not specific on who may have or may not have access to the information in these registers. Secondly, the law does not spell out what security measures ought to be put in place to secure the information contained in the registers. Thirdly, the regulations do not indicate what should happen in case there is unauthorised access to the databases. Fourthly, there is no suggestion of independent oversight over how these databases are managed. All these shortcomings point to deficient regulation. This revelation informs my seventh recommendation:

Recommendation 7:

Enact the Data Protection (Statutory Database) Regulations under the KDPA. These proposed Regulations will have provisions similar to the Data Protection (Civil Registration) Regulations, 2020 and cover all databases not provided for in the Data Protection (Civil Registration) Regulations.

4.7.2 Communication surveillance

Communication surveillance is another response to the "how?" question. Communication surveillance involves close monitoring of private information within a communication system. The United Nations High Commissioner for Human Rights on communication surveillance has stated:

> '…any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications

information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association'.[111]

Section 42(3)(c)(iii) of the National Intelligence Service Act grants powers to the National Intelligence Service to monitor communication subject to authorisation by the Director General of the Service and a warrant from the High Court which may only be valid for 180 days unless extended. An application for a warrant from the High Court is made through an *ex parte* application. The National Intelligence Service Act does not make it an offence for an intelligence officer to intercept communications contrary to the provisions of the Act as is the Case in the Prevention of Terrorism Act.[112] In view of this, my eighth recommendation is:

Recommendation 8:
Amend the National Intelligence Service Act as follows: Section 42 is amended by inserting the following new sub-section – Section 42(4) an officer of the service who undertakes covert operations contrary to the provisions of this Act commits and offence and is liable upon conviction for a fine not exceeding... or to imprisonment for a term not exceeding...or to both.

Further on communication surveillance, section 36 of the Prevention of Terrorism Act provides for "power to intercept communication and the admissibility of intercepted communication". The provision grants a police officer above the rank of Chief Inspector of Police the power to intercept communication subject to written consent of the Inspector

[111] Office of the UN High Commissioner for Human Rights (OHCHR), 'The Right to Privacy in the Digital Age. Report of the United Nations High Commissioner for Human Rights' (30 June 2014) UN Doc A/HRC/27/37 47 ('A/HRC/27/37') 20.
[112] Act No. 30 of 2012.

General of Police or the Director of Public Prosecutions and a court order. Section 36(3) of the Act states that the court may make an order:

(a) 'requiring a communications service provider to intercept and retain specified communication of a specified description received or transmitted, or about to be received or transmitted by that communications service provider; or
(b) authorizing the police officer to enter any premises and to install on such premises, any device for the interception and retention of a specified communication and to remove and retain such device.'

Section 36(4) further states that the court may not make an order for interception of communication "unless it is satisfied that the information to be obtained relates to (a) the commission of an offence under this Act; or (b) the whereabouts of the person suspected by the police officer to have committed the offence". As per section 36(5), information contained in intercepted communication obtained subject to the Act and any other written law is admissible as evidence. Section 36(6) makes it an offence for a police officer to intercept communication contrary to the provisions of the Act. An application for an order for surveillance from the High Court is made through an *ex parte* application.

To emphasize the importance of the process to obtain surveillance warrants, Steeves and Piñero argue, any surveillance that is conducted without a valid warrant violates "basic civil liberties and threaten democratic governance".[113] Due to the threat of violations, independent oversight over State surveillance is critical to strike the balance between personal data protection and State surveillance powers.[114]

Section 36A(1) of the Prevention of Terrorism Act expands the powers for interception of communications to all national security organs. The section states that "the National Security Organs may intercept communication for the purposes of detecting, deterring and disrupting terrorism in accordance with procedures to be prescribed by the Cabinet Secretary". Section 36A(2) of the Prevention of Terrorism Act provides that the Cabinet Secretary responsible for matters relating to internal security is to make Regulations which would take effect after

[113] V Steeves and V Piñero 'Privacy and Police Powers: Situating the Reasonable Expectation of Privacy Test' (2008) *Canadian Journal of Criminology and Criminal Justice* 26.
[114] Ibid 264.

approval by the National Assembly to enable National Security Organs intercept communications. The Regulations are not in place which means that the law is inadequate, and that National Security Organs should not intercept communications until the Regulations are enacted.

Section 36A(3) of the Prevention of Terrorism Act indicates that "the right to privacy under Article 31 of the Constitution shall be limited under this section for the purpose of intercepting communication directly relevant in the detecting, deterring and disrupting terrorism". For the right to be limited and to ensure adequate regulation of personal data protection, these provisions under the Act must be supported by the Regulations required under section 36A(2).

Further on communication surveillance, the Kenya Information and Communications Act,[115] makes it an offence for a licensed telecommunications operator to intercept and disclose information. Section 31 of the Act provides:

> 'A licensed telecommunication operator who otherwise than in the course of his business—
>
> (a) intercepts a message sent through a licensed telecommunication system; or
> (b) discloses to any person the contents of a message intercepted under paragraph (a); or
> (c) discloses to any person the contents of any statement or account specifying the telecommunication services provided by means of that statement or account,
>
> commits an offence and shall be liable on conviction to a fine not exceeding three hundred thousand shillings or, to imprisonment for a term not exceeding three years, or to both.'

Noting that National Security Organs require collaboration with telecommunication operators, section 31 above provides another layer of protection against arbitrary and unwarranted interception of communications. The ideal situation would be where the State strictly adheres to the constitutional and legislative provisions when carrying out communications surveillance.

[115] Act No. 2 of 1998.

Privacy International, a non-governmental organisation in March 2017 published a Report dubbed 'Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya.'[116] The report outlines how communications surveillance was being carried out by Kenyan State actors without oversight and outside of the procedures required by Kenyan law. According to the Report, communication surveillance was carried out through direct access to telecommunication networks, access at the telecommunications provider, flagging targets, social media monitoring, and device access management.[117] The report indicates that intercepted communications content and data were used to facilitate gross human rights abuses, to spy on, profile, locate, track and ultimately arrest, torture, kill or disappear suspects.[118]

To curb unprocedural interception of communications and to ensure intercepted information is not used for human rights abuses, the Privacy International Report proposes reform of the communication surveillance legislation.[119] Secondly, the Report emphasises the need for telecommunication operators to publish reports indicating number of instances where they receive and act on interception requests from national security organs.[120] Thirdly, the report indicated the need to audit national security organs operations relating to interception of communications.[121]

On the EU front, the Court of Justice of the European Union in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs*,[122] on indiscriminate bulk surveillance stated:

> 'Article 15(1) of Directive 2002/58, as amended by Directive 2009/136, read in the light of Article 4(2) TEU and Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation enabling a State authority to require providers of electronic communications services to carry out the general and indiscriminate transmission of traffic

[116] Privacy International "Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya." available at <https://www.privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf> last accessed 14 February 2022.
[117] Ibid 19 -21.
[118] Ibid.
[119] Ibid 36, 37.
[120] Ibid.
[121] Ibid.
[122] Case C-623/17,

data and location data to the security and intelligence agencies for the purpose of safeguarding national security.'

In *H. K. v Prokuratuur*, the Court stated that EU law must be read:

> 'as precluding national legislation that permits public authorities to have access to a set of traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security, and that is so regardless of the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period.'[123]

Comparably, the Grand Chamber of the European Court of Human Rights in *Big Brother Watch v. The United Kingdom,*[124] declared bulk interception of communications by the United Kingdom to be a violation Article 8 on the right to privacy as protected by the European Convention for the Protection of Human Rights and Fundamental Freedoms.[125] The decision had been occasioned by disclosures by Edward Snowden, a former United States National Security Agency contractor.

Snowden narrates how the United States government undertook covert mass surveillance; Snowden's first-hand account illustrates the intrusive nature of mass surveillance. [126] Snowden argues:

> 'The freedom of a country can only be measured by its respect for the rights of its citizens, and it's my conviction that these rights are in fact limitations of state power that determine exactly where and when a government may not infringe into that domain of personal or individual freedoms that during the American Revolution was called "liberty" and during the Internet Revolution is called "Privacy".[127]

[123] Case C-746/18.
[124] (Applications nos. 58170/13, 62322/14 and 24960/15).
[125] 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.
[126] Snowden (note 15 above) preface.
[127] Ibid Ch. 11.

Snowden recounts how after 11 September 2001, the US government enacted legislation that gave security and intelligence agencies unfettered powers for warrantless collection of internet and telephone communications both domestic and international. The National Security Agency moved from targeted surveillance to bulk surveillance.[128]

Snowden contends that privacy of personal data depends on ownership of data and that laws are meant to make the work of law enforcement harder[129]. Law enforcement agencies ought to constantly be under court supervision. There should be limitations to law enforcement encroaching on privacy without warrants.[130] It is for the State to justify violations to the right to privacy through clear and unambiguous written laws.[131]

Constitutional and legislative safeguards are critical in communication surveillance. In South Africa, the Regulation of Interception of Communications and Provision of Communication-related information Act (RICA) regulated communication surveillance.[132] The constitutionality of the Act was challenged in *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services,* a case concerning bulk surveillance.[133] The South African Constitutional Court affirmed a declaration by the High Court of South Africa that had held RICA to be unconstitutional.

The South African courts held that RICA failed to provide adequate safeguards to protect the right to privacy by not providing for notification to persons under surveillance, not having adequate provision for personal information management, and not providing safeguards where the individual under surveillance is a practicing lawyer or journalist.[134] This decision goes on to show that courts when evaluating legislation regulating communication surveillance by the State should ensure the respect, protection, and promotion of fundamental rights and freedoms.

[128] Ibid Ch. 16.
[129] Ibid.
[130] Ibid Ch. 17.
[131] Ibid Ch. 18.
[132] No. 70 of 2002.
[133] (CCT 278/19; CCT 279/19) [2021] ZACC 3 (4 February 2021).
[134] Ibid.

Duncan in providing a critique of RICA mentions certain weaknesses.[135] First, subjects of communication surveillance are unaware that they are under surveillance.[136] Secondly, the grounds that allow for communication surveillance are too broad and vague.[137] Thirdly, no information is publicly available on the number of communication interceptions carried out and their degree of success in either securing convictions, stopping criminal activities, or averting the commission of crimes.[138] Fourthly, there is lack of independent monitoring of State surveillance activities.[139] Fifthly, the data collected for mass surveillance purposes is excessive and there is probability of abuse by those with access to the data.[140]

In my view, the court made the right call. Communication surveillance must be supported by express and comprehensive legislation that leaves no room for vagueness, ambiguity, or potential for abuse. Basimanyane in interrogating mass communication surveillance in South Africa posits that first, there needs to be proof of effectiveness of surveillance.[141] Secondly, there must be proof and legal justification that the surveillance is necessary.[142] Thirdly, "the law in a democratic state should stipulate in clear terms upon which crimes electronic surveillance may be employed and to what extent".[143] Fourthly, there must be an inquiry into whether laws that allow for State surveillance are "reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom".[144]

The arguments under this section point to deficiencies in regulating State surveillance. Law reform is required as I propose in recommendation nine to provide clarity in the law allowing for communication surveillance in Kenya:

[135] J Duncan *Stopping the Spies: Constructing and resisting the surveillance state in South Africa* (2018) 92.
[136] Ibid.
[137] Ibid 93.
[138] Ibid 93, 94.
[139] Ibid 95.
[140] Ibid 95, 96.
[141] Basimanyane (note 39 above) 376.
[142] Ibid.
[143] Ibid 377.
[144] Ibid 378.

Recommendation 9:

The Cabinet Secretary in charge of internal security shall enact Regulations on interception of communications under the Prevention of Terrorism Act and other enabling statutes. The Regulations under recommendation nine would feature among other issues justification for communication surveillance, limits to the surveillance, independent oversight mechanisms, remedies to data subjects, and penalties for non-compliance.

4.7.3 Options for data subjects

Another response to the "how?" question is the options available to data subjects when the State is carrying out surveillance. Article 22(1) of the Kenyan Constitution grants individuals "the right to institute court proceedings claiming that a right or fundamental freedom in the Bill of Rights has been denied, violated or infringed, or is threatened". Where proceedings are instituted under Article 22, Article 23(3) provides that "a court may grant appropriate relief, including: (a) a declaration of rights; (b) an injunction; (c) a conservatory order; (d) a declaration of invalidity of any law that denies, violates, infringes, or threatens a right or fundamental freedom in the Bill of Rights and is not justified under Article 24; (e) an order for compensation; and (f) an order of judicial review". In summary, a petition to the courts is one option available to data subjects.

Section 66 of the National Intelligence Act establishes the Intelligence Service Complaints Board whose functions include to "receive and inquire into complaints against the Service made by any person aggrieved by anything done by the Director-General or any member of the Service in the exercise of the powers or the performance of the functions of the Service". Ideally, any person who is aggrieved by the Intelligence Service carrying out surveillance should have recourse to the Complaints Board. But this is not as easy as stated in the Act, the challenges are first, whether an individual would know they are under surveillance. Secondly,

whether the Complaints Board is operational and thirdly, what the recourse would be in the absence of the Board.

In *Katiba Institute v Attorney General*, the Petitioners challenged the State for not operationalising the Intelligence Service Complaints Board.[145] The court ruled that the State's "failure, neglect or refusal to establish and operationalize the Intelligence Service Complaints Board under section 66 of the National Intelligence Service Act is a violation of Article 10 (2), Article 47, Article 48 and Article 50(1) of the Constitution of Kenya, 2010".[146] For adequacy to be achieved, the Complaints Board must be established and operationalised.

The Independent Policing Oversight Authority Act establishes the Independent Policing Oversight Authority.[147] Section 5 of the Independent Policing Oversight Authority Act sets out the objectives of the Authority as to "hold the Police accountable to the public in the performance of their functions; and give effect to the provision of Article 244 of the Constitution that the Police shall strive for professionalism and discipline and shall promote and practice transparency and accountability". What this provision signifies is that an individual has the option of making a complaint to the Independent Policing Oversight Authority where harms are cause by surveillance carried out by police officers. No data is publicly available on whether individuals have made complaints to the Authority arising out of violations of privacy by the Policer Service.

An individual who has been subject to State surveillance may also make a complaint to the Office of the Data Protection Commissioner. Section 56 of the KDPA indicates that a data subject who is "aggrieved by a decision of any person under (the) Act may lodge a complaint with the Data Commissioner". Section 8(2) of the KDPA requires that the Data Commissioner to "collaborate with the national security organs". The nature of the collaboration is not stipulated in the Act. Perhaps, dealing with State surveillance complaints could be one of elements of such collaboration.

[145] *Katiba Institute v Attorney General & 3 others; Kenya National Commission on Human Rights (Interested Party)* [2019] eKLR.
[146] Ibid.
[147] Act. No. 35 of 2011.

While I discuss the role of the Office of the Data Protection Commissioner in chapter six of this study, it is evident that individuals have numerous avenues available when seeking remedies for harms caused through State surveillance. It will be interesting to observe how the complaints process under the KDPA is handled by the Data Commissioner and the courts moving forward.

4.8 Conclusion

The need for adequate personal data protection is to ensure that State surveillance does not overstep constitutional and legislative boundaries. From my analysis in this chapter, several conclusions may be drawn regarding the adequacy of personal data protection *vis a vis* State surveillance.

First, the Data Protection (General) Regulations do not articulate the mandate of national security organs.

Secondly, the General Regulations do not define what criteria the Cabinet Secretary will adopt in deciding on exemption on the ground of national security. The question arises as to how a data controller or data processor who is not a national security organ would be processing personal data for national security purposes; this points to inadequacy.

Thirdly, it is not clear whether the Cabinet Secretary will be providing national security exemptions to private sector entities that aid State surveillance and whether such exemptions would be made public, another indication of inadequacy.

Fourthly, in an indication of adequacy, constitutional and legislative provisions identify the main actors defined as national security organs by Article 239 of the Kenyan Constitution. The law adequately identifies the data controllers and data processors that are constitutionally and legislatively mandated to carryout State surveillance. The law also identifies the data subject who is the focus of personal data protection regulation.

Fifthly, when interrogating harms occasioned by State surveillance, Kenyan law adequately provides for the framework to determine the proportionality of actions undertaken by national security organs. Sixthly, the law while identifying the personal data subject to protection under the law, it is inadequate to the extent that it does not pay attention to emerging technologies that constantly redefine data sources and data points.

Seventhly, in an indication of adequacy, the law sets out data protection principles to be applied when carrying out State surveillance. Legislation such as the Kenya Defence Forces Act and the National Intelligence Service Act outline guiding principles. The same cannot be said of the National Police Service Act.

Eighthly, the law is adequate in that it provides for sources of data such as databases mandate by law. Such databases include, the population register, births and deaths register, voters register, and databases of mobile phone subscribers. The shortfalls in the statutory regulation of the registers highlighted above is that the law is not specific on who may have or may not have access to the information in these registers. The law does not spell out what security measures ought to be put in place to secure information contained in the registers. The regulations do not indicate what may happen in case there is unauthorised access to the databases and there is no suggestion of independent oversight over how these databases are managed.

Ninthly, communication surveillance regulation is inadequate to the extent that there are no clear guidelines on independent oversight, there are no indications about the ramifications for abusing communication surveillance, and under the Prevention of Terrorism Act, the State carries out surveillance without the requisite Regulations being in place.

Tenthly, the law is adequate to the extent that it provides avenues for data subjects to seek remedies. These avenues include the courts, the Independent Policing Oversight Authority, and the Office of the Data Protection Commissioner. However, the National Intelligence Service Act is inadequate as the Intelligence Service Complaints Board that provides an avenue for redress under the Act is not in place.

With the above findings, I propose law reforms that are collated in the table below.

Recommendation 1:

Amend section 2 of the KDPA as follows:

Insert a new definition –

"public authority" means

(a) an organ, department, or institution in the national or a county government; or

(b) any other organ, department, or institution when—

(i) exercising a power or performing a duty in terms of the Constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation

Amend the Data Protection (General) Regulations as follows:

Insert a new Regulation 54A –

Data subjects for purposes of personal data processing for national security shall include -

(a) 'persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
(b) persons convicted of a criminal offence;
(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and
(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).'

Recommendation 2:

Amend section 2 of the KDPA as follows:

Insert a new definition –

"national security" means national security as defined under Article 238(1) of the Constitution and includes prevention, investigation, detection or prosecution of criminal offences, and the execution of criminal penalties.

Amend Regulation 54 of the Data Protection (General) Regulations as follows:

- Insert a new paragraph immediately after sub-Regulation 54(1) – "for purposes of this Regulation, mandate means the mandate set out under the Constitution and relevant statutory provisions".
- Delete sub-Regulations 54(2), 54(3), and 54(3) and insert a new sub-Regulation 54(2) – "exemptions shall be limited to a data subject's right:
  (a) to information;
  (b) of access;
  (c) to rectification or erasure of personal data; and
  (d) to restriction of processing.

Recommendation 3:

Amend the KDPA by deleting section 30(1)(b)(v).

Recommendation 4:

Amend section 2 of the KDPA as follows:

The definition of "sensitive personal data" is amended to insert the words "political opinions" and "trade union membership" immediately after the phrase "sexual orientation of the data subject".

Recommendation 5:

Amend section 25 of the KDPA as follows:

Section 25 is amended by inserting the following new sub-section –

Section 25(i) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Section 25 is amended by inserting the following new paragraph immediately after section 25(i):

The controller shall be responsible for and be able to demonstrate compliance with this section.

Recommendation 6:

Amend Regulation 26(2) of the Data Protection (General) Regulations as follows:

- Insert a new sub-Regulations -
  26(2)(g) – prevention, investigation, detection, or prosecution of criminal offences.
  26(2)(h) – execution of criminal penalties.

Recommendation 7:

Enact the Data Protection (Statutory Database) Regulations under the KDPA. These proposed Regulations will have provisions similar to the Data Protection (Civil Registration) Regulations, 2020 and cover all databases not provided for in the Data Protection (Civil Registration) Regulations.

Recommendation 8:

Amend the National Intelligence Service Act as follows:

Section 42 is amended by inserting the following new sub-section –

Section 42(4) an officer of the service who undertakes covert operations contrary to the provisions of this Act commits and offence and is liable upon conviction for a fine not exceeding... or to imprisonment for a term not exceeding...or to both.

Recommendation 9:

The Cabinet Secretary in charge of internal security shall enact Regulations on interception of communications under the Prevention of Terrorism Act and other enabling statutes. The Regulations under recommendation nine would feature among other issues justification for communication surveillance, limits to the surveillance, independent oversight mechanisms, remedies to data subjects, and penalties for non-compliance.

CHAPTER FIVE: ADEQUACY IN SURVEILLANCE CAPITALISM

5.1 Introduction

This chapter interrogates the adequacy of personal data protection regulation in surveillance capitalism. In chapter one of this study, I pointed out that unfettered use of personal data for commercial purposes is a challenge in Kenya with entities such as data brokers, multinational digital platforms, and digital lenders processing personal data with little or no regard for constitutional and statutory provisions on privacy and data protection. In chapter three I highlighted what generally, at the very least must be contained in personal data protection regulation for it to be considered adequate.

Considering the foundation set by chapters one and three, this chapter applies the determination-of-adequacy framework set out in chapter three with the "who?", "why?", "what?", "when?", "where?", and "how?" questions posed on surveillance capitalism. For each question, just as in chapter four, I outline the Kenyan data protection provisions which I compare with the GDPR and POPIA, and then offer my reflections. In responding to the questions, I indicate whether the responses point to adequate personal data protection regulation in Kenya, and I propose law reforms where the regulation falls short. This presents a refined approach to determination-of-adequacy that is specific to surveillance capitalism as opposed to the general responses set out in chapter three of this study.

The Black's Law Dictionary defines surveillance as "close observation or listening of a person or place in the hope of gathering evidence" and capitalism as "an economic system that depends on the private ownership of the means of production and on competitive forces to determine what is produced".[1] Surveillance capitalism is thus close observation carried out by private entities for commercial or economic gain.

[1] Black's Law Dictionary 9th Edition.

Zuboff generally argues that surveillance capitalism involves principles and concepts around technology that cannot be isolated from society and economics.[2] Zuboff explains that surveillance capitalism is about mass extraction of personal data that is used by corporations for commercial purposes.[3] The extracted data is analysed to make predictions about human behaviour.[4] Corporations use the information to target individuals with information that would likely guarantee changes in the behaviour of the individuals. The more is known about an individual, the easier it is to control and nudge them towards purchasing or accessing certain goods or services.[5] Zuboff contends that surveillance capitalism is done without taking into consideration privacy and data protection principles that benefit a data subject.[6]

Corporations use personal data that captures behavioural data to shape an individual's thinking and actions.[7] With copious amounts of data, corporations are able to nudge individuals towards certain directions with better precision and can predict an individual's thinking and actions.[8] Nudging results into commercial gain; individuals are persuaded to purchase goods, services, or products from the corporations that engage in the nudging.

Much of surveillance capitalism is executed without paying attention to privacy of individuals and without abiding by basic data protection principles. It is for these reasons that personal data protection regulation must provide for a definitive framework to tame the excesses of surveillance capitalism. In the next sections, starting with responses to the "who?" question, I outline the law that governs surveillance capitalism *vis a vis* personal data protection to interrogate its adequacy.

[2] S Zuboff *In the Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Kindle Edn 2019)
[3] Ibid.
[4] Ibid.
[5] Ibid Ch. 6.5.
[6] Ibid Ch. 1.5.
[7] Ibid.
[8] Ibid.

5.2 Who?

The first response to the "who?" question is found under section 2 of the KDPA which defines a data controller as "a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data". The provision defines a data processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller". The key words in relation to surveillance capitalism are "natural or legal person" and "agency or other body". That is any natural or legal person processing personal data and who is not a public authority. In chapter four of this study, I discuss the definition of a public authority.

Section 37 of the KDPA makes provision for commercial use of personal data and gets clarity from Regulation 14(1) of the Data Protection (General) Regulations, 2021 which states that in relation to commercial use of data:

> 'a data controller or data processor shall be considered to use personal data for commercial purposes where personal data of a data subject is used to advance commercial or economic interests, including inducing another person to buy, rent, lease, join, subscribe to, provide or exchange products, property, information or services, or enabling or effecting, directly or indirectly, a commercial transaction.' [9]

Reading Regulation 14(1) together with section 2 of the KDPA indicates that the first response to the "who?" question is a natural or legal person who determines that the purpose of processing personal data will be commercial or economic in nature. The GDPR does not outline provisions similar to Regulation 14 above. POPIA on the other hand defines activities that may amount to commercial use of personal data. POPIA in section 1 defines "direct marketing":

> '…to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –
>
> (a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

[9] Legal Notice No. 263 of 2021.

(b) requesting the data subject to make a donation of any kind for any reason.'

Under POPIA, the response to the "who?" question is a data controller or data processer who is engaged in direct marketing.[10] In my responses to the "why?" question below I argue that while the KDPA refers to commercial use of personal data, just like POPIA, the KDPA narrows it down to just direct marketing which in my view is inadequate.

The second response to the "who?" question is the data subject, that is the individual whose right to privacy is protected under Article 31 of the Constitution and the KDPA. This individual according to section 2 of the KDPA is the person who provides personal data. Hence, the second "who?" response is the identified or identifiable natural person whose data is processed for surveillance capitalism purposes. In chapter four of this study, I have provided a detailed analysis of the "who?" question response being a natural person. The KDPA is adequate in this regard.

5.3 Why?

This section responds to the "why?" question; explicit and specified purposes for carrying out surveillance capitalism must be articulated in law. In this section, I identify and discuss statutory provisions that regulate surveillance capitalism, and secondly, I highlight the potential harms to surveillance capitalism.

5.3.1 Commercial purpose

A response to the "why?" question is found under Regulation 14(1) of the Data Protection (General) Regulations, 2021 which states that commercial purpose is use of personal data to:

[10] See E De Stadler, E Hattingh , P Esselaar, and J Boast *Over-Thinking the Protection of Personal Information Act* (2021) 471 – 516.

'…advance commercial or economic interests, including inducing another person to buy, rent, lease, join, subscribe to, provide or exchange products, property, information or services, or enabling or effecting, directly or indirectly, a commercial transaction.'

Regulation 14(2) goes further to enumerate how the commercial interests may be advanced:

'A data controller or data processor is considered to use personal data to advance commercial interests where personal data is used for direct marketing through—

(a) sending a catalogue through any medium addressed to a data subject;
(b) displaying an advertisement on an online media site where a data subject is logged on using their personal data; or
(c) sending an electronic message to a data subject about a sale, or other advertising material relating to a sale, using personal data provided by a data subject.'

This Regulation is inadequate as it assumes that commercial interests are only advanced through direct marketing. It does not consider factors such as data brokers who I define and discuss in this chapter. Secondly, it does not regulate the use of personal data to train algorithms which I discuss in chapter three of this study. In comparison, the GDPR and POPIA also have a narrow approach towards commercial use of personal data by only regulating direct marketing.

The first response to the "why?" question which is found under Regulation 14(1) of the Kenyan Data Protection (General) Regulations, 2021 discussed above is inadequate for being too narrow and only focused on direct marketing. This inadequacy informs my tenth recommendation of this study which will expand the definition of commercial purposes to include personal data processing for any commercial and economic purposes.

Recommendation 10:

Amend section 2 of the KDPA as follows:
Insert a new definition –
"commercial purposes" includes direct marketing and processing personal data for commercial or economic interests.

5.3.2 Surveillance capitalism harms

In applying the determination-of-adequacy framework, potential harms arising from surveillance capitalism should be identified, and an inquiry carried out to determine whether the law provides mechanisms to mitigate the harms. Citron and Solove identify harms that may be attributed to surveillance capitalism.[11] Where personal data is not processed in line with the rights of a data subject and data protection principles, a data subject may suffer economic harm.[12] Economic harm may result from data breaches which may give rise to identity theft and anxiety to the data subject as they seek to mitigate potential financial effects of incursions into their privacy.[13] Psychological harms that Citron and Solove identify include "anxiety, anguish, concern, irritation, disruption, or aggravation".[14]

Other harms are attributable to AI, automated decision making, and direct marketing practices in what Citron and Solove call "autonomy harms".[15] These they state "involve restricting, undermining, inhibiting, or unduly influencing people's choices. People are prevented from making choices that advance their preferences".[16] In surveillance capitalism there is coercion, manipulation, and failure by surveillance capitalists to provide adequate information to data subjects.[17]

Digital colonialism is another harm. Mhlambi argues that digital colonialism and surveillance capitalism are harms and just like their predecessor colonialism are effected through attacks on personhood. Colonialism attacked "the things that make us feel human and dignified".[18] As per Mhlambi, "digital colonialism and surveillance capitalism enabled by artificial intelligence will not preserve the human dignity of all". [19] Of note is that Article 28 of the

[11]D Citron and D Solove 'Privacy Harms' (2022) *Boston University Law Review* 793 – 863.
[12] Ibid 814 - 819
[13] Ibid.
[14] Ibid 841 – 844.
[15] Ibid 841.
[16] Ibid.
[17] Ibid 848 – 849.
[18] M Mhlambi 'From Rationality to Relationality: Ubuntu as an Ethical & Human Rights Framework for Artificial Intelligence Governance' (2020) *Carr Center Discussion Paper*.
[19] Ibid 5.

Kenyan Constitution provides that "every person has inherent dignity and the right to have that dignity respected and protected". Surveillance capitalism and its nuances negatively impact an individual's right to have their dignity respected and protected.

Another harm is algorithmic bias. Slaughter, Kopec, and Batal submit that algorithms can be used to facilitate discrimination where individuals are targeted based on identified characteristics. [20] Where algorithms are trained using faulty data, the biases and prejudices from the data may be replicated causing inequalities and injustices.[21] This may negatively impact an individual's chances to gain employment, access medical care, housing, education, insurance, or credit facilities.[22] European Digital Rights (EDRi), an international advocacy organisation reports that discrimination and unfair exclusion occurs in targeted online advertising.[23] Such discrimination and exclusion as per EDRi:

> 'in the case of online job or housing ads that either exclude, or predominately target a specific demographic or otherwise defined group, discriminatory outcomes in online advertising mean that protected groups are excluded from opportunities.'[24]

Discrimination runs afoul of Article 27(4) and (5) of the Kenyan constitution:

> '(4) The State shall not discriminate directly or indirectly against any person on any ground, including race, sex, pregnancy, marital status, health status, ethnic or social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth.
>
> (5) A person shall not discriminate directly or indirectly against another person on any of the grounds specified or contemplated in clause (4).'

Algorithmic bias is unconstitutional. Surveillance capitalists producing discriminatory outcomes with their AI, automated decision making, and targeted advertising are in breach of the constitutional right to equality and freedom from discrimination. EDRi argues that apart from discrimination, targeted online advertising can engage in harmful targeting and

[20] R Slaughter, J Kopec, and M Batal 'Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission (2021) *ISP Digital Future Whitepaper & Yale Journal of Law and Technology Special Publication* 7.
[21] Ibid 10.
[22] Ibid 6 – 37.
[23] EDRi H*ow online ads discriminate: Unequal harms of online advertising in* Europe (2021) 11.
[24] Ibid

misclassification in profiling.[25] Profiling has led to proliferation of hate speech, fake news, misinformation, and disinformation online.[26] Algorithms used to push commercial messaging are also used to push hate speech, fake news, misinformation, and disinformation.[27]

The fast paced and constant evolution of algorithms enable surveillance capitalism to grow and become more sophisticated.[28] Slaughter, Kopec, and Batal posit that the opacity in the use of algorithms works towards inhibiting "competition and harm consumers by facilitating anticompetitive conduct and enhancing market power".[29] Ghosh and Couldry report that surveillance capitalism has generated monopolies in consumer internet, social media, email searches, e-commerce, online video sharing, and internet-based texting.[30] The intersection between competition and data protection is discussed later in this chapter.

In recognition that harms may be caused by processing of personal data and in dealing with the harms, section 65(1) of the KDPA states that "a person who suffers damage by reason of a contravention of a requirement of this Act is entitled to compensation for that damage from the data controller or the data processor". Section 65(4) explains that damage "includes financial loss and damage not involving financial loss, including distress". Regulation 14(3)(e) of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 provides that one of the remedies the Data Commissioner may issue is "an order for compensation to the data subject by the respondent".

On damages, Article 82 of the GDPR refers to "material and non-material damages" which may warrant compensation to the data subject.[31] Meanwhile, section 99 of POPIA provides that a data subject may institute an action for damages and that the courts may order an amount to the data subject.[32] My view on this is that the KDPA, the GDPR, and POPIA are at

[25] Ibid 12, 13.
[26] Ibid.
[27] Ibid.
[28] Slaughter, Kopec, and Batal (note 20 above) 7.
[29] Ibid.
[30] D Ghosh and N Couldry 'Digital Realignment Rebalancing Platform Economies from Corporation to Consumer'(2020) *M-RCBG Associate Working Paper Series* 15.
[31] See G Zanfir-Fortuna 'Article 82 Right to compensation and liability' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 1160 – 1179.
[32] See Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (2018) 255 – 258.

par in recognising the potential of harms being caused by processing of personal data and providing for damages in the event that the harms materialise.

While there is yet to be an award for damages directly linked to violations of the KDPA, Kenyan Courts have awarded damages in right to privacy matters. In *C.O.M. v Standard Group Limited*[33] the Petitioner's claim related to publication of his photos in the Respondents' newspaper without his consent, being a violation of his right to privacy under Article 31. The court awarded general damages for pain and suffering to the Petitioner.[34]

In *David Lawrence Kigera Gichuki v Aga Khan University Hospital*[35] the issue in contention was that the Respondent had released medical information in relation to the Petitioner to a third party without consent thus violating the Petitioner's right to privacy under Article 31.[36] In this case, the court was of the view that it was "not satisfied that there was any loss occasioned to the petitioner, or that damages, are as a result of such disclosure, merited" hence no damages were awarded.[37] Another decision on commercial use of personal data is *N W v Green Sports Africa Ltd*[38] the issue in contention was the use of minors' images to promote gambling on billboards. The court made an award for compensation for violation of the right to privacy.

The court decisions indicate that commercial entities may be challenged for processing personal data outside the confines of the law. Legal justifications are fundamental in commercial processing of personal data. Kenyan law is adequate to the extent that it recognises that there may be harm occasioned from processing of personal data and that there ought to be remedies available to an individual who has suffered harm. However, the law is inadequate as it only identifies distress as the harm that is not financial in nature. From the discussions above, non-financial harms could include coercion, and discrimination which informs my eleventh recommendation:

---

[33] *C.O.M. v Standard Group Limited & another* [2013] eKLR
[34] Ibid 32.
[35] Ibid.
[36] Ibid 22.
[37] Ibid 39, 40.
[38] *N W R & another v Green Sports Africa Ltd & 4 others* [2017] eKLR.

Recommendation 11:

Amend section 65(4) of the KDPA as follows:
Insert the words “, discrimination, coercion, and disruption” immediately after the word “damage”.

5.4 What?

Adequate regulation must spell out what information or data is subjected to surveillance capitalism. There is no limit as to the information relating to an identified or identifiable person that is relevant for commercial processing of personal data. Section 2 of the KDPA states that personal data is “any information relating to an identified or identifiable natural person” which is similar to the GDPR definition. Section 1 of POPIA offers a wider definition (I have cited the full text of section 1 of POPIA in chapter three of this study). As I argue in chapter four, while POPIA’s definition is laudable, what is key is that the law regulates any data that may identify a data subject.

Just as I discussed in chapter four, there is information that requires a higher degree of protection. Section 2 of the KDPA singles out "sensitive personal data" which is described as “data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject”. Regulation 15(1) of the Data Protection (General) Regulations, 2021 prohibits the use of sensitive personal data for direct marketing:

> ‘A data controller or data processor may use personal data, other than sensitive personal data, concerning a data subject for the purpose of direct marketing where—
>
> (a) the data controller or data processor has collected the personal data from the data subject;
>
> (b) a data subject is notified that direct marketing is one of the purposes for which personal data is collected;

(c) the data subject has consented to the use or disclosure of the personal data for the purpose of direct marketing;

(d) the data controller or data processor provides a simplified opt out mechanism for the data subject to request not to receive direct marketing communications; or

(e) the data subject has not made an opt out request.'

The above provision is to the effect that even consent is not a justification for processing sensitive personal data for direct marketing purposes. This creates an additional layer of protection to data subjects against direct marketing initiatives. Under Article 9 of the GDPR, sensitive personal data may be processed where there is consent, where the data controller and data processors are obligated to do so under the law, to protect the vital interests of the data subject, where the data is made public by the data subject, for judicial processes, and for public interest. In juxtaposition, section 26 of South Africa's POPIA regarding special personal information:

2. 'A responsible party may, subject to section 27, not process personal information concerning—

...

(c) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

(d) the criminal behaviour of a data subject to the extent that such information relates to—

iii. the alleged commission by a data subject of any offence; or

iv. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.'

To process special personal information, section 27 of POPIA requires that the processing is done either with the consent of the data subject; for an obligation of the law; for historical, research and statistical reasons; and where the data subject makes the information public. Section 27 of POPIA further states that the Information Regulator may authorise a responsible party to process sensitive personal data "if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject".[39]

[39] On pre-authorisation, see De Stadler (note 10 above) 240 – 251.

For direct marketing by means of unsolicited electronic communications, section 69(2) of POPIA states that "a responsible party may approach a data subject:

i. 'whose consent is required in terms of subsection (1)(a); and
ii. who has not previously withheld such consent,
iii. only once in order to request the consent of that data subject.'

Unlike the Kenyan General Regulations, POPIA does not distinguish between personal data and sensitive personal data for direct marketing purposes. Consent may be relied upon to process sensitive personal data for direct marketing purposes.

In my view, when interrogating the "what?" question responses, the key point to consider is what personal data is permitted for processing for commercial purposes. If personal data is sensitive personal data, then as per the KDPA, such data may not be used.[40] A critical examination of the law reveals that it is only for commercial processing of personal data where such restrictions exist. My conclusion is that in identifying the personal data subject to commercial use and regulating it, the law is adequate.

5.5 When?

In this section, I examine the principles that commercial processing of personal data must adhere to. Secondly, I examine the intersection between commercial processing of personal data and legitimate interest. Thirdly, I highlight data protection by design and by default. Fourthly, I make the case for algorithmic transparency, and fifthly, I highlight the place of consumer protection in personal data protection regulation.

[40] See J Turow *The Voice Catchers* (2021).

5.5.1 Commercial use of personal data

"When?" question responses include respect, promotion, and protection of the right to privacy under Article 31 of the Constitution; adherence to data protection principles under section 25 of the KDPA; respecting, protecting, and promoting the rights of the data subjects as per section 26 of the Act; and ensuring that processing of personal data for a commercial purpose is one of the lawful processing operations sanctioned by the Act. A specific response to the "when?" question in commercial processing of personal data is set out in the KDPA and the Data Protection (General) Regulations, 2021. Section 37 of the KDPA provides:

(1) 'A person shall not use, for commercial purposes, personal data obtained pursuant to the provisions of this Act unless the person—
   (a) has sought and obtained express consent from a data subject; or
   (b) is authorised to do so under any written law and the data subject has been informed of such use when collecting the data from the data subject.

(2) A data controller or data processor that uses personal data for commercial purposes shall, where possible, anonymise the data in such a manner as to ensure that the data subject is no longer identifiable.'

Section 37(1)(b) is curious as it seems to indicate that there might be written law that may specifically allow for commercial processing of personal data. Currently, no such law is in place. If the law is enacted, it will have to pass the proportionality test discussed in chapters three and four of this study. Regulation 15(1) of the Data Protection (General) Regulations, 2021 sets out the guidelines for permitted commercial use of personal data specifically for direct marketing:

'a data controller or data processor may use personal data, other than sensitive personal data, concerning a data subject for the purpose of direct marketing where—

   (a) the data controller or data processor has collected the personal data from the data subject;
   (b) a data subject is notified that direct marketing is one of the purposes for which personal data is collected;
   (c) the data subject has consented to the use or disclosure of the personal data for the purpose of direct marketing;

(d) the data controller or data processor provides a simplified opt out mechanism for the data subject to request not to receive direct marketing communications; or

(e) the data subject has not made an opt out request.'

While section 37(1)(a) makes its mandatory to seek and obtain express consent from a data subject for commercial processing of personal data, Regulation 15(1) waters down this provision. Regulation 15(1) grants a data controller or data processor the options set out in sub-regulations 15(1)(a) to (e) by the use of the word "or" before sub-regulation 15(1)(e). The use of "or" denotes a disjunctive interpretation of the sub-regulations whilst if the word used would have been "and", the provisions would have been construed conjunctively. In my view, the correct word that ought to be used is "and" to ensure that all the sub-regulations 15(1)(a) to (e) apply to direct marketing. As the Regulations are subsidiary legislation, the provisions of the Act ought to take precedence; the Regulation is inadequate.

In contrast, Article 21 of the GDPR simply states:

1. 'Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
2. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.'

What Article 21 emphasizes is the option for a data subject to object to use of their personal data for direct marketing and that such objection ought to be complied with.[41] On the other hand, POPIA has provisions similar to section 37 of the KDPA. Section 69(1) of POPIA states:

'The processing of personal information of a data subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs or e-mail is prohibited unless the data subject—

(a) has given his, her or its consent to the processing; or

(b) is, subject to subsection (3), a customer of the responsible party.'

[41] See See G Zanfir-Fortuna 'Section 4 Right to object and automated individual decision-making: Article 21. Right to object' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 508 – 521.

Section 69(3) of POPIA provides:

> 'A responsible party may only process the personal information of a data subject who is a customer of the responsible party in terms of subsection (1)(b)—
>
> (a) if the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;
> (b) for the purpose of direct marketing of the responsible party's own similar products or services; and
> (c) if the data subject has been given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its electronic details—
> (i) at the time when the information was collected; and
> (ii) on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.'

POPIA in the above provision points to the fact that an individual who receives direct marketing be a "customer of the responsible party". This indicates an ongoing relationship between the data subject and the data controller or the data processor. Hence, where there is no ongoing relationship, consent is paramount. POPIA lists the means through which direct marketing may be carried out. The use of the words "any form of electronic communication" in section 69(1) of POPIA acknowledges the fact that emerging technologies may bring with them different ways to carry out direct marketing.[42] In my view, this narrows the scope of regulating direct marketing as it may be carried out in forms that do not constitute electronic communication. Regulation of direct marketing ought to be technology neutral.

Comparing the KDPA, the GDPR, and POPIA, my view is that the KDPA Regulations require minor revision to be considered adequate. This informs my twelfth recommendation:

Recommendation 12:
Amend Regulation 15(1) of the Data Protection (General) Regulations, 2021 as follows: Delete the word "or" appearing immediately before Regulation 15(1)(e) and substitute therefor the word "and".

[42] See De Stadler (note 10 above).

5.5.2 Legitimate interest

Legitimate interest may be a response to the "when?" question. Section 30(1)(b)(vii) of the KDPA provides:

> 'A data controller or data processor shall not process personal data, unless the processing is necessary:
>
> …for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject'.

In addition, Regulation 29(a) of the Data Protection (General) Regulations, 2021 states that "the elements necessary to implement the principle of lawfulness include appropriate legal basis or legitimate interests clearly connected to the specific purpose of processing". Legitimate interests are not defined under the KDPA or in the General Regulations, an indication of inadequacy. Meanwhile, Article 6(1)(f) of the GDPR on legitimate interest:

> 'processing shall be lawful only if and to the extent that at least one of the following applies:
>
> …processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.'

Recital 47 of the GDPR on Article 6(1)(f) interprets 'legitimate interests' to exist "where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller".[43] The Recital goes further to state that "the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest". The riders that Recital 47 sets are, first, that the data subject should reasonably expect the processing of their personal data to include processing for direct marketing.[44] Secondly, the interests, fundamental rights,

[43] EU "GDPR Recitals" available at <Recital 47 - Overriding Legitimate Interest - General Data Protection Regulation (GDPR) (gdpr-info.eu)> last accessed 22 September 2022.
[44] Ibid.

and freedoms of the data subject for purposes of "legitimate interest" processing of personal data will override the interests of the data controller or the data processor.[45]

Conditions necessary for legitimate interests and for processing of personal data to be lawful were enumerated by the Court of Justice of the European Union in *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme":*

> 'first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence.' [46]

The decision calls for responses to four questions when seeking to process personal data for legitimate interests that are commercial in nature. First, has a legitimate interest been identified? Secondly, is the processing of personal data necessary for the identified legitimate interest? Thirdly, what is the balance between the fundamental rights and freedoms of the data subject and the legitimate interests being pursued? Fourthly, what will be the impact on the data subject? Critical is that the legitimate interests be communicated to the data subjects.

In 2014, the European Union Article 24 Data Protection Working Party listed "conventional direct marketing and other forms of marketing or advertisement" as possible legitimate interest activities when processing personal data.[47] Just like the Court of Justice of the European Union decision in *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme" the* Working Party stated that for legitimate interests to prevail, the interests must:

a. 'be lawful (i.e. in accordance with applicable EU and national law);
b. be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently specific);
c. represent a real and present interest (i.e. not be speculative).'

---

[45] Ibid.
[46] *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme"* Case C-13/16 28.
[47] Article 29 Data Protection Working Party *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* Adopted on 9 April 2014 25.

POPIA also provides for legitimate interests. Section 11(1)(f) of POPIA reads: "personal information may only be processed if… processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied". Under section 12(2)(d)(v) of POPIA, information may be collected from another source that is not the data subject "to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied". Just like the KDPA, POPIA does not define what legitimate interest of the responsible party or of a third party. The GDPR Recitals which I associate myself with provide an apt description of legitimate interests.

The conclusion I make is that commercial use of personal data may be a legitimate interest in the processing of personal data. The rider is that such processing must adhere to the law, balance interests, and be specific. Draper and Turrow emphasize on the need for companies to demonstrate commitment to consumer privacy by use of privacy policies and transparency initiatives that adequately keep the data subject informed.[48] This is relevant for data controllers and data processors pursuing the legitimate interest angle to process personal data for commercial purposes. Draper and Turrow caution against the practice used by companies to make it harder for data subjects to comprehend the data controller or data processors personal data processing operations.[49] Companies may use what Draper and Turrow call "placation, diversion, jargon, and misnaming" to confuse data subjects.[50] Draper and Turrow define these:

> 'Placation involves efforts to falsely appease concerns. Diversion refers to efforts to shift individuals' focus away from controversial practices. The use of jargon—terminology that is difficult for those outside a specific group to understand—not only generates confusion, but may frustrate efforts at comprehension. Similarly, misnaming describes efforts to occlude industrial practices through the use of misleading labels.'[51]

[48] N Draper and J Turow 'The corporate cultivation of digital resignation' (2019) *New Media & Society* 1830.
[49] Ibid.
[50] Ibid.
[51] Ibid.

The challenge with the regulation of legitimate interests in Kenya is that while provided for under the KDPA and the General Regulations, they are not defined which informs my thirteenth recommendation:

Recommendation 13:
In view of section 74(1)(a) of the KDPA, the Office of the Data Protection Commission should issue guidance notes on what constitutes legitimate interests in the Kenyan context.

5.5.3 Data protection by design and by default

Another response to the "when?" question is adoption of "privacy-first models". Data protection by design and by default are "privacy-first initiatives" that "do not put the responsibility of data protection on the user. They are designed in such a way that data protection is inherent and functional from the beginning".[52] Processing of personal data is minimised and not extractive as in the surveillance capitalism model. Section 41(1) of the KDPA provides for data protection by default or by design:

> 'every data controller or data processor shall implement appropriate technical and organisational measures which are designed—
>
> (a) to implement the data protection principles in an effective manner; and
> (b) to integrate necessary safeguards for that purpose into the processing.'

Apart from the "proportionality test", and "legitimate interest" test, data controllers and data processors must design their personal data processing operations in a manner that implements data protection principles. Part V of the Data Protection (General) Regulations, 2021 enumerates elements of protection by design or by default to include lawfulness,[53] transparency,[54] purpose limitation,[55] integrity, confidentiality and availability,[56] data

[52] Digital Future Society *Privacy First: A New Business Model for the Digital Era* (2020) 25.
[53] Regulation 29.
[54] Regulation 30.
[55] Regulation 31.
[56] Regulation 32.

minimisation,[57] accuracy,[58] storage limitation, [59] and fairness.[60] Privacy by design or by default means operating within the confines of data protection principles set out under section 25 of the KDPA. In comparison, Article 25 of the GDPR also provides for data protection by design and by default:

1. 'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.'

Recital 78 of the GDPR on privacy by design and by default states:

> 'When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.'[61]

POPIA does not have a provision that specifically spells out privacy by design and by default. The KDPA provisions are similar to the GDPR on privacy by default and by design. The Regulations under the KDPA dig deeper and unpack what constitutes privacy by default and

[57] Regulation 33.
[58] Regulation 34.
[59] Regulation 35.
[60] Regulation 36.
[61] See L. Bygrave 'Article 25. Data protection by design and by default' in C Kuner , L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 571 – 581.

by design. The Regulations in my view are comprehensive and to this extent, the privacy first provisions under the KDPA and General Regulations are adequate.

5.5.4 Automated decision making

Another response to the "when?" question is transparency in automated decision making. Algorithms are used in automated decision-making processes. Where algorithms are applied to the processing of personal data and carrying out automated individual decision making, section 35 of the KDPA states that a "data subject has a right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject".

Algorithmic transparency is critical in surveillance capitalism's processing of personal data. Where a decision that affects a data subject is made through automated processing, section 35(3) of the KDPA requires that the data subject be informed, and that the data subject be able to request reconsideration of the decision. Regulation 22(2) of the Data Protection (General) Regulations, 2021 on automated decision making states:

'pursuant to section 35 of the Act, a data controller or data processor shall—

(a) inform a data subject when engaging in processing based on automated individual decision making;
(b) provide meaningful information about the logic involved;
(c) ensure—
    (i) specific transparency and fairness requirements are in place.
    (ii) rights for a data subject to oppose profiling and specifically profiling for marketing are present; and
    (iii) where conditions specified under section 31 of the Act arise, a data protection impact assessment is carried out;
(d) explain the significance and envisaged consequences of the processing;
(e) ensure the prevention of errors;
(f) use appropriate mathematical or statistical procedures;

(g) put appropriate technical and organisational measures in place to correct inaccuracies and minimise the risk of errors;
(h) process personal data in a way that eliminates discriminatory effects and bias; and
(i) ensure that a data subject can obtain human intervention and express their point of view.'

Section 35 of the KDPA and Regulation 22 of the Data Protection (General) Regulations, 2021 are basic requirements for automated decision making and algorithmic transparency. Article 22 of the GDPR mirrors the above provisions with regulation of automated decision making and profiling. Recital 71 of the GDPR offers guidance on automated decision making that has legal effects on a data subject. Recital 71 cites "automatic refusal of an online credit application or e-recruiting practices" plus analysis and predictions "concerning the data "subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location, or movements" as operations a data subject should not be subjected to without any human intervention.[62] Similarly, section 71(1) of POPIA states:

> '… a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.'[63]

Grochowski, Jabłonowska, Lagioia, and Sartor report that the lack of transparency in automated decision making has the effect of having consumers not knowing the reasons they are offered or denied an opportunity and will not be aware of commercial entities seeking to profit from their vulnerabilities and biases.[64] Grochowski, Jabłonowska, Lagioia, and Sartor rightly argue that the opaque microtargeting using consumers' information for political

[62] See L Bygrave 'Article 22. Automated individual decision-making, including profiling' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 522 – 542.
[63] See De Stadler (note 10 above) 441 – 468 and Burns and Burger-Smidt (note 32 above) 186.
[64] M Grochowski, A Jabłonowska, F Lagioia, and G Sartor 'Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Premises' (2021) *Critical Analysis of Law* 49.

purposes that happened with Cambridge Analytica could also be used in economic contexts.[65] Grochowski, Jabłonowska, Lagioia, and Sartor indicate that lack of transparency may:

> '…limit consumers' understanding and trust and increase the extent to which the suppliers' market power can be arbitrarily used. As a consequence, consumers may be deceived and led into choices they may regret; they may be unable to challenge the behavior of suppliers by exposing unfairness and illegality or to access legal or other redress.'[66]

In my analysis, it is for these reasons that algorithmic transparency as provided for under section 35 of the KDPA and Regulation 22 of the Data Protection (General) Regulations, 2021 is critical. Transparency enhances consumer trust and confidence in the surveillance capitalism market.[67] It is in the quest for algorithmic transparency that the EU came up with the proposed EU Artificial Intelligence Act. While Kenya may consider beefing up provisions on automated decision making processes, in the long term there may be need for specific regulation of technologies to ensure transparency, explainability, and accountability.

Grochowski, Jabłonowska, Lagioia, and Sartor emphasize that attention should be "paid to the accessibility, conciseness and understandability of information" provided to consumers in the quest for transparency.[68] Transparency enables a data subject to exercise their data subject rights.[69] Algorithmic transparency requires that those with access to the technology and interact with it have access to useful information.[70]

In my view, section 35 of the KDPA and Regulation 22 of the General Regulations are adequate in regulating automated decision making. However, I posit that Kenya requires specific regulation of artificial intelligence and algorithms akin to EU's Artificial Intelligence. This informs my fourteenth recommendation:

Recommendation 14:
Enact an Act of Parliament to regulate application of technologies such as Artificial Intelligence

[65] Ibid 46.
[66] Ibid 49.
[67] Ibid.
[68] Ibid 51.
[69] Ibid 53.
[70] Ibid 54.

5.5.5 Consumer protection

Another response to the "when?" question is guaranteeing consumer protection when carrying out surveillance capitalism operations. There is scant academic discussion on the intersection between data protection and consumer protection. Consumer data "forms the foundation of a wide variety of services, products, and business models, with enormous benefits to both competition and consumers".[71] Consumer data is a commodity and as Ohlhausen and Okuliar argue, in surveillance capitalism, "consumer data is both an input for other online services and a commodity asset for advertisers. As an input, detailed consumer data can help improve and refine downstream products and services".[72] Ohlhausen and Okuliar believe that consumer protection provides a good basis to protection of consumer privacy.[73]

Concerns are rife on how processing of consumer information to provide fuel to products and services affects privacy.[74] As consumer data forms the bedrock of products and services, commercial entities ought to provide products or services that respect, protect, and promote a data subject's rights. To ensure respect of privacy, McQuoid-Mason posits that legislation is required that would minimise the intrusiveness occasioned upon consumers, ensure fairness, and create legally enforceable expectations of privacy.[75] Article 46(1) of the Kenyan Constitution protects consumers by providing for consumer rights:

> 'Consumers have the right—
>
> (a) to goods and services of reasonable quality;
> (b) to the information necessary for them to gain full benefit from goods and services;
> (c) to the protection of their health, safety, and economic interests; and
> (d) to compensation for loss or injury arising from defects in goods or services.'

[71] M Ohlhausen and A. Okuliar 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) *Antitrust Law Journal* 130.
[72] Ibid 131.
[73] Ibid 165.
[74] Ibid 132.
[75] D McQuoid-Mason 'Consumer Protection and the Right to Privacy' (1982) *Comparative and International Law Journal of Southern Africa* 135 – 157.

The Consumer Protection Act that gives effect to Article 46 has the aim to "provide for the protection of the consumer, (and) prevent unfair trade practices in consumer transactions".[76] Section 3(4) of the Act lists other purposes of the Act:

> "(a)establishing a legal framework for the achievement and maintenance of a consumer market that is fair, accessible, efficient, sustainable and responsible for the benefit of consumers generally;
>
> (c) promoting fair and ethical business practices;
>
> (d) protecting consumers from all forms and means of unconscionable, unfair, unreasonable, unjust or otherwise improper trade practices including deceptive, misleading, unfair or fraudulent conduct;"

Surveillance capitalism practices that do not pay attention to the rights and interests of a consumer are unfair and unethical trade practices. The Consumer Protection Act lists the unfair and unethical trade practices to include false representation and unconscionable representation. Section 15(1) of the Act requires that "no person shall engage in an unfair practice". Hence the argument for transparency and explainability of algorithms.

On agreements and contracts, section 2 of the Consumer Protection Act defines a consumer agreement to mean "an agreement between a supplier and a consumer in which the supplier agrees to supply goods or services for payment". Section 31 of the Act regulates internet agreements:

(a) 'Before a consumer enters into an internet agreement, the supplier shall disclose the prescribed information to the consumer.
(b) The supplier shall provide the consumer with an express opportunity to accept or decline the agreement and to correct errors immediately before entering into it.
(c) In addition to the requirements set out in section 5, disclosure under this section shall be accessible and shall be available in a manner that ensures that—
    a. the consumer has accessed the information; and
    b. the consumer is able to retain and print the information.'

Section 31 of the Consumer Protection Act somewhat mirrors section 26(a) of the KDPA which provides that "a data subject has a right… to be informed of the use to which their personal

[76] Act No. 46 of 2012. See also J Malala 'Consumer Law and Policy in Kenya' (2018) *Journal of Consumer Policy* 355-372.

data is to be put". Section 29 of the KDPA is relevant as it provides for the duty of the data controller to inform a data subject of:

(a) 'the rights of data subject specified under section 26;
(b) the fact that personal data is being collected;
(c) the purpose for which the personal data is being collected;
(d) the third parties whose personal data has been or will be transferred to, including details of safeguards adopted;
(e) the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data;
(f) a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data;
(g) the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and
(h) the consequences if any, where the data subject fails to provide all or any part of the requested data.'

Sections 26(1) and 29 of the KDPA must be read together with section 31 of the Consumer Protection Act where internet agreements are concerned, and personal data is processed. The above provisions are about statute mandated disclosures which Busch postulates "are a well-suited tool for increasing consumer self-determination and promoting consumer empowerment".[77] In addition, Busch makes a case that mandated disclosures should be personalised and not generic.[78]

The African Union Data Policy Framework while discussing data governance and consumer protection calls for African Union (AU) Member States to pay attention to online consumer protection as they ensure data regulation.[79] The AU framework decrees that "clear, strong and enforceable rules related to data governance can provide adequate defence for digital consumer protection while creating a predictable, structured framework for doing digital business".[80]

[77] C Busch 'Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law' (2019) *University of Chicago Law Review* 310.
[78] Ibid 309-332.
[79] African Union *African Union Data Policy Framework* (2022).
[80] Ibid 33.

The AU framework envisages collaboration between consumer protection regulators and data regulations with specific focus on "digital devices and services, e-commerce".[81] This kind of collaboration is not spelt out under Kenyan law and in my fifteenth recommendation below I propose law reform on how the Office of the Data Protection Commissioner may collaborate with other regulators on matters of mutual interest.

5.5.6 Competition law

Another response to the "when?" question is the need to comply with competition law. The convergence point between competition law and data protection law has not elicited any academic debate in Kenya notwithstanding the fact that personal data has market and monetary value.[82] According to O'Callaghan:

> '… companies monetise personal data by exploiting indirect network effects. On the one side they offer free services to attract as many users as possible and, on the other side, they sell user data to advertisers. The more details a service provider can collect about its users, the more precise information it can sell to its advertisers. This benefits advertisers who can then better target their advertising'.[83]

O'Callaghan further argues:

> 'While online platforms such as Google and Facebook use personal data to enhance users' experiences and provide more personally relevant services, the accumulation of vast amounts of data about consumer behaviour combined with the expansion of targeted advertising imposes costs in the form of the loss of privacy on consumers.'[84]

The processing of personal data in the manner described necessitates the regulation of markets where personal data is traded. O'Callaghan identifies the intersection between

[81] Ibid 32.
[82] F Costa-Cabral and O Lynskey 'Family ties: the intersection between data protection and competition in EU Law' (2017) *Common Market Law Review* 11 – 50.
[83] L O'Callaghan 'The Intersection between Data Protection and Competition Law: How To Incorporate Data Protection, as a Non-Economic Objective, into EU Competition Analysis' (2018) *Trinity College Law Review* 109.
[84] Ibid 128.

competition law and data protection.[85] O'Callaghan argues that competition law is meant to ensure consumer protection and welfare, hence, data subjects largely being consumers require the protection of their personal data to enhance their welfare.[86] As power asymmetries get entrenched in the market place, competition law seeks to protect consumers from unfavourable market power while data protection regulation protects the processing of personal data that causes the asymmetries.[87]

Ohlhausen and Okuliar report that an analysis of data driven industries "demonstrated how valuable personal data can have competitive significance".[88] Unbridled market power can have the effect of exclusive control over large data processing operations.[89] This may act to reinforce market dominance and unfair competition.[90] For large technology companies "data is probably the most critical asset that generates market power".[91] Competition regulation has a role to play in not only regulating fair competition but also directing the governance of personal data. Ohlhausen and Okuliar however, believe that competition law may not be the ideal to deal with consumer privacy issues.[92] This informs my recommendation fifteen below on the need for collaboration between regulators.

The AU Data Policy Framework recognises that competition regulation has a role to play in data governance:

> 'As regulators in Africa struggle to introduce and enforce traditional competition regulation, there is a danger that static competition regulation to govern dynamic and adaptive systems may inhibit innovation and damage the underlying technology that enables innovation. For example, the regulation that focuses on curbing dominance in only the app layer of the Internet could negatively impact and even harm the entire internet and its infrastructure. Regulators need to be cautions of instrumentally applying single-sided market competition rules based on static efficiency models to new data platforms

[85] Ibid 111.
[86] Ibid.
[87] Ibid.
[88] Ohlhausen and Okuliar (note 71 above) 123.
[89] L Cabral, J Haucap, G Parker, G Petropoulos, T Valletti, and M Van Alstyne *The EU Digital Markets Act: A Report from a Panel of Economic Exper*ts (2021) 7.
[90] Ibid.
[91] Ibid 20.
[92] Ohlhausen and Okuliar (note 71 above) 156.

> and products based on dynamic efficiency that may produce innovative complementary products (such as WhatsApp) that enhance consumer welfare and choice or even offer opportunities for local competition on their platforms while being dominant in the underlying global market (Facebook).'[93]

The Framework argues that as data protection laws apply to personal data, competition regulation should apply to data where the control over that data has anti-competitive effects.[94] The Framework calls for AU Member States to "update or adoption of competition law frameworks and regulations that consider the challenges of analysing competition issues, designing remedies and enforcing their powers to safeguard competition in data-driven markets, as well as building the capacity of competition regulators to implement these rules".[95] Kenya does have a Competition Act.[96]

The Competition Act was enacted to "promote and safeguard competition in the national economy; (and) to protect consumers from unfair and misleading market conduct." Section 3 of the Competition Act lists its objects to include protection of consumers and promoting competitiveness. On consumer welfare, Part VI of the Act deals with false and misleading representations, unconscionable conduct, product safety standards, unsafe goods and services, product information standards, and liability for defective goods. The Act does not provide for product information standards and liability for deceitful services. Deceitful services fuel surveillance capitalism. Not providing guidance on deceitful services points to inadequacy.

The Court of Justice of European Union (CJEU) has considered anti-competitive behaviour by dominant players within digital platform services. In *Google and Alphabet v Commission* the CJEU found that Google and Alphabet had abused their dominant position and confirmed fines issued by lower courts.[97] The abuse of power included how they processed personal data in the EU.

---

[93] Ibid 33.
[94] Ibid 34.
[95] Ibid 35.
[96] Act No. 12 of 2010.
[97] *Google and Alphabet v Commission* Case T-612/17.

With a view to tame the anti-competitive behaviour of digital platform services, the European Union formulated the Digital Markets Act.[98] The Preamble of the Act provides that the Regulation has given due regard to the "need to safeguard public order, protect privacy and fight fraudulent and deceptive commercial practices". The Regulation gives due attention to the fact that "data protection and privacy interests of end users are relevant to any assessment of potential negative effects of the observed practice of gatekeepers to collect and accumulate large amounts of data from end users".

Article 1(1) of the Digital Markets Act states that the Act "lays down harmonised rules ensuring contestable and fair markets in the digital sector across the Union where gatekeepers are present". Gatekeepers are defined under Article 3(1) as:

> 'A provider of core platform services shall be designated as gatekeeper if:
>
> (a) it has a significant impact on the internal market;
> (b) it operates a core platform service which serves as an important gateway for business users to reach end users; and
> (c) it enjoys an entrenched and durable position in its operations or it is foreseeable that it will enjoy such a position in the near future.'

In terms of privacy, Article 11(2) on consent states that "where consent for collecting and processing of personal data is required to ensure compliance with this Regulation, a gatekeeper shall take the necessary steps to either enable business users to directly obtain the required consent to their processing"; "gatekeeper shall not make the obtaining of this consent by the business user more burdensome than for its own services". Distinctly, competition law and data protection regulation have similar principles.

It is critical that Kenyan law, just like EU law defines the intersection between competition law and data protection regulation. In surveillance capitalism, the two are seeds in the same pod. The need for law reform in consumer protection and competition law *vis a vis* data protection informs my fifteenth recommendation.

[98] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

Recommendation 15:

Amend the KDPA as follows:

The Act is amended by inserting a new section –

Collaboration with regulators

(a) The Data Commissioner shall collaborate with the relevant regulator(s) where a complaint includes matters outside the provisions of this Act.

(b) In collaborating, the Data Commissioner and the regulator(s) shall:

i) Form joint investigation committees; and

ii) Consider the complaint jointly and issue a joint finding covering all matters before them.

Amend the Competition Act as follows:

The Act is amended by inserting a new section immediately after section 64 –

64A – Liability for deceitful services

(1) Where a person provides services, and such services cause harm as a result of which an individual suffers loss or injury, such person is liable to compensate the individual for the loss or injury suffered.

(2) An individual who suffers loss or damage may recover compensation through court action

5.6 Where?

In Section 3.8 of this study, I have set out the jurisdictional issues related to data protection in Kenya. With section 4 of the KDPA providing the point of reference. The jurisdiction clauses in the KDPA as discussed in chapter three of this study are adequate but require better clarity through guidance notes by the Office of the Data Protection Commissioner which brings me to my sixteenth recommendation:

Recommendation 16:

In view of section 74(1)(a) of the KDPA, the Office of the Data Protection Commission should issue guidance notes on application of section 4 of the KDPA.

5.7 How?

Surveillance capitalism is mostly carried out in a digital environment which must be regulated by law. Key responses to the "how?" question are technology, profiling, and data brokers.

5.7.1 Technology and profiling

In chapter three of this study, I discuss the use of technology and profiling to process personal data. Section 2 of the KDPA defines profiling as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behaviour, location or movements". Profiling is at the centre stage of processing personal data and is well defined under the Act.

5.7.2 Data brokers

While data controllers and data processors may process personal data on their own behalf, data brokers play a crucial role in surveillance capitalism. Neither the KDPA, the GDPR, or POPIA offer a regulatory framework for data brokers. Williams, Brooks, and Shmargad indicate that data brokers collect and collate personal data from public and private sources to create databases of profiles that may be accessible to State organs and surveillance capitalists at a fee.[99] Crain and Nadler report that data brokers "record and synthesize a wide range of

[99] B Williams, C Brooks, and Y Shmargad 'How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications' (2018) *Journal of Information Policy* 81.

consumer data across applications and devices in order to more effectively target them with ads".[100]

The United States Federal Trade Commission (FTC) identifies sources of data for data brokers as government sources, publicly available sources such as social media, blogs, the internet, and commercial data sources.[101] Once collected the data is sold for direct marketing, online marketing, marketing analytics, identity verification, fraud detection, and people search.[102] Some of the clients who purchase data from data brokers for commercial purposes include telecommunication, retail, pharmaceutical, marketing, advertising, technology, non-profit, political, media, financial, insurance, hospitality, energy, transport, and payment firms.[103]

Bounie, Dubus, and Waelbroeck indicate that the data collected by data brokers includes "names, addresses, revenues, loan default information, and registers". [104] Data brokers trade in the data collected to help data controllers and data processors "learn more about their customers to better target ads, tailor services, or price-discriminate consumers".[105] Bounie, Dubus, and Waelbroeck argue that data brokers even decide the quality and quantity of data they put out in the market.[106] Most of the personal data collected by data brokers is collected without paying attention to the rights of the data subject and data protection principles.

In chapter four of this study, I pointed out that the State has access to databases that are created through legislation; for surveillance capitalism and data brokers specifically, these databases become sources of information for surveillance capitalists. Private databases whether created by data brokers are a partial response to the "how?" question. Incidentally,

---

[100] M Crain and A Nadler 'Political Manipulation and Internet Advertising Infrastructure' (2019) *Journal of Information Policy* 376, 377.
[101] United States Federal Trade Commission "Data Brokers: A Call for Transparency and Accountability" (2014) available at < Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission (May 2014) (ftc.gov)> 11 – 18 last accessed 24 March 2022.
[102] Ibid 23 – 34.
[103] Ibid 39, 40.
[104] D Bounie, A Dubus, and P Waelbroeck "Selling Strategic Information in Digital Competitive Markets" (2018) available at < david bouie_ antoine dubus_patrick waelbroeck.pdf (europa.eu)> 2 last accessed 24 March 2022.
[105] Ibid 2.
[106] Ibid 3.

there are no specific regulations that define and govern the operations of data brokers. This brings me to my seventeenth recommendation:

Recommendation 17:

Amend the Data Protection (General) Regulations, 2021 as follows:

Insert new definition –

"data broker" means a data controller or data processor that collects personal data from a variety of sources and offers that information for a consideration".

Insert new Regulations –

(a) A data broker shall register with the Data Commissioner

(b) An application for registration shall include the following information -

i) Description of personal data processed by the data broker;

ii) Sources of personal data;

iii) Evidence of lawful collection of personal data;

iv) A list of data controllers and data processors the data broker sells data to;

v) Contact details of the data broker; and

vi) Measures to implement data protection by design and by default.

(c) The Data Commissioner shall issue a data broker certificate where a data broker meets the requirements for registration.

(d) A certificate under this Regulation shall be for a period of twelve months.

(e) The Data Commissioner may vary or cancel a data broker certificate where the data broker fails to comply with the provisions of the Act and these Regulations.

(f) The Data Commissioner shall keep and maintain a register of the data brokers.

5.7.3 Options for data subjects

Another response to the "how?" question is the options available to data subjects in seeking redress. An individual who has been subjected to surveillance capitalism may make a complaint to the Office of the Data Protection Commissioner in line with section 56 of the KDPA. The complaints handling procedure is outlined in the Data Protection (Complaints

Handling Procedure and Enforcement) Regulations, 2021 whose objectives are stated under Regulation 3:

(a) 'facilitate a fair, impartial, just, expeditious, proportionate and affordable determination of complaints lodged with the Data Commissioner in accordance with the Act and these Regulations, without undue regard to technicalities of procedure;
(b) provide for issuance of enforcement notices as contemplated under section 58 of the Act;
(c) provide for issuance of issuance of penalty notices as contemplated under section 62 of the Act;
(d) provide for the procedure for hearing and determining of complaints; and
(e) provide for the resolution of complaints lodged with the Data Commissioner by means of alternative dispute resolution mechanisms as specified under section 9(1) of the Act.'

To facilitate the complaints handling mechanisms, the Office of the Data Protection Commissioner issued Alternative Dispute Resolution Framework & Guidelines.[107] The Guidelines provide for mediation, conciliation, and negotiation as means of resolving dispute arising out of the KDPA. I discuss the place of alternative dispute resolution in data protection in chapter six of this study.

On complaints Article 56(2) of the GDPR states that each supervisory authority is "competent to handle a complaint lodged with it".[108] POPIA on the other hand under section 74 provides that "any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject".[109]

The KDPA, the GDPR, and POPIA at a minimum provide for complaints handling mechanisms. However, the availability of the mechanisms does not guarantee their success. It is for this reason than in chapter six of this study I interrogate the role of the Office of the Data Protection Commissioner and remedies available to data subjects.

[107] ODPC "Alternative Dispute Resolution Framework & Guidelines" <Alternative Dispute Resolution Framework (ADR) – OFFICE OF THE DATA PROTECTION COMMISSIONER KENYA (odpc.go.ke)> las accessed 20 December 2022.
[108] See H Hijmans 'Article 51. Supervisory authority' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 863 – 872
[109] See Burns and Burger-Smidt (note 32 above) 144.

5.8 Conclusion

Adequacy in personal data regulation specific to surveillance capitalism goes beyond the constitutional right to privacy of an individual. In this chapter I have indicated that regulation assumes that commercial interests may only be articulated through direct marketing. The regulations fail to consider other commercial and economic interests.

Secondly, while regulation identifies harms that may be financial and non-financial, the non-financial harm spelt out is distress. I submit that this does not pay attention to the fact that there are other non-financial harms such as loss of autonomy, restriction of choices, coercion, and discrimination. Nonetheless, Kenyan courts have in the past awarded damages for breach of privacy occasioned by commercial activities.

Thirdly, the description of protected data does not pay attention to emerging technology that constantly innovates new ways to identify data subjects. Fourthly, legitimate interest as far as surveillance capitalism is concerned is vaguely articulated in the law. Fifthly, it is key to note that privacy first models of privacy by design and by default are well provided for in the law. Sixthly, the intersection between consumer protection, competition law and data protection is not spelt out in Kenyan legislation. With these findings, I propose law reforms that are collated in the table below.

Recommendation 10: Amend section 2 of the KDPA as follows: Insert a new definition – "commercial purposes" includes direct marketing and processing personal data for commercial or economic interests.
Recommendation 11: Amend section 65(4) of the KDPA as follows: Insert the words ",discrimination, coercion, and disruption" immediately after the word "damage".
Recommendation 12: Amend Regulation 15(1) of the Data Protection (General) Regulations, 2021 as follows:

Delete the word "or" appearing immediately before Regulation 15(1)(e) and substituting therefor the word "and".

Recommendation 13:

In view of section 74(1)(a) of the KDPA, the Office of the Data Protection Commission should issue guidance notes on what constitutes legitimate interests in the Kenyan context.

Recommendation 14:

Enact an Act of Parliament to regulate application of technologies such as Artificial Intelligence

Recommendation 15:

Amend the KDPA as follows:

The Act is amended by inserting a new section –

Collaboration with regulators

(a) The Data Commissioner shall collaborate with the relevant regulator(s) where a complaint includes matters outside the provisions of this Act.

(b) In collaborating, the Data Commissioner and the regulator(s) shall:

i) Form joint investigation committees; and

ii) Consider the complaint jointly and issue a joint finding covering all matters before them.

Amend the Competition Act as follows:

The Act is amended by inserting a new section immediately after section 64 –

64A – Liability for deceitful or defective services

(1) Where a person provides services, and such services cause harm as a result of which an individual suffers loss or injury, such person is liable to compensate the individual for the loss or injury suffered.

(2) An individual who suffers loss or damage may recover compensation through court action

Recommendation 16:

In view of section 74(1)(a) of the KDPA, the Office of the Data Protection Commission should issue guidance notes on application of section 4 of the KDPA.

Recommendation 17:

Amend the Data Protection (General) Regulations, 2021 as follows:

Insert new definition –

"data broker" means a data controller or data processor that collects personal data from a variety of sources and offers that information for a consideration".

Insert new Regulations –

Data Brokers

(a) A data broker shall register with the Data Commissioner

(b) An application for registration shall include the following information -

i) Description of personal data processed by the data broker;

ii) Sources of personal data;

iii) Evidence of lawful collection of personal data;

iv) A list of data controllers and data processors the data broker sells data to;

v) Contact details of the data broker; and

vi) Measures to implement data protection by design and by default.

(c) The Data Commissioner shall issue a data broker certificate where a data broker meets the requirements for registration.

(d) A certificate under this Regulation shall be for a period of twelve months.

(e) The Data Commissioner may vary or cancel a data broker certificate where the data broker fails to comply with the provisions of the Act and these Regulations.

(f) The Data Commissioner shall keep and maintain a register of the data brokers.

CHAPTER SIX: EFFECTIVE REMEDIES

6.1 Introduction

An adequate regulatory framework ought to provide for effective remedies. In chapter one of this study, I highlighted provisions of the KDPA that point to lack of effective remedies and lack of statutory independence of the Office of the Data Protection Commissioner. In chapter three I highlighted what generally, at a bare minimum must be contained in personal data protection regulation for it to be adequate.

In this chapter I apply the determination-of-adequacy framework set out in chapter three with the "who?", "why?", "what?", "when?", "where?", and "how?" posed on availability of effective remedies. For each question just as in chapters four and five, I outline the Kenyan data protection provisions which I compare with the GDPR and POPIA, and then offer my reflections. In responding to the questions, I indicate whether the responses point to adequate personal data protection regulation in Kenya, and I propose law reforms where the regulation falls short. This presents a refined approach to determination-of-adequacy that is specific to effective remedies as opposed to the general responses set out in chapter three of this study.

In chapter four and five, where I discussed some of the responses to the "how?" question, I pointed to the fact that the KDPA, the GDPR, and POPIA provide for mechanisms for a data subject to access remedies. I also argued that availability of the complaints handling mechanisms does not guarantee an effective remedy. One of the statutory institutions that would provide a measure of success to data protection complaints handling mechanisms is the Office of the Data Protection Commissioner. In this chapter, I interrogate the role of the Office of the Data Protection Commissioner, the courts, and statutory remedies available to data subjects.

6.2 Who?

In chapters four and five, I discussed one response to the "who?" question which is the data subject. In this chapter, I will not belabour on that response, instead, I focus on two responses to the "who?" question, that is, institutions that may offer effective remedies to data subjects, namely, the Office of the Data Protection Commissioner, and the courts.

6.2.1 Office of the Data Protection Commissioner

One of the authorities that may offer the possibility of an effective remedy for data protection disputes is the Office of the Data Protection Commissioner. Section 5 of the KDPA establishes the Office as a body corporate and a State Office in line with Article 260(q) of the Kenyan Constitution. Section 8 of KDPA lists the functions of the Office:

(a) 'oversee the implementation of and be responsible for the enforcement of this Act;
(b) establish and maintain a register of data controllers and data processors;
(c) exercise oversight on data processing operations, either of own motion or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;
(d) promote self-regulation among data controllers and data processors;
(e) conduct an assessment, on its own initiative of a public or private body, or at the request of a private or public body for the purpose of ascertaining whether information is processed according to the provisions of this Act or any other relevant law;
(f) receive and investigate any complaint by any person on infringements of the rights under this Act;
(g) take such measures as may be necessary to bring the provisions of this Act to the knowledge of the general public;
(h) carry out inspections of public and private entities with a view to evaluating the processing of personal data;
(i) promote international cooperation in matters relating to data protection and ensure country's compliance on data protection obligations under international conventions and agreements;
(j) undertake research on developments in data processing of personal data and ensure that there is no significant risk or adverse effect of any developments on the privacy of individuals;'

To execute its functions, section 9 of the KDPA indicates that the Data Commissioner has powers to:

a) 'conduct investigations on own initiative, or on the basis of a complaint made by a data subject or a third party;
b) obtain professional assistance, consultancy or advice from such persons or organisations whether within or outside public service as considered appropriate;
c) facilitate conciliation, mediation and negotiation on disputes arising from the Act;
d) issue summons to a witness for the purposes of investigation;
e) require any person that is subject to the Act to provide explanations, information and assistance in person and in writing;
f) impose administrative fines for failures to comply with this Act;
g) undertake any activity necessary for the fulfilment of any of the functions of the Office; and
h) exercise any powers prescribed by any other legislation.'

The GDPR in comparison, under Article 51(1) states this regarding supervisory authorities:

> "Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union."[1]

Recital 117 of the GDPR emphasises the fact that:

> "The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure."[2]

In comparison, POPIA under section 39 establishes the Information Regulator as a juristic person. Under section 40 of POPIA, the Information Regulator has powers, duties, and functions that include provision of education, monitoring enforcement and compliance,

[1] See H Hijmans 'Article 51. Supervisory authority' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 863 – 872.
[2] Ibid.

handling complaints, conducting research, and facilitating cross border cooperation.[3] Comparing the KDPA, the GDPR and POPIA, my conclusion is that Kenya's personal data protection regulation is adequate to the extent that it establishes the Office of the Data Protection Commissioner and spells out the functions and powers of the Office. The question that I deal with in response to the "when?" question below is whether the Office under the KDPA has complete independence provided for under statute.

6.2.2 Courts

Courts are another avenue for accessing effective remedies. Article 22(1) of the Kenyan Constitution provides that an individual may institute court proceeding if they claim that "a right or fundamental freedom in the Bill of Rights has been denied, violated or infringed, or is threatened". With data protection being derived from Article 31 of the Constitution on the right to privacy, a data subject who has had their right to privacy denied, violated, infringed, or threatened may institute court proceedings. Court proceedings may also ensue where one is dissatisfied with administrative action by the Data Commissioner. Where a remedy requires administrative action, Article 47 of the Kenyan Constitution provides that:

> (1) 'Every person has the right to administrative action that is expeditious, efficient, lawful, reasonable and procedurally fair.
> (2) If a right or fundamental freedom of a person has been or is likely to be adversely affected by administrative action, the person has the right to be given written reasons for the action.'

The KDPA makes reference to the courts in very specific circumstance. Section 64 of KDPA states that "a person against whom any administrative action is taken by the Data Commissioner, including in enforcement and penalty notices, may appeal to the High Court". In comparison, Article 78 of the GDPR provides for the "right to an effective judicial remedy against a supervisory authority":

[3] See E De Stadler, E Hattingh , P Esselaar, and J Boast *Over-Thinking the Protection of Personal Information Act* (2021) 586 – 591.

1. 'Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.
2. Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy where the supervisory authority which is competent pursuant to Article 55 and Article 56 does not handle a complaint or does not inform the data subject within three months on the progress or outcome of the complaint lodged pursuant to Article 77.'[4]

Kotschy reiterates that supervisory authorities under the GDPR are administrative in nature with powers to issue binding decisions which ought to be open to judicial review.[5] Meanwhile, section 97 of POPIA provides:

1. 'A responsible party on whom an information or enforcement notice has been served may, within 30 days of receiving the notice, appeal to the High Court having jurisdiction for the setting aside or variation of the notice.
2. A complainant, who has been informed of the result of the investigation in terms of section 77(3) or 96, may, within 180 days of receiving the result, appeal to the High Court having jurisdiction against the result.'[6]

The gap in section 64 of the KDPA is that it specifically provides for appeals for "persons against whom administrative action is taken", meaning the right of appeal is to data controllers and data processors only. There is no provision within the Act that states that a data subject has a right of appeal for any action or decision made by the Office of the Data Protection Commissioner as is the case with the GDPR and POPIA. This state of affairs renders the KDPA inadequate. To ensure clarity, I submit my eighteenth recommendation:

Recommendation 18:
Amend the KDPA as follows:
The KDPA is amended by deleting Section 64 and substituting therefor the following new section –

[4] See W Kotschy 'Article 78. Right to an effective judicial remedy against a supervisory authority' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 1125 – 1132.
[5] Ibid 1129.
[6] See Y Burns and A Burger-Smidt *A Commentary on the Protection of Personal Information Act* (2018) 237 – 239.

Section 64 – A person aggrieved by a decision or action taken by the Data Commissioner may appeal to the High Court.

Notwithstanding section 64 of the KDPA, a data subject may still rely on Article 23 of the Constitution to seek redress in the courts. Read together with Article 21 of the Constitution, Article 23(1) grants the High Court jurisdiction "in accordance with Article 165, to hear and determine applications for redress of a denial, violation or infringement of, or threat to, a right or fundamental freedom in the Bill of Rights". In line with Article 23(3) the court may grant reliefs that include:

(a) 'a declaration of rights;
(b) an injunction;
(c) a conservatory order;
(d) a declaration of invalidity of any law that denies, violates, infringes, or threatens a right or fundamental freedom in the Bill of Rights and is not justified under Article 24;
(e) an order for compensation; and
(f) an order of judicial review.'

The judicial decisions I discussed in chapter two of this study are a good indicator of the courts taking action where the right to privacy of an individual is infringed. While the court decisions reveal a mixed bag of fortunes, they point to the fact that notwithstanding any statutory provisions, an individual may still seek judicial redress where their right to privacy is denied, violated, or threatened.

6.3 Why?

Where there is a right there is a remedy. There ought to be effective remedies for personal data protection violations. Article 8 of the Universal Declaration of Human Rights (UDHR)

provides for a right to an effective remedy[7] and so does Article 2(3) of the International Covenant on Civil and Political Rights (ICCPR).[8] An effective remedy according to the UDHR and ICCPR has four components. First, there ought to be a violation of a fundamental right that is recognised by law. Secondly, there ought to be a remedy for the violation. Thirdly, the determination of the remedy is to be undertaken by a competent authority. Fourthly, the remedy should be enforced by competent authorities once it is granted.

In the EU, Article 47 of the Charter of Fundamental Rights provides that "everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal".[9] Article 79 of the GDPR provides for a "right to an effective judicial remedy against a controller or processor":

> 'Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.'

Section 38 of the South African Constitution dictates that anyone "has the right to approach a competent court, alleging that a right in the Bill of Rights has been infringed or threatened, and the court may grant appropriate relief, including a declaration of rights".[10] These provisions lay emphasis on the principle that where there is a right, there is a remedy.

Data subject rights are recognised by law in Kenya which means that where a violation occurs, competent authorities must be available to provide effective remedies. Case law has expounded on the right to an effective remedy. The High Court of Kenya in *Republic v Firearms Licensing Board* described an effective remedy:

> 'An internal remedy is effective if it offers a prospect of success, and can be objectively implemented, taking into account relevant principles and values of administrative justice present in the Constitution and the law,

[7] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III).
[8] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171
[9] European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.
[10] Act No. 108 of 1996.

> and available if it can be pursued, without any obstruction, whether systemic or arising from unwarranted administrative conduct. An internal remedy is adequate if it is capable of redressing the complaint."[11]

The South African Constitutional Court in *Fose v Minister of Safety and Security* was of the view that "without effective remedies for breach, the values underlying, and the rights entrenched in the Constitution cannot properly be upheld or enhanced".[12] The African Commission on Human and Peoples' Rights in *Sir Dawda K Jawara v The Gambia* on remedies ruled that "a remedy is considered available if the petitioner can pursue it without impediment, it is deemed effective if it offers a prospect of success, and it is found sufficient if it is capable of redressing the complaint".[13]

From case law and in addition to the four components to an effective remedy, an effective remedy should be one that an individual can pursue without any inhibitions. There ought to be a prospect of success in the available remedies and the remedy ought to be sufficient to address the complaint made to the administrative or judicial authorities. I discuss some of the remedies available below.

Discussing remedies under the right to privacy, Varuhas and Moreham[14] point to the fact that privacy action has always been recognised in common law.[15] Privacy action has involved issues such as phone hacking, revenge porn, covert filming, or the disclosure of sensitive medical, relationship or financial information.[16] While discussing the importance of remedies for breach of privacy, Varuhas and Moreham draw attention to the effects breach of privacy may have on an individual. Breach of privacy could destroy an individual's home life and seriously affect their family.[17] Intrusions on an individual's solitude may cause distress and anxiety.[18] Remedies

[11] *Republic v Firearms Licensing Board & another Ex parte Boniface Mwaura* [2019] eKLR 50.
[12] *Fose v Minister of Safety and Security* (CCT14/96) [1997] ZACC 6; 1997 (7) BCLR 851; 1997 (3) SA 786 (5 June 1997) 69. See G Musila 'The right to an effective remedy under the African Charter on Human and Peoples' Rights' (2006) *African Human Rights Law Journal* 442 – 464.
[13] *Sir Dawda K Jawara v The Gambia* Communication No. 147/95, 149/96 32.
[14] J Varuhas and N Moreham 'Remedies for Breach of Privacy' in J Varuhas and N Moreham(eds.) *Remedies for Breach of Privacy* (Kindle edn 2018).
[15] Ibid Ch. 1.
[16] Ibid Ch. 1.
[17] Ibid.
[18] Ibid Ch. 1.

available for these negative effects include privacy injunctions[19] and damages for breach of privacy.[20]

Varuhas and Moreham posit that "remedies make rights real in practice for plaintiffs. They can provide redress and solace, punish, and condemn outrageous violations, potentially deter future harmful conduct, and vindicate interests that are of importance to individuals and society as a whole".[21] Varuhas and Morenham argue that remedies cannot be divorced from the rights they are tied to.[22] It is for this reason that an effective remedy for the right to privacy and data protection must pay attention to responses to the determination-of-adequacy framework.

Varuhas and Morenham make the argument that "if remedies are analysed in isolation of rights, it is not apparent why a given remedy ought to issue for breach of a given right; there would be no necessary or logical connection between right and remedy"[23]. A determination of whether a remedy is effective will require an analysis of the parties involved, the reason for incursion into a data subject's rights, the harms caused by the incursion, the personal data or information involved, the legitimacy of the incursion, the manner in which the incursion was undertaken, and the environment within which the incursion took place.

The determination-of-adequacy framework is at the centre of effective remedies for the right to privacy and data protection. My conclusion on responses to the "why?" questions is that data protection is a right enshrined in the Constitution and any violation to this right demands an effective remedy.

[19] M Tugendhat 'Privacy Injunctions and the Rule of Law' in J Varuhas and N Moreham(eds.) *Remedies for Breach of Privacy* (Kindle edn 2018) Ch. 2.
[20] J Varuhas 'Varieties of Damages for Breach of Privacy' in J Varuhas and N Moreham(eds.) *Remedies for Breach of Privacy* (Kindle edn 2018) Ch.
[21] J Varuhas and N Moreham 'Remedies for Breach of Privacy' in J Varuhas and N Moreham(eds.) *Remedies for Breach of Privacy* (Kindle edn 2018) Ch 1.
[22] Ibid.
[23] Ibid.

6.4 What?

Responses to the "what?" question in this chapter relate to complaints that are central to seeking effective remedies. Section 56(1) of the KDPA provides for "complaints" to the Data Commissioner with the provision stating that "a data subject who is aggrieved by a decision of any person under this Act may lodge a complaint with the Data Commissioner". The Schedule of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 sets out what would be contained in a complaint.[24] The complaint form under the Regulations includes the particulars of the complainant or their representatives, the description of the complaint, whom the complaint is against, and the remedy sought.

The GDPR under Article 57(1)(f) states that "without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80…".[25] In addition, Article 77(1) of the GDPR provides:

> "without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation".[26]

In juxtaposition, section 74(1) of POPIA states that "any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject". Form 5 of the Regulations Relating to the Protection of Personal Information, 2017 on complaints requires a complainant to provide information on their particulars, particulars of person interfering with personal information, and the reasons for the complaint.[27]

---

[24] Legal Notice No. 264 of 2021.
[25] See H Hijmans 'Article 57. Tasks' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 927 - 938.
[26] See W Kotschy 'Article 77. Right to lodge a complaint with a supervisory authority' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 1125 – 1132.
[27] De Stadler (note 3 above) 596 – 603; see also Y Burns and A Burger-Smidt (note 6 above) 219 – 239.

Looking at the KPDA, the GDPR, and POPIA, a complaint is an allegation of infringements occasioned upon a data subject in relation to their personal data. The KDPA, adequately identifies this and provides for process to address the complaint.

6.5 When?

There are two main responses to the "when?" question when discussing effective remedies. First, is the need to have an independent data protection authority or regulator and secondly, is the need to exhaust available remedies when settling data protection disputes.

6.5.1 Independent data protection authority

The Office of the Data Protection Commissioner exercises its functions and powers as outlined in the KDPA.[28] Section 8(3) of the KDPA requires that the Data Commissioner acts independently. Even with the requirement of independence, some provisions of the KDPA reveal that the independence of the Office of the Data Protection Commissioner is watered down.

Section 5(5) of the KDPA provides that "the Data Commissioner shall in consultation with the Cabinet Secretary, establish such directorates as may be necessary for the better carrying of the functions of the Office". Section 8(2) provides that "the Office of the Data Commissioner may, in the performance of its functions collaborate with the national security organs". The nature of the collaboration is not defined. Under Section 12, a report by the Public Service Commission for removal of the Data Commissioner is made to the Cabinet Secretary. The Cabinet Secretary is to make Regulations and practice guidelines as provided for by sections 35(5), 37(3), 50, and 71. Under section 68, annual financial estimates of the Office of the Data

[28] P Schütz 'Assessing Formal Independence of Data Protection Authorities in a Comparative Perspective' (2012) in J Camenisch, B Crispo, S Fischer-Hübner, R Leenes, and G Russello (eds) *Privacy and Identity Management for Life. Privacy and Identity* 45 – 58.

Protection Commissioner are first submitted to the Cabinet Secretary before tabling in the National Assembly. Also, section 70(1) requires the Office to "submit to the Cabinet Secretary a report of the operations of the Office for the immediately preceding year". The Cabinet Secretary in reference here is the one in charge of information, communication, and technology.

Regulation 26 of the Data Protection (General) Regulations, 2021[29] gives the Cabinet Secretary powers to make determinations on requirement for specified processing to be done in Kenya. Regulation 54 of the same Regulations provides that applications for exemptions on account of national security are made to the Cabinet Secretary. These provisions in the Data Protection (General) Regulations, 2021 indicate that the Office of the Data Protection Commissioner's role is intertwined with that of the Cabinet Secretary. Under statute, the Office of the Data Protection Commissioner is not an independent data protection authority.

Schütz argues that where a supervisory authority such as a data protection authority is subject to administrative supervision by a Ministry for example, it produces "anticipatory obedience" which weakens the independence of the supervisory authority.[30] Kenya's Office of the Data Protection Commissioner is subject to national government supervision with a defined role for the Cabinet Secretary. The fact that section 8(2) of the KDPA calls for collaboration with national security organs that traditionally in their operations constantly make incursions into a data subjects' rights calls to question the *de jure* and *de facto* nature of the independence of the Office of the Data Protection Commissioner.[31]

Inappropriate linkages between the Office of the Data Commissioner and other constitutional, statutory, or public offices ought to be severed. Inappropriate linkages weaken the functions and powers of the Office of the Data Commissioner. The Office ought

[29] Legal Notice NO. 263 of 2021.
[30] Ibid 52.
[31] Ibid 52, 53.

to be impartial and objective.[32] It is critical to personal data protection regulation that the Office be perceived and be seen to be credible, stable, and predictable.[33]

Statutory independence of the Office of the Data Protection Commissioner inspires confidence in availability of effective remedies. Only the Courts should review decisions of the Office as indicated by section 64 of the KDPA which provides for a right of appeal against administrative action taken by the Data Commissioner.[34] To wit:

> 'direct and indirect influence on the decisions of DPAs (and to ensure their obligatory extensive functional independence), it is postulated that these authorities should have, among others, organizational independence (organizational separation from existing ministries and departments), personal and management independence (autonomy over internal administration, staff and protection against dismissal without due cause), and financial independence (an earmarked, secure, and adequate source of funding)'.[35]

Comparatively, Article 51 of the GDPR states that "each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union". On independence of supervisory authorities, Article 52 of the GDPR states:

1. 'Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.
2. The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.
3. Member or members of each supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.
4. Each Member State shall ensure that each supervisory authority is provided with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks

[32] Case Law, 'Principles underlying independence of national data protection authorities: Commission v. Austria' (2013) *Common Market Law Review* 1816.
[33] Ibid 1817.
[34] Ibid 1818.
[35] Ibid 1819.

and exercise of its powers, including those to be carried out in the context of mutual assistance, cooperation and participation in the Board.

5. Each Member State shall ensure that each supervisory authority chooses and has its own staff which shall be subject to the exclusive direction of the member or members of the supervisory authority concerned.
6. Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.'

As for POPIA, section 39(1)(b) provides that the Information Regulator "is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour or prejudice". Section 39(1)(d) further states that the Information Regulator "is accountable to the National Assembly". Section 112(1) of POPIA limits the Minister's role in making Regulations to "the establishment of the Regulator; and fees referred to in section 111(1)". Other Regulations under POPIA are to be enacted by the Information Regulator.

In comparison, Kenya's Data Protection Commissioner is far from independent. Borrowing from POPIA, Kenya's Data Protection Commissioner ought to be accountable to Parliament and should have powers to make Regulations under the KDPA. The independence contemplated by the GDPR and POPIA eludes the Kenyan Data Commissioner simply by the way the KDPA is drafted.

Sajo argues that independence of independent authorities is tied to their "distance from constitutionally recognized branches of power". [36] Independence of these authorities speaks to the integrity of the service which the independent authority renders.[37] According to Sajo, "appointment, dismissal, qualification, fixed term, conflict of interest rules (*incompatibilite*) of commissioners and other independent authority leaders are considered fundamental guarantees of authority independence".[38] Independence is not absolute as the independent

[36] A Sajo, 'Independent Regulatory Authorities as Constitutional Actors: A Comparative Perspective' (2007) *Annales Universitatis Scientiarum Budapestinensis de Rolando Eotvos Nominatae* 14.
[37] Ibid.
[38] Ibid.

authorities ought to be subject to oversight from institutions such as Parliament and courts.[39] Parliament and courts may however, only undertake oversight within their constitutional mandates.[40] Oversight does not mean receiving order or instructions from organs of the State or non-State entities.[41]

The Kenyan Office of the Data Protection Commissioner by having to consult with the Cabinet Secretary on establishment of directorates and being mandated to collaborate with national security organs clearly indicates that the Office will receive orders from these institutions. This in my view has unprecedented impact on the independence of the Office. *De facto* and *de jure* independence is key for the Office of the Data Protection Commissioner to be in a position to offer effective remedies to individuals aggrieved by incursions into their data subject rights. Independence ensures that the Office of the Data Protection Commissioner is a competent authority.

The Court of Justice for the European Union in *European Data Protection Supervisor (EDPS) v Republic of Austria* ruled that independent supervisory authorities are "an essential component of the protection of individuals with regard to the processing of personal data".[42] The court also stated that supervisory authorities "must enjoy an independence which allows them to perform their duties free from external influence".[43] The court argued that data protection authorities "must remain free from any external influence, direct or indirect, which is liable to have an effect on their decisions".[44] The same court in *European Commission v Hungary* on independence of data protection authorities found that:

> 'supervisory authorities responsible for supervising the processing of personal data must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes inter alia any directions or any other external influence in whatever form, whether direct or indirect, which may have an effect on their decisions and which could call into question the performance

[39] Ibid 13, 24.
[40] Ibid 24. See also Case Law (note 32 above) 1822.
[41] Ibid.
[42] *European Data Protection Supervisor (EDPS) v Republic of Austria [2012]* (Case C-614/10) ECLI:EU:C:2012:631,37.
[43] Ibid 41.
[44] Ibid.

by those authorities of their task of striking a fair balance between the protection of the right to private life and the free movement of personal data'[45]

'operational independence of supervisory authorities, in that their members are not bound by instructions of any kind in the performance of their duties, is thus an essential condition that must be met if those authorities are to satisfy the criterion of independence'[46]

'mere risk that the State scrutinising authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter in the independent performance of their tasks.'[47]

In *Maximillian Schrems v Data Protection Commissioner*, the Court of Justice of the European Union reiterated *European Commission v Hungary*:

'The guarantee of the independence of national supervisory authorities is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was established in order to strengthen the protection of individuals and bodies affected by the decisions of those authorities.'[48]

The court posited that national supervisory authorities "must be able to examine, with complete independence, any claim concerning the protection of a person's rights and freedoms in regard to the processing of personal data relating to him".[49] Giurgiu and Larsen reiterate the findings in the above decisions by stating that national supervisory authorities act as guardians of individual rights while ensuring compliance with data protection laws and regulations.[50] It is for this reason that Schütz emphasises the need to have regulatory authorities "independent from government influence".[51]

[45] *European Commission v Hungary [2014]* (Case C-288/12) ECLI:EU:C:2014:237, 51.
[46] Ibid 52.
[47] Ibid 53.
[48] *Maximillian Schrems v Data Protection Commissioner* Case [2015] (Case C-362/14) ECLI:EU:C:2015:650, 41.
[49] Ibid 99. See also M Vidović 'Schrems V Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities'(2015) *Croatian Yearbook of European Law & Policy* 259 – 276.
[50] A Giurgiu and T Larsen 'Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?' (2016) *European Data Protection Law Review* 342.
[51] P Schütz (note 28 above) 47.

My analysis of the KDPA reveals that the Office of the Data Protection Commissioner is not a *de jure* independent office with statutory influence from the Cabinet Secretary and national security organs. The Office may not be able to act impartially and objectively which dents the competence and ability of the Office to offer effective remedies. This state of affairs informs my nineteenth recommendation.

Recommendation 19:

Amend the KDPA as follows:

The KDPA is amended by deleting sub-section 5(5) and substituting therefor the following new sub-section – 5(5) – The Data Commissioner shall establish such directorates as may be necessary for the better carrying of the functions of the Office.

Section 8(2) is hereby deleted.

Section 35(5) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner".

Section 37(3) is amended by deleting the words "Cabinet Secretary, in consultation with the"

Section 59 is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner".

Section 68(3) is amended by deleting the words "Cabinet Secretary for tabling in the"

Section 70(1) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "National Assembly"

Section 70(2) is herby deleted.

Section 71(1) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner".

6.5.2 Exhaustion of remedies

Can an individual take their complaint to the courts and bypass the Data Commissioner? In *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology* an individual had petitioned the High Court directly.[52] In considering the petition, the court stated that section 56 of the KDPA provided data subjects with an internal statutory mechanism to have their complaints addressed. This internal mechanism had to be exhausted before the data subject could approach the courts for remedies. Conversely, the court ruled that a legal person did not have the *locus* to lodge complaints to the Data Commissioner under the KDPA; a legal person could approach the courts directly.

The Court failed to consider section 27 of the KDPA that provides for exercise of rights of data subjects:

> 'A right conferred on a data subject may be exercised—
>
> (a) where the data subject is a minor, by a person who has parental authority or by a guardian;
> (b) where the data subject has a mental or other disability, by a person duly authorised to act as their guardian or administrator; or
> (c) in any other case, by a person duly authorised by the data subject'.

"A person duly authorised by the data subject" may include a legal person. Article 57(1)(f) of the GDPR states that "without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory: handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80…". Article 77(1) further states:

> 'Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.'

[52] *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another (Exparte); Immaculate Kasait, Data Commissioner (Interested Party)* (Judicial Review Application E1138 of 2020) [2021] KEHC 122 (KLR) (Judicial Review) (14 October 2021) (Judgment).

The High Court in *Mwangi & another v Naivasha County Hotel* was specific on exhaustion of remedies under the KDPA.[53] The court ruled that a Petitioner to the High Court had to demonstrate two things, either they had exhausted remedies under the KDPA or were exempt from the exhaustion rule.[54] My view is that the court made the right pronouncement in this matter; exhaustion of remedies under the KDPA is critical.

In South Africa, section 74(1) of POPIA provides that "any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject". Section 1 of POPIA defines a person as "a natural person or a juristic person". Therefore, under POPIA, whether a natural or juristic person, one ought to first articulate their complaints through the Information Regulator. Comparing the KDPA, the GDPR, and POPIA, my take is that they all point to the need to first approach the data protection authority to consider data protection related complaints. The ambiguity created by the Kenyan High Court needs to be remedied.

The *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology* decision is under consideration by the Court of Appeal. Before the Court of Appeal renders its decision, an individual must first exhaust remedies under the KDPA before seeking redress at the High Court. Secondly, the fact that legal persons circumvent the Office of the Data Protection Commissioner was an error in interpretation by the High Court. Unless under exceptional circumstances, all persons whether natural or legal aggrieved by how personal data is processed, should first seek direction from the Office of the Data Protection Commissioner. My view is that the provisions on the need to exhaust remedies under the KDPA are adequate but were misinterpreted by the High Court.

[53] *Mwangi & another v Naivasha County Hotel t/a Sawela Lodges* (Petition E003 of 2021) [2022] KEHC 10975 (KLR) (19 July 2022) (Ruling).
[54] Ibid 30.

6.6 How?

In this section I offer four responses to the "how?" question on effective remedies. First, I look at the process to lodge complaints with the Office of the Data Protection Commissioner. Secondly, I analyse the provision for conciliation, mediation, and negotiation in the complaints handling framework. Thirdly, I discuss judicial action, and fourthly, I interrogate damages for harms caused by violations of the KDPA.

6.6.1 Lodging complaints

Sections 56(2) – 56(5) of the KDPA outline how a complaint may be lodged and handled. The provisions are read together with the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021.[55] Regulation 3 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 outlines their objects and purpose as to:

(a) 'facilitate a fair, impartial, just, expeditious, proportionate and affordable determination of complaints lodged with the Data Commissioner in accordance with the Act and these Regulations, without undue regard to technicalities of procedure;
(b) provide for issuance of enforcement notices as contemplated under section 58 of the Act;
(c) provide for issuance of issuance of penalty notices as contemplated under section 62 of the Act;
(d) provide for the procedure for hearing and determining of complaints; and
(e) provide for the resolution of complaints lodged with the Data Commissioner by means of alternative dispute resolution mechanisms as specified under section 9(1) (c) of the Act.'

Regulation 4 provides that a complaint is to be lodged using Form DPC 1 set out in the Schedule. A complaint may be made orally, through electronic means, or by what the Regulations term as "other appropriate means". Section 56(3) of the KDPA stipulates that

[55] Legal Notice No. 264 of 2021.

where a complaint is made orally, the Data Commissioner is to facilitate a process where the complaint is recorded in writing. Regulation 4(3) indicates that a complaint may be lodged:

(a) 'by the complainant in person;
(b) by a person acting on behalf of the complainant;
(c) by any other person authorized by law to act on behalf of a data subject; or
(d) anonymously.'

The GDPR does not go into much detail on how a complaint may be lodged, but Article 77(1) of GDPR pronounces:

> 'Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.'[56]

Essentially under the GDPR a data subject has the right to lodge a complaint with a supervisory authority. On the other hand, section 75(1) of POPIA dictates that "a complaint to the Regulator must be made in writing" with a rider in section 75(2) that "the Regulator must give such reasonable assistance as is necessary in the circumstances to enable a person, who wishes to make a complaint to the Regulator, to put the complaint in writing". Comparing the KDPA, the GDPR and POPIA, my conclusion is that the KDPA and the Complaints Regulations are adequate in providing for how a complaint may be made to the Office of the Data Protection Commissioner.

6.6.2 Conciliation, mediation, and negotiation

One of the powers of the Office of the Data Protection Commissioner under section 9(1)(c) of the KDPA is to "facilitate conciliation, mediation and negotiation for dispute arising" out of the Act. Regulation 15 of the Data Protection (Complaints Handling Procedure and

[56] See Kotschy (note 26 above).

Enforcement) Regulations, 2021[57] sets out the process for complaints handing through negotiation, mediation, and conciliation. Alternative dispute resolution mechanisms are not new to dispute resolution in Kenya. Article 159(2)(c) of the Kenyan Constitution provides that "alternative forms of dispute resolution including reconciliation, mediation, arbitration and traditional dispute resolution mechanisms shall be promoted".

With the Office of the Data Protection Commissioner having powers to facilitate conciliation, mediation, and negotiation in disputes arising out of the KDPA, it is apparent that these alternative dispute resolution mechanisms might be the norm. For this section though, I focus on mediation as it is provided for in other statutes such as the Civil Procedure Act.[58] Section 2 of the Civil Procedure Act defines mediation:

> "an informal and non-adversarial process where an impartial mediator encourages and facilitates the resolution of a dispute between two or more parties, but does not include attempts made by a judge to settle a dispute within the course of judicial proceedings related thereto".

Section 59B of the Civil Procedure Act empowers a Court to direct a dispute to mediation "on the request of parties concerned; or where it deems it appropriate to do so; or where the law so requires". Section 59B(4) and (5) indicates that an agreement by parties to a mediation is to be "recorded in writing and registered with the Court" and "enforceable as if it were a judgment of that Court" which may not be appealed against. Section 59D indicates that the enforceable agreements are those "entered into with the assistance of qualified mediators".

Under Section 59C "a suit may be referred to any other method of dispute resolution where the parties agree, or the Court considers the case suitable for such referral". Section 59A establishes a Mediation Accreditation Committee that determines "the criteria for the certification of mediators"; proposes "rules for the certification of mediators"; maintains "a register of qualified mediators"; and enforces a "code of ethics for mediators". The court mandated mediation process has been in operation for a few years.

[57] Legal Notice No. 264 of 2021.
[58] Cap 21 Laws of Kenya.

Perhaps to mirror the Civil Procedure Act framework, the Office of the Data Protection Commissioner enacted an "Alternative Dispute Resolution (ADR) Framework/Guideline".[59] The ADR Framework has provision for initiating ADR, commencing ADR, determination for suitability for ADR, ADR facilitators, rules to guide facilitators, management and procedures of ADR, the ADR agreement, and reservation of rights among other provisions. Clause 7 of the ADR Framework lays down what the Data Commissioner is to consider when determining whether a dispute is suitable for ADR. Clause 7 states that a dispute is not eligible for ADR where a settlement would be contrary to the Constitution, the KDPA and any other statute. Secondly, if the dispute necessitates technical interpretation of the law. Thirdly, if judicial intervention would be ideal. Fourthly, if one party is unwilling to submit to ADR. Fifthly, where an enforcement notice has already been issued.

As for the GDPR, Article 40(2)(K) provides for the development of codes of conduct relating to "out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79".[60] Articles 77 and 79 relate to the right to lodge a complaint with a supervisory authority and the right to an effective judicial remedy against a controller or processor respectively. I am yet to come across the code of conduct regulating out of court proceedings under the GDPR.

Section 40(1)(c)(iii) of POPIA provides that the Information Regulation may consult interested parties by "acting as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by a responsible party in the interests of the protection of the personal information of a data subject". Under POPIA, the Information Regulator is the mediator. Clause 10 of the Kenyan ADR Framework stipulates that the Data Commissioner appoints a facilitator who is eligible to facilitate the ADR process, the Data Commissioner is not the mediator. In Kenya, to determine which framework works best will require an analysis

[59] ODPC "Alternative Dispute Resolution Framework/Guidelines" available at < Alternative Dispute Resolution Framework (ADR) – OFFICE OF THE DATA PROTECTION COMMISSIONER KENYA (odpc.go.ke)> last accessed 9 January 2023.

[60] See I Kamara 'Article 40. Codes of Conduct' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) 716 – 724.

of disputes referred to ADR over a period of time. At the time of writing this chapter no referrals to ADR have been publicly acknowledged by the Data Commissioner.

The provision for mediation in statute raises several questions. Does mediation offer an effective remedy for data protection complaints? Will mediation be undertaken by a competent authority? Are data subjects able to pursue mediation without inhibitions? Is there prospect of success with mediation? Is the mediation process sufficient to address data protection complaints?

Hedeen argues that mediation may be "distinguished from other forms of dispute resolution by its (emphasis is) on impartiality, confidentiality, and disputant self-determination".[61] Hedeen submits that self-determination is the bedrock of effective mediation, that is volition of the parties to be involved in the mediation process.[62] Compulsion to be subject to a mediation process erodes the self-determination of the parties.[63]

Feehily discusses the imbalances that exist between parties in a commercial mediation process.[64] As I argued in chapter five of this study, power imbalances exist between a data subject and a data controller or data processor. Due to imbalance of power, Feehily rightly argues that "there is … the possibility of weaker parties being pressured into accepting less than their full entitlement, while the fact that a dispute has been resolved does not guarantee that the public interest has been appropriately served".[65] Feehily emphasizes the need for involvement of courts in commercial mediation processes, for example, in defining the processes and structures.[66] Feehily also points out that commercial mediation unlike the courts does not play an important preventative and precedent-setting role.[67]

[61] T Hedeen 'Coercion and Self-determination in Court-Connected Mediation: All Mediations Are Voluntary, But Some Are More Voluntary than Others' (2005) *The Justice System Journal* 274.
[62] Ibid 275.
[63] Ibid.
[64] R Feehily 'Commercial mediation: commercial conflict panacea or an affront to due process and the justice ideal?' (2015) *The Comparative and International Law Journal of Southern Africa* 317 - 358.
[65] Ibid 321.
[66] Ibid.
[67] Ibid 322.

On power imbalance in mediation, Muigua argues that "the conflict which often involves a compromise and is power-based where the power relations keep changing thus turning the process into a contest of whose power will be dominant".[68] Muigua posits that "court annexed mediation is really not mediation".[69] According to Muigua, in court annexed mediation, the voluntariness and autonomy in relation to the process and outcome are compromised owing to the fact that the mediation is mandated by a court order and any settlement has to be ratified by the court that ordered the mediation.[70]

Muigua contends that court mediation in legal processes lacks "voluntariness; autonomy over the forum; choice of the mediator; control over the process and the outcome".[71] Such dispute resolution processes as per Muigua provide for "superficial addressing the issues of the conflict only and which may later flare up again when power balances change".[72] Where parties are not in a position to voluntarily submit to mediation or where mediation is imposed on them, the mediator will not effectively guide the parties through the mediation process.[73] As Muigua put it, an "order by the court calling for mediation interferes with a fundamental quality of mediation - its voluntary nature."[74] Muigua's submission is that effective mediation is only possible where it is an informal process as opposed to a legal one.[75]

My take on suitability of ADR is that Clause 7 of the ADR Framework eases some doubts. With the Data Commissioner having powers to determine suitability, where applied appropriately, these powers will deal with the issue of power imbalance between the parties. However, since it is the Data Commissioner to appoint the ADR Facilitator, this takes away the autonomy of the parties which is central to an effective mediated process. The Data Commissioner ought to plug into the Judiciary's framework that has the Mediation Accreditation Committee which

[68] K Muigua "Court Sanctioned Mediation in Kenya-An Appraisal" (2015) available at <kmco.co.ke/wp-content/uploads/2018/08/Court-Sanctioned-Mediation-in-Kenya-An-Appraisal-By-Kariuki-Muigua.pdf> last accessed 5th May 2022 6.
[69] Ibid 7.
[70] Ibid.
[71] Ibid 8.
[72] Ibid.
[73] Ibid 10.
[74] Ibid 11.
[75] Ibid 22.

may possibly guarantee of appointment of competent facilitators. This brings me to my twentieth recommendation.

Recommendation 20:
Amend the ADR Framework as follows – Insert a new clause 10.6 – the Data Commissioner shall appoint a facilitator from the list of mediators accredited by the Judiciary Mediation Accreditation Committee.

6.6.3 Judicial action

While the KDPA does not have a provision for appeal by data subjects who may aggrieved by actions or decisions of the Office of the Data protection Commissioner, data subjects may rely on Articles 21 and 23 of the Constitution to seek redress at the High Court. Any action by the Office of the Data Protection Commissioner is administrative action. Article 47 of the Constitution provides for the right to fair administrative action and the Fair Administrative Action Act gives effect to Article 47 of the Constitution.[76] Section 7(2) of the Fair Administrative Action Act provides guidance on institution of judicial review proceedings:

'A court or tribunal under subsection (1) may review an administrative action or decision, if–

(a) the person who made the decision–
  (i) was not authorized to do so by the empowering provision;
  (ii) acted in excess of jurisdiction or power conferred under any written law;
  (iii) acted pursuant to delegated power in contravention of any law prohibiting such delegation;
  (iv) was biased or may reasonably be suspected of bias; or
  (v) denied the person to whom the administrative action or decision relates, a reasonable opportunity to state the person's case;

[76] Act No. 4 of 2015.

(b) a mandatory and material procedure or condition prescribed by an empowering provision was not complied with;
(c) the action or decision was procedurally unfair;
(d) the action or decision was materially influenced by an error of law;
(e) the administrative action or decision in issue was taken with an ulterior motive or purpose calculated to prejudice the legal rights of the applicant;
(f) the administrator failed to take into account relevant considerations;
(g) the administrator acted on the direction of a person or body not authorised or empowered by any written law to give such directions;
(h) the administrative action or decision was made in bad faith;
(i) the administrative action or decision is not rationally connected to–

(i) the purpose for which it was taken;

(ii) the purpose of the empowering provision;

(iii) the information before the administrator; or

(iv) the reasons given for it by the administrator;

(j) there was an abuse of discretion, unreasonable delay or failure to act in discharge of a duty imposed under any written law;
(k) the administrative action or decision is unreasonable;
(l) the administrative action or decision is not proportionate to the interests or rights affected;
(m) the administrative action or decision violates the legitimate expectations of the person to whom it relates;
(n) the administrative action or decision is unfair; or
(o) the administrative action or decision is taken or made in abuse of power.'

Where a data subject is of the view administrative action and a decision of the Office of the Data Protection Commissioner is not expeditious, efficient, lawful, reasonable, procedurally fair, and adversely affects the data subject's rights, the data subject may seek judicial redress. Article 165(6) of the Constitution grants the High Court "supervisory jurisdiction over the subordinate courts and over any person, body or authority exercising a judicial or quasi-judicial function…". This includes supervisory jurisdiction over the Office of the Data Protection Commissioner. My take is that these provisions are adequate.

6.6.4 Damages

What kind of damages that are appropriate in data protection regulation? Varuhas outlines two types of damages when dealing with privacy. First, is what he terms as "normative damages" and secondly, "compensatory damages".[77] Compensatory damages are for "material or factual loss".[78] Normative damages on the other hand are awarded where there is unwarranted interference with the right to privacy and data protection notwithstanding the absence of material or factual loss.[79] According to Varuhas, normative damages for unwarranted incursions into the right to privacy provide strong protection and contribute towards emphasizing the importance of the right.[80] Varuhas argues that the role damages play is to ensure an aggrieved individual is compensated for "negative physical, emotional, psychological or economic effects actually suffered by the claimant in consequence of a wrong, such as costs of repairing a machine, pain and suffering or distress".[81]

Varuhas argues that one's interests ought not be violated and where an incursion is made into the interests without justification, the law ought to recognise the incursion as a violation to the individual.[82] In my analysis, for the courts and the Office of the Data Protection Commissioner to offer effective remedies in the form of damages, they ought to carry out an inquiry which will interrogate whether an incursion into a data subject rights has occurred, whether the incursion was justified and executed according to the law, the kind of personal data that was involved in the incursion, whether harms were occasioned upon the individual, the duration of the incursion, and the manner in which the incursion was carried out.

From the outcome of the inquiry alluded to above, first, where an unwarranted incursion has taken place, normative damages ought to be awarded at first instance. This is due to the fact that there will be proof of a violation of the right to privacy and the claimant would have had

[77] Varuhas (note 20 above).
[78] Ibid.
[79] Ibid.
[80] Ibid.
[81] Ibid
[82] Ibid.

a reasonable expectation for protection of their rights. Normative damages would also impress on the importance of privacy as a constitutional right. Secondly, in awarding any other forms of damages, the inquiry outcome would guide the courts and the Office of the Data Protection Commissioner on the gravity of the violation and the scale of damages to award.

6.7 Conclusion

I have argued and indicated that where a right exists, there must be a remedy. Data subjects must be afforded access to effective remedies. I have indicated that institutions that offer effective remedies to data subjects are the Office of the Data Protection Commissioner, and the courts.

Secondly, I pointed out that while the KDPA provides for internal mechanisms for dispute resolution, the Constitution still provides avenues to seek judicial redress.

Thirdly, I have argued that a determination of whether a remedy is effective will require an analysis of the parties involved, the reason for incursion into the right to privacy and data protection, the harms caused by the incursion, the personal data or information involved, the legitimacy of the incursion, the manner in which the incursion was undertaken, and the environment within which the incursion took place. Thus, the determination-of-adequacy framework is instrumental.

Fourthly, I pointed out that the KDPA adequately identifies and provides for the process to address a data protection related complaint.

Fifthly, with no provision within the KDPA that states that a data subject has a right of appeal for any action or decision made by the Office of the Data Protection Commissioner as is the case with the GDPR and POPIA, the KDPA inadequate and I propose law reforms below.

Sixthly, I revealed that the Office of the Data Protection Commissioner is not an independent office as it has statutory influence from the Cabinet Secretary and national security organs. This points to inadequacy in the law, thus the need for law reform.

Seventhly, I concluded that the KDPA and the Complaints Regulations are adequate in providing for how a complaint may be made to the Office of the Data Protection Commissioner.

Eighthly, supervision by the courts over the Office of the Data Protection Commissioner is adequate.

Ninthly, where an unwarranted incursion has taken place, normative damages ought to be awarded at first instance and other damages issued depending on the gravity of incursions into a data subject's rights.

With these findings, I propose law reforms that are collated in the table below.

Recommendation 18: Amend the KDPA as follows: The KDPA is amended by deleting Section 64 and substituting therefor the following new section – Section 64 – A person aggrieved by a decision or action taken by the Data Commissioner may appeal to the High Court.
Recommendation 19: Amend the KDPA as follows: The KDPA is amended by deleting sub-section 5(5) and substituting therefor the following new sub-section – 5(5) – The Data Commissioner shall establish such directorates as may be necessary for the better carrying of the functions of the Office. Section 8(2) is hereby deleted. Section 35(5) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner". Section 37(3) is amended by deleting the words "Cabinet Secretary, in consultation with the"

Section 59 is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner". Section 68(3) is amended by deleting the words "Cabinet Secretary for tabling in the" Section 70(1) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "National Assembly" Section 70(2) is herby deleted. Section 71(1) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner".
Recommendation 20: Amend the ADR Framework as follows – Insert a new clause 10.6 – the Data Commissioner shall appoint a facilitator from the list of mediators accredited by the Judiciary Mediation Accreditation Committee.

CHAPTER SEVEN: CONCLUSION AND RECOMMENDATIONS

7.1 Overview

In this study I set out to answer five questions:

1. How has data protection evolved in Kenya?
2. What framework should be used to determine the adequacy of data protection regulations?
3. To what extent is the legal framework on state surveillance adequate?
4. To what extent is the legal framework on commercial use of personal data adequate?
5. How adequate are the available remedies in relation to data protection in Kenya?

In the quest to respond to these questions, I analysed data protection regulation in Kenya and made comparisons between the KDPA, the GDPR, and POPIA. In chapter two, I traced the evolution of the right to privacy and data protection since independence from colonial rule. In chapter three, I outlined an objective determination-of-adequacy framework that I used in chapters four, five, and six to determine the extent to which data protection regulation in Kenya was adequate. In chapter four, I focused on adequacy in regulating state surveillance, in chapter five the focus was on adequacy in regulating surveillance capitalism, and in chapter six I zeroed in on adequacy in access to effective remedies in data protection disputes.

The conclusions I draw from this study are pegged on the fact that to ensure adequacy of data protection regulation in Kenya, there ought to be law reforms. In the recommendation section below, I propose amendments to the KDPA, the Data Protection (General) Regulations, the National Intelligence Service Act, and the Competition Act. In addition, I propose enactment of new statutes and regulations in the areas of use of technology and regulating databases. The aim of this chapter is to summarise the conclusions I make in this study. In the next section I summarise the specific responses to the five questions I set to answer in this study.

7.2 Research findings

7.2.1 How has data protection evolved in Kenya?

The independence and post-independence constitutional text provided for the right to privacy on an individual's home and property. The texts indicated the need for consent, justification for violating this right, and situations where the right could be limited. However, the texts did not provide for an express individual right to privacy. It was not until the promulgation of the Constitution of Kenya, 2010 that the individual right to privacy was a right enshrined in the constitutional text under Article 31.

On jurisprudence, the courts have to a large extent ruled in favour of respect, protection, and promotion of the right to privacy. Jurisprudence indicates that courts will interrogate action by State and non-State actors. But the jurisprudence reveals a disjointed approach by the courts in considering damages for breach of the right to privacy and data protection.

On legislation, there is legislation that provides for privacy rights or elements of the rights. One of these is the KDPA enacted in November 2019 and which the High Court declared to apply retrospectively from the date the Constitution of Kenya was promulgated. The KDPA provides a framework to inquire into the adequacy of data protection regulations. The Act unpacks the right to privacy by providing for data subject rights, data protection principles and legitimate processing of personal data.

Other statutes with privacy and confidentiality elements include the Children Act, the HIV and AIDS Control and Prevention Act. Provisions of the HIV and AIDS and Control Act have been subject to disputes considered by the HIV & AIDS Tribunal. The Tribunal often ruling in favour of confidentiality of HIV and AIDS status information and requiring complainants to prove breaches against their confidentiality rights and that they have suffered actual harm in the

process. These Acts, read together with the KDPA ensure comprehensive protection of the right to privacy and data protection in Kenya.

The Registration of Persons Act, the National Intelligence Service Act, the National Police Service Act, and the Private Security Regulation Act are statutes that limit the right to privacy. The National Police Service Act and the Kenya Defence Forces Act expressly limit the right to privacy for individuals who are regulated under the two statutes.

7.2.2 What framework should be used to determine the adequacy of data protection regulations?

The determination-of-adequacy framework I present provides responses to the "who?", "why?", "what?", "when?", "where?", and "how?" questions. Comprehensive responses to these questions reveal whether a country's data protection regulation is adequate. The questions may be used for introspection by Kenya or when Kenya is determining the adequacy of data protection laws of another country. In chapter three of this study, the responses provided the bare minimum that personal data protection regulation must achieve.

The "who?" question responses identify individuals whose activities or information is subject to regulation by law. First, on the "who?" question, an adequate legal framework would identify the natural or legal persons whose personal data is subject to regulation. Secondly, the law ought to identify the natural or legal persons whether in public or private sector who seek to process personal data or information of persons identified in the first response to the "who?" question.

The "why?" question responses identify whether the law provides for explicit and specified justification for personal data protection and for personal data processing. In responding to the "why?" question, attention must be paid to the value of personal data protection. The law ought to provide for checks and balances against those who wish to make incursions into personal data protection. Responses to the "why?" question are made while recognising that

harms may be caused by incursions into data subject rights; hence, it is crucial that the law provides remedies to data subjects for the harms they are subjected to.

On the "what?" question responses, the law ought to indicate the kind of personal data or personal information that is regulated. This may include what may be termed as normal personal data and special or sensitive data. There must be no ambiguity on the nature of data regulated or protected by law.

"When?" question responses identify the legitimate circumstances under which the law allows for processing of personal data. The legitimate reasons that ought to be provided for by law, include consent, contractual obligations, statutory obligations, and public purpose or interest. These legitimate reasons are to be read together with principles of personal data protection set out in law. In responding to the "when?" question, one must pay attention to the fact that the Constitution may provide for the limitation of the right to privacy.

"Where?" question responses relate to jurisdictional issues. The law must answer the question of the territorial scope of the law. Where the law has extra-territorial application, the law ought to be clear and specific on the boundaries of the application.

The "how?" question responses indicate what kind of data processing operations are regulated by law. Does the law regulate the collection, storage, disclosure, transmission, dissemination, destruction, and analysis of personal data? Does the law identify and regulate technology when personal data is processed? This is bearing in mind that technology has an impact on effecting personal data protection. Technology might bring about bias and may be affected by digital and algorithmic colonialism. Hence, it is critical that the law provides a framework to minimise the negative effects technology may have on personal data protection.

Secondly, responses to the "how?" question outline how the law deals with oversight of data protection regulation. Is there an independent oversight authority and what are the powers and functions of that authority? Thirdly, the "how?" question responses identify how the law deals with access to effective remedies for data subjects.

7.2.3 To what extent is the legal framework on state surveillance adequate?

The need for adequate personal data protection is so that State surveillance does not overstep constitutional and legislative boundaries. In applying the determination-of-adequacy framework, I drew several conclusions regarding the adequacy of personal data protection *vis a vis* State surveillance.

First, the Data Protection (General) Regulations do not articulate the mandate of national security organs.

Secondly, the General Regulations do not define what criteria the Cabinet Secretary is to adopt in deciding on exemptions on the ground of national security. The question arises as to how a data controller or data processor who is not a national security organ would be processing personal data for national security purposes; which points to inadequacy.

Thirdly, it is not clear whether the Cabinet Secretary will be providing national security exemptions to private sector entities that aid State surveillance and whether such exemptions would be made public, another indication of inadequacy.

Fourthly, in an indication of adequacy, constitutional and legislative provisions identify the main actors defined as national security organs by Article 239 of the Kenyan Constitution. The law adequately identifies the data controllers and data processors that are constitutionally and legislatively mandated to carryout State surveillance. The law also identifies a data subject who is the focus of personal data protection regulation.

Fifthly, when interrogating harms occasioned by State surveillance, Kenyan law adequately provides for the framework to determine the proportionality of actions undertaken by national security organs.

Sixthly, the law while identifying the personal data subject to protection under the law, it is inadequate to the extent that it does not pay attention to emerging technologies that constantly redefine data sources and data points.

Seventhly, in an indication of adequacy, the law sets out data protection principles to be applied when carrying out State surveillance. Legislation such as the Kenya Defence Forces Act and the National Intelligence Service Act outline guiding principles. The same cannot be said of the National Police Service Act.

Eighthly, the law is adequate in that it provides for sources of data such as databases mandated by law. Such databases include, population register, births and deaths register, voters register, and databases of mobile phone subscribers. The shortfalls in the statutory regulation of the registers are that the law is not specific on who may have or may not have access to the information in these registers. The law does not spell out what security measures ought to be put in place to secure the information contained in the registers. The regulations do not indicate what may happen in case there is unauthorised access to the databases and there is no suggestion of independent oversight over how these databases are managed.

Ninthly, communication surveillance regulation is inadequate to the extent that there are no clear guidelines on independent oversight, there are no indications about the ramifications for abusing communication surveillance, and under the Prevention of Terrorism Act, the State carries out surveillance without the requisite Regulations being in place.

Tenthly, the law is adequate to the extent that it provides avenues for data subjects to seek remedies. These avenues include courts and the Office of the Data Protection Commissioner. However, the National Intelligence Service Act is inadequate as the Intelligence Service Complaints Board that provides an avenue for redress under the Act is not in place.

The conclusion I make is that while there are provisions of the law that adequately regulate State surveillance, there are gaps and ambiguities that must be addressed to raise the level of adequacy.

7.2.4 To what extent is the legal framework in commercial use of personal data adequate?

Adequacy in personal data regulation on surveillance capitalism goes beyond the constitutional right to privacy of an individual. In applying the determination-of-adequacy framework, I drew several conclusions. First, the regulations assume that commercial interests may only be articulated through direct marketing. The regulations fail to consider other commercial and economic interests.

Secondly, while the regulations identify harms that may be financial and non-financial, the non-financial harm spelt out is distress. This does not pay attention to the fact that there are other non-financial harms such as loss of autonomy, restriction of choices, coercion, and discrimination. Nonetheless, Kenyan courts have in the past awarded damages for breach of privacy occasioned by commercial activities.

Thirdly, the description of protected data does not pay attention to emerging technology that constantly innovates new ways to identify data subjects.

Fourthly, legitimate interests as far as surveillance capitalism is concerned are vaguely articulated in the law. Fifthly, models of privacy by design and by default are well provided for in the law. Sixthly, the intersection between consumer protection, competition law and data protection is not spelt out in Kenyan legislation.

The conclusion I make is that while there are provisions of the law that adequately regulate surveillance capitalism, there are gaps and ambiguities that must be addressed to raise the level of adequacy.

7.2.5 How adequate are the available remedies in relation to data protection in Kenya?

Where a right exists, there must be a remedy. Data subjects must be afforded access to effective remedies. In applying the determination-of-adequacy framework, I drew several

conclusions. Institutions that offer effective remedies to data subjects are the Office of the Data Protection Commissioner, and courts. Secondly, while the KDPA provides for internal mechanisms for dispute resolution, the Constitution still provides avenues to seek judicial redress.

Thirdly, a determination of whether a remedy is effective requires an analysis of the parties involved, the reason for incursion into the right to privacy and data protection, the harms caused by the incursion, the personal data involved, the legitimacy of the incursion, the manner in which the incursion was undertaken, and the environment within which the incursion took place. Thus, the determination-of-adequacy framework is instrumental.

Fourthly, the KDPA adequately identifies and provides for the process to address a complaint.

Fifthly, there is no provision within the KDPA that states that a data subject has a right of appeal for any action or decision made by the Office of the Data Protection Commissioner, a situation that needs to be remedied.

Sixthly, the Office of the Data Protection Commissioner is not an independent office as it has statutory influence from the Cabinet Secretary in charge of information, communication, and technology and national security organs. This points to inadequacy in the law.

Seventhly, the KDPA and the Complaints Regulations are adequate in providing for how a complaint may be made to the Office of the Data Protection Commissioner.

Eighthly, supervision by the courts over the Office of the Data Protection Commissioner is adequate. Ninthly, where an unwarranted incursion has taken place, normative damages ought to be awarded at first instance and other damages issued depending on the gravity of incursions into a data subject's rights.

The conclusion I make is that while there are provisions of the law that adequately provide for access to effective remedies, there are gaps and ambiguities that must be addressed to raise the level of adequacy.

7.3 Recommendations

With my conclusions in mind, and the research findings I submit my recommendations for law reforms below.

Recommendation 1:

Amend section 2 of the KDPA as follows:

Insert a new definition –

"public authority" means

(a) an organ, department, or institution in the national or a county government; or

(b) any other organ, department, or institution when—

(i) exercising a power or performing a duty in terms of the Constitution; or

(ii) exercising a public power or performing a public function in terms of any legislation

Amend the Data Protection (General) Regulations as follows:

Insert a new Regulation 54A –

Data subjects for purposes of personal data processing for national security shall include -

(e) 'persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;

(f) persons convicted of a criminal offence;

(g) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and

(h) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).'

Justification: the KDPA ought to define what a public authority under the Act is and define data subjects for purposes of personal data processing for national security purposes.

Recommendation 2:

Amend section 2 of the KDPA as follows:

Insert a new definition –
"national security" means national security as defined under Article 238(1) of the Constitution and includes prevention, investigation, detection or prosecution of criminal offences, and the execution of criminal penalties.

Amend Regulation 54 of the Data Protection (General) Regulations as follows:

- Insert a new paragraph immediately after sub-Regulation 54(1) – "for purposes of this Regulation, mandate means the mandate set out under the Constitution and relevant statutory provisions".
- Delete sub-Regulations 54(2), 54(3), and 54(3) and insert a new sub-Regulation 54(2) – "exemptions shall be limited to a data subject's right:
  (a) to information;
  (b) of access;
  (c) to rectification or erasure of personal data; and
  (d) to restriction of processing.

Justification: the KDPA and the General Regulations should provide clarity on the mandate of national security organs when processing personal data and define the boundaries of exemptions under the Act.

Recommendation 3:

Amend the KDPA by deleting section 30(1)(b)(v).

Justification: it is instructive that the law is clear on regulating State surveillance and providing for limited and specific exceptions that are not vague, broad, or ambiguous.

Recommendation 4:

Amend section 2 of the KDPA as follows:
The definition of "sensitive personal data" is amended to insert the words "political opinions" and "trade union membership" immediately after the phrase "sexual orientation of the data subject".

Justification: the definition of sensitive data under the KDPA is limited and ought to be expanded to include political opinions and trade union membership.

Recommendation 5:

Amend section 25 of the KDPA as follows:
Section 25 is amended by inserting the following new sub-section –
Section 25(i) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

Section 25 is amended by inserting the following new paragraph immediately after section 25(i):

The controller shall be responsible for and be able to demonstrate compliance with this section.

Justification: the current version of the KDPA does not provide for the data protection principles of security and accountability. The proposed amendment remedies this.

Recommendation 6:

Amend Regulation 26(2) of the Data Protection (General) Regulations as follows:

- Insert a new sub-Regulations -
  26(2)(g) – prevention, investigation, detection, or prosecution of criminal offences.
  26(2)(h) – execution of criminal penalties.

Justification: the Regulation needs to provide for limitation of location of where personal data related to prevention, investigation, detection, or prosecution of criminal offences and execution of criminal penalties is processed.

Recommendation 7:

Enact the Data Protection (Statutory Database) Regulations under the KDPA. These proposed Regulations will have provisions similar to the Data Protection (Civil Registration) Regulations, 2020 and cover all databases not provided for in the Data Protection (Civil Registration) Regulations.

Justification: regulation of databases in Kenya is inadequate. Hence, there is a need for new Regulation that provides a regulatory framework for all databases created and managed by the State.

Recommendation 8:

Amend the National Intelligence Service Act as follows:
Section 42 is amended by inserting the following new sub-section –

Section 42(4) an officer of the service who undertakes covert operations contrary to the provisions of this act commits and offence and is liable upon conviction for a fine not exceeding... or to imprisonment for a term not exceeding...or to both.

Justification: the National Intelligence Service Act does not make it an offence for an intelligence officer to intercept communication contrary to the provisions of the Act.

Recommendation 9:

The Cabinet Secretary in charge of internal security shall enact Regulations on interception of communications under the Prevention of Terrorism Act and other enabling statutes. The Regulations under recommendation nine would feature among other issues justification for communication surveillance, limits to the surveillance, independent oversight mechanisms, remedies to data subjects, and penalties for non-compliance.

Justification: the Cabinet Secretary in charge of internal security has over the years through action or omission not enacted regulations required under the Prevention of Terrorism Act.

Recommendation 10:

Amend section 2 of the KDPA as follows:
Insert a new definition –
"commercial purposes" includes direct marketing and processing personal data for commercial or economic interests.

Justification: the KDPA only mentions direct marketing as a commercial purpose for processing personal data. It is therefore instructive to expand the definition of commercial purposes to include all processing for personal data for commercial or economic interests.

Recommendation 11:

Amend section 65(4) of the KDPA as follows:
Insert the words ",discrimination, coercion, and disruption" immediately after the word "damage".

Justification: the KDPA only identifies distress as a non-financial harm. This is limiting hence the expansion of what constitutes non-financial harm.

Recommendation 12:

Amend Regulation 15(1) of the Data Protection (General) Regulations, 2021 as follows:
Delete the word "or" appearing immediately before Regulation 15(1)(e) and substitute therefor the word "and".

Justification: the recommendation corrects a grammatical error in the provision.

Recommendation 13:
In view of section 74(1)(a) of the KDPA, the Office of the Data Protection Commission should issue guidance notes on what constitutes legitimate interests in the Kenyan context.

Justification: legitimate interests are not defined under Kenyan law hence the need to have clarity on what constitutes legitimate interests.

Recommendation 14:

Enact an Act of Parliament to regulate application of technologies 'to data protection' such as Artificial Intelligence

Justification: with the ubiquitous application of AI, it is high time Kenya regulated these technologies to ensure respect, protection, and promotion of fundamental rights and freedoms when the technologies are deployed.

Recommendation 15:

Amend the KDPA as follows:

The Act is amended by inserting a new section –

Collaboration with regulators

(c) The Data Commissioner shall collaborate with the relevant regulator(s) where a complaint includes matters outside the provisions of this Act.

(d) In collaborating, the Data Commissioner and the regulator(s) shall:

i) Form joint investigation committees; and

ii) Consider the complaint jointly and issue a joint finding covering all matters before them.

Amend the Competition Act as follows:

The Act is amended by inserting a new section immediately after section 64 –

64A – Liability for deceitful services

(1) Where a person provides services, and such services cause harm as a result of which an individual suffers loss or injury, such person is liable to compensate the individual for the loss or injury suffered.

(2) An individual who suffers loss or damage may recover compensation through court action

Justification: It is critical that Kenyan law defines the intersection between competition law and data protection regulation and secondly, the Office of the Data Protection Commissioner should collaborate with other regulators where they are dealing with matters of mutual statutory interest.

Recommendation 16:

In view of section 74(1)(a) of the KDPA, the Office of the Data Protection Commission should issue guidance notes on the application of section 4 of the KDPA.

Justification: there is need for clarity on the application of the jurisdictional provisions under section 4 of the KDPA.

Recommendation 17:

Amend the Data Protection (General) Regulations, 2021 as follows:
Insert new definition –
"data broker" means a data controller or data processor that collects personal data from a variety of sources and offers that information for a consideration".

Insert new Regulations –

Data Brokers

(a) A data broker shall register with the Data Commissioner

(b) An application for registration shall include the following information -

i) Description of personal data processed by the data broker;

ii) Sources of personal data;

iii) Evidence of lawful collection of personal data;

iv) A list of data controllers and data processors the data broker sells data to;

v) Contact details of the data broker; and

vi) Measures to implement data protection by design and by default.

(c) The Data Commissioner shall issue a data broker certificate where a data broker meets the requirements for registration.

(d) A certificate under this Regulation shall be for a period of twelve months.

(e) The Data Commissioner may vary or cancel a data broker certificate where the data broker fails to comply with the provisions of the Act and these Regulations.

(f) The Data Commissioner shall keep and maintain a register of the data brokers.

Justification: data brokers and in the business of creating databases for commercial purposes. Currently, there is no regulation of data brokers in Kenya; a situation that must be remedied.

Recommendation 18:

Amend the KDPA as follows:

The KDPA is amended by deleting Section 64 and substituting therefor the following new section –

Section 64 – A person aggrieved by a decision or action taken by the Data Commissioner may appeal to the High Court.

Justification: there is no provision under the KDPA that indicates that a data subject has a right of appeal for any action or decision made by the Office of the Data Protection Commissioner.

Recommendation 19:

Amend the KDPA as follows:

The KDPA is amended by deleting sub-section 5(5) and substituting therefor the following new sub-section –

5(5) – The Data Commissioner shall establish such directorates as may be necessary for the better carrying out of the functions of the Office.

Section 8(2) is hereby deleted.

Section 35(5) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner".

Section 37(3) is amended by deleting the words "Cabinet Secretary, in consultation with the"

Section 59 is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner".

Section 68(3) is amended by deleting the words "Cabinet Secretary for tabling in the"

Section 70(1) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "National Assembly"

Section 70(2) is hereby deleted.

Section 71(1) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner".

Justification: the Office of the Data Protection Commissioner will not be independent so long as the Cabinet Secretary and national security organs have a role to play under the KDPA.

Recommendation 20:

Amend the ADR Framework as follows –

Insert a new clause
10.6 – the Data Commissioner shall appoint a facilitator from the list of mediators accredited by the Judiciary Mediation Accreditation Committee.

Justification: the Data Commissioner ought to plug into the Judiciary's framework that has a Mediation Accreditation Committee which will guarantee appointment of competent facilitators in handling complaints under the KDPA.

Annex 1

The table below groups the proposed amendments according to the specific statutes sought to be amended as they would generally appear in a proposed amendment Bill.

Amendments to the KDPA
Amend section 2 of the KDPA as follows: Insert a new definitions – "commercial purposes" includes direct marketing and processing personal data for commercial or economic interests. "data broker" means a data controller or data processor that collects personal data from a variety of sources and offers that information for a consideration". "public authority" means (a) an organ, department, or institution in the national or a county government; or (b) any other organ, department, or institution when— (i) exercising a power or performing a duty in terms of the Constitution; or (ii) exercising a public power or performing a public function in terms of any legislation "national security" means national security as defined under Article 238(1) of the Constitution and includes prevention, investigation, detection or prosecution of criminal offences, and the execution of criminal penalties. The definition of "sensitive personal data" is amended to insert the words "political opinions" and "trade union membership" immediately after the phrase "sexual orientation of the data subject".
The KDPA is amended by deleting sub-section 5(5) and substituting therefor the following new sub-section – 5(5) – The Data Commissioner shall establish such directorates as may be necessary for the better carrying of the functions of the Office.
Section 8(2) is hereby deleted.
Amend section 25 of the KDPA as follows: Section 25 is amended by inserting the following new sub-section – Section 25(i) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures. Section 25 is amended by inserting the following new paragraph immediately after section 25(i): The controller shall be responsible for and be able to demonstrate compliance with this section.
Amend the KDPA by deleting section 30(1)(b)(v).

Section 35(5) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner".
Section 37(3) is amended by deleting the words "Cabinet Secretary, in consultation with the"
Section 59 is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner".
The KDPA is amended by deleting Section 64 and substituting therefor the following new section – Section 64 – A person aggrieved by a decision or action taken by the Data Commissioner may appeal to the High Court.
Amend section 65(4) of the KDPA as follows: Insert the words ",discrimination, coercion, and disruption" immediately after the word "damage".
Section 68(3) is amended by deleting the words "Cabinet Secretary for tabling in the"
Section 70(1) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "National Assembly" Section 70(2) is herby deleted.
Section 71(1) is amended by deleting the words "Cabinet Secretary" and substituting therefor with the words "Data Commissioner".
In view of section 74(1)(a) of the KDPA, the Office of the Data Protection Commission should issue guidance notes on what constitutes legitimate interests in the Kenyan context.
In view of section 74(1)(a) of the KDPA, the Office of the Data Protection Commission should issue guidance notes on application of section 4 of the KDPA.
The Act is amended by inserting a new section – **Collaboration with regulators** (a) The Data Commissioner shall collaborate with the relevant regulator(s) where a complaint includes matters outside the provisions of this Act. (b) In collaborating, the Data Commissioner and the regulator(s) shall: i) Form joint investigation committees; and ii) Consider the complaint jointly and issue a joint finding covering all matters before them.
Amendments to Data Protection (General) Regulations
Insert new definition – "data broker" means a data controller or data processor that collects personal data from a variety of sources and sells that information
Amend Regulation 15(1) of the Data Protection (General) Regulations, 2021 as follows: Delete the word "or" appearing immediately before Regulation 15(1)(e) and substituting therefor the word "and".
Amend Regulation 26(2) of the Data Protection (General) Regulations as follows: • Insert a new sub-Regulations - 26(2)(g) – prevention, investigation, detection, or prosecution of criminal offences. 26(2)(h) – execution of criminal penalties.

- Insert a new paragraph immediately after sub-Regulation 54(1) – "for purposes of this Regulation, mandate means the mandate set out under the Constitution and relevant statutory provisions".
- Delete sub-Regulations 54(2), 54(3), and 54(3) and insert a new sub-Regulation 54(2) – "exemptions shall be limited to a data subject's right:
  (a) to information;
  (b) of access;
  (c) to rectification or erasure of personal data; and
(d) to restriction of processing.

Insert a new Regulation 54A –
Data subjects for purposes of personal data processing for national security shall include -

(a) 'persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
(b) persons convicted of a criminal offence;
(c) victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and
(d) other parties to a criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, persons who can provide information on criminal offences, or contacts or associates of one of the persons referred to in points (a) and (b).'

Insert new Regulations –

Data Brokers

(a) A data broker shall register with the Data Commissioner

(b) An application for registration shall include the following information -

  i) Description of personal data processed by the data broker;

  ii) Sources of personal data;

  iii) Evidence of lawful collection of personal data;

  iv) A list of data controllers and data processors the data broker sells data to;

  v) Contact details of the data broker; and

  vi) Measures to implement data protection by design and by default.

(c) The Data Commissioner shall issue a data broker certificate where a data broker meets the requirements for registration.

(d) A certificate under this Regulation shall be for a period of twelve months.

(e) The Data Commissioner may vary or cancel a data broker certificate where the data broker fails to comply with the provisions of the Act and these Regulations.

(f) The Data Commissioner shall keep and maintain a register of the data brokers.

Amendments to the National Intelligence Service Act

Section 42 is amended by inserting the following new sub-section –
Section 42(4) an officer of the service who undertakes covert operations contrary to the provisions of this act commits and offence and is liable upon conviction for a fine not exceeding... or to imprisonment for a term not exceeding...or to both.

Amendments to the Competition Act

The Act is amended by inserting a new section immediately after section 64 – **64A – Liability for deceitful services** (1) Where a person provides services, and such services cause harm as a result of which an individual suffers loss or injury, such person is liable to compensate the individual for the loss or injury suffered. (2) An individual who suffers loss or damage may recover compensation through court action
Amendments to the ADR Framework
Insert a new clause 10.6 – the Data Commissioner shall appoint a facilitator from the list of mediators accredited by the Judiciary Mediation Accreditation Committee.
New Statutes and Regulations
Enact the Data Protection (Statutory Database) Regulations under the KDPA. These proposed Regulations will have provisions similar to the Data Protection (Civil Registration) Regulations, 2020 and cover all databases not provided for in the Data Protection (Civil Registration) Regulations.
The Cabinet Secretary in charge of internal security shall enact Regulations on interception of communications under the Prevention of Terrorism Act and other enabling statutes. The Regulations under recommendation nine would feature among other issues justification for communication surveillance, limits to the surveillance, independent oversight mechanisms, remedies to data subjects, and penalties for non-compliance
Enact an Act of Parliament to regulate application of technologies such as Artificial Intelligence

BIBLIOGRAPHY

Books

Black's Law Dictionary 9th Edition (2009) Minnesota: West.

Burns Y and Burger-Smidt A *A Commentary on the Protection of Personal Information Act* (2018) Durban: LexisNexis.

Crain M *Privacy Over Profit* (2021) Minnesota: University of Minnesota Press.

De Stadler E, Hattingh I, Esselaar P, and Boast J *Over-Thinking the Protection of Personal Information Act* (2021) Cape Town: Juta and Company Ltd.

Duncan J *Stopping the Spies: Constructing and resisting the surveillance state in South Africa* (2018) Johannesburg: Wits University Press.

Farrell H and Newman A *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security* (2019) Princeton: Princeton University Press.

Foucault M *Discipline and Punish: The Birth of the Prison* (1975) New York: Vintage Books.

Frey R *Interests and Rights, The Case* Against Animals (1980) New York: Oxford University Press.

Gaines P *From Truth to Technique at Trial* (2016 New York: Oxford University Press.

Gichuhi A *Litigation: The Arts of Strategy and Practice* (2017) Nairobi: LawAfrica Publishing.

Kipling R *Just Do Stories* (1902) Minnesota: Squid Ink Classics.

Kuner C, Bygrave L and Docksey C (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Lumumba P and Mbondenyi M *The Constitution of Kenya: Contemporary Readings* (2011) Nairobi: LawAfrica Publishing.

Mbondenyi M and Ambani O *The New Constitutional Law of Kenya: Principles, Government and Human Rights* (2012) Nairobi: LawAfrica Publishing.

Mill J *On Liberty* (Kindle Edn 1859). London: Arcturus Classics

Moore A *Privacy Rights: Moral and Legal Foundations* (2010) Pennsylvania: The Pennsylvania State University Press

Moore B *Privacy: Studies in Social and Cultural History* (1984) London: Routledge.

Muigai G and Juma D *Power, Politics & Law: Dynamics of Constitutional Change in Kenya, 1887 – 2002* (2022) Kabarak: Kabarak University Press.

Richard L and Rigaud S *Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy* (2023) New York: Henry Holt & Company Inc.

Richardson J *Law and the Philosophy of Privacy* (2016) New York: Routledge.

Roos A 'Legal Protection of Personal Information' in J Neethling, J Potgieter and A Roos *Neethling on Personality Rights* (2019) Johannesburg: LexisNexis.

Russell S *Human Compatible: AI and the Problem of Control* (Kindle Edn. 2019) USA: Penguin Books

Samuel G *An Introduction to Comparative Law Theory and Method* (2014) Oxford: Hart Publishing.

Schwab K *The Fourth Industrial Revolution* (2016) Geneva: World Economic Forum.

Selinger E and Hartzog W 'Obscurity and Privacy' in J Pitt and A Shew (eds.) *Routledge Companion to Philosophy of Technology* (2014) London: Routledge.

Snowden E *Permanent Record* (Kindle Edn 2019) London: Macmillan.

Solove D *Understanding privacy* (2008) Cambridge: Harvard University Press.

Tugendhat M 'Privacy Injunctions and the Rule of Law' in Varuhas J and Moreham N (eds.) *Remedies for Breach of Privacy* (Kindle edn 2018) Sydney: Hart Publishing

Turow J *The Voice Catchers* (2021) New Haven: Yale University Press.

Veliz C *Privacy is Power* (Kindle Edn 2020) London: Melville House.

Watt E *State Sponsored Cyber Surveillance* (2021) London: Elgar.

Wyle C *Mind F*ck* (Kindle Edn 2019) London: Random House.

Zuboff S *In the Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Kindle Edn 2019) New York: Public Affairs – Hachette Book Group.

Chapters in books

Austin L 'Lawful Illegality: What Snowden Has taught Us about the Legal Infrastructure of the Surveillance State' (2015) *in* M Geist (ed) *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* Ottawa: University of Ottawa Press.

Bhat P 'Historical Legal Research: Implications and Applications' (2019) in P Bhat *Idea and Methods of Legal Research* Oxford: Oxford University Press.

Bygrave L 'Article 22. Automated individual decision-making, including profiling' in Kuner C, Bygrave L and Docksey C (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Bygrave L 'Article 25. Data protection by design and by default' in Kuner C, Bygrave L and Docksey C (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Bygrave L and L Tosoni L 'Article 4(11) Consent' in Kuner C, Bygrave L and Docksey C (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Christakis T and Bouslimani K 'National Security, Surveillance and Human Rights' in R. Geiss, N. Melzer (Eds), *Oxford Handbook on the International Law of Global Security* (2021) Oxford: Oxford University Press.

Geist M 'Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era' in M Geist (ed) *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (2015) Ottawa: University of Ottawa Press.

Georgieva L and Kuner 'Article 9. Processing of special categories of personal data' Kuner C, Bygrave L and Docksey C (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Gutwirth S and Hert P 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E Claes, A Duff & S Gutwirth (eds..), *Privacy and the criminal law* (2006) Antwerp/Oxford: Intersentia.

Hijmans H 'Article 51. Supervisory authority' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Hijmans H 'Article 57. Tasks' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Kamara I 'Article 40. Codes of Conduct' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Kosta E 'Article 7 Conditions for consent' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Kotschy W 'Article 6. Lawfulness of processing' in in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Kotschy W 'Article 77. Right to lodge a complaint with a supervisory authority' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Kotschy W 'Article 78. Right to an effective judicial remedy against a supervisory authority' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Kotschy W 'Article 79 Right to an effective judicial remedy against a controller or processor' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Kulhari S 'Data Protection, Privacy and Identity: A Complex Triad' in *Building-Blocks of a Data Protection Revolution* (2018) Berlin: Nomos Verlagsgesellschaft mbH.

Kuner C'Chapter V: Transfers of Personal Data to Third Countries or International Organisations (Articles 44–50)' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) (2020) Oxford: Oxford University Press.

Makulilo A 'The Context of Data Privacy in Africa' in A Makulilo (ed) *African Data Privacy Laws* (206) Bremen: Springer.

Polčák R 'Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Rodotà S 'Data Protection as a Fundamental Right' S Gutwirth, Y Poullet, P Hert, C Terwangne, S Nouwt (eds) *Reinventing Data Protection?* (2009) Brussels: Springer.

Roos A 'Legal Protection of Personal Information' in J Neethling, J Potgieter and A Roos *Neethling on Personality Rights* (2019) Johannesburg: LexisNexis South Africa.

Roos A *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* (2003) LLD Thesis: UNISA.

Rouvroy A and Poullet Y 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' S Gutwirth, Y Poullet, P Hert, C Terwangne, S Nouwt (eds) *Reinventing Data Protection?* (2009) Brussels: Springer.

Scassa T 'A Human Rights-Bases Approach to Data Protection in Canada' in E. Dubois and F Martin-Bariteau (eds.) *Citizenship in a Connected Canada: A Research and Policy Agenda* (2020) Ottawa: University of Ottawa Press.

Schütz P 'Assessing Formal Independence of Data Protection Authorities in a Comparative Perspective' (2012) in J Camenisch, B Crispo, S Fischer-Hübner, R Leenes, and G Russello (eds) *Privacy and Identity Management for Life. Privacy and Identity* Heidelberg, Dordrecht: Springer.

Selinger E and Hartzog W (2018) 'Obscurity and Privacy' in J Pitt and and A Shew *Spaces for the Future: A Companion to Philosophy of Technology* New York: Routledge.

Silungwe C 'On 'African' Legal Theory: A Possibility, an Impossibility or Mere Conundrum? in O Onazi (ed) *African Legal Theory and Contemporary Problems* (2014) New York: Springer.

Svantesson D 'Article 3. Territorial scope' in in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Terwangne C 'Article 5. Principles relating to processing of personal data' in in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Tosoni L and Bygrave L 'Article 4. Definitions' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Tosoni L and Bygrave L 'Article 4(2). Processing' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Tugendhat M 'Privacy Injunctions and the Rule of Law' in J Varuhas and N Moreham(eds.) *Remedies for Breach of Privacy* (Kindle edn 2018) Sydney: Hart Publishing.

Varuhas J 'Varieties of Damages for Breach of Privacy' in Varuhas J and Moreham N (eds.) *Remedies for Breach of Privacy* (Kindle edn 2018) Sydney: Hart Publishing.

Varuhas J and Moreham N 'Remedies for Breach of Privacy' in Varuhas J and Moreham N(eds.) *Remedies for Breach of Privacy* (Kindle edn 2018) Sydney: Hart Publishing.

Zanfir-Fortuna G 'Section 4 Right to object and automated individual decision-making: Article 21. Right to object' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Zanfir-Fortuna G 'Article 82 Right to compensation and liability' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Zerdick T 'Article 52. Independence' in C Kuner, L Bygrave and C Docksey (eds) *The EU General Data Protection Regulation (GDPR): A Commentary* (2020) Oxford: Oxford University Press.

Journal articles

Abdulrauf L 'The Challenges for the Rule of Law Posed by the Increasing Use of Electronic Surveillance in Sub-Saharan Africa' (2018) African Human Rights Law Journal 365.

Agbor T, Kandeh A, and Futcher L 'Enforcement of the Protection of Personal Information (POPI) Act : perspective of data management professionals.' (2018) South *African Journal of Information Management* 1

Andrus M 'The New Oil: The Right to Control One's Identity in Light of the Commoditization of the Individual' (2017) *Business Law Today* 1.

Austin L 'Is Consent the Foundation of Fair Information Practices? Canada's Experience under Pipeda' (2006) *The University of Toronto Law Journal* 181.

Barrett L 'Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries' (2019) *Seattle University Law Review* 1057.

Basimanyane D 'The Regulatory Dilemma on Mass Communications Surveillance and the Digital Right to Privacy in Africa: The Case of South Africa' (2022) African Journal of International and Comparative Law 361.

Birhane A 'Algorithmic Colonization of Africa' (2020) *SCRIPTed* 389.

Boorstin D 'Tradition and Method in Legal History' (1941) *Harvard Law Review* 424.

Borgesius F 'Personal Data Processing for Behavioural Targeting: Which Legal Basis?' (2015) *International Data Privacy Law* 163.

Boshe P, Hennemann M and Meding R 'African Data Protection Laws Current Regulatory Approaches, Policy Initiatives, and the Way Forward'(2021) *Global Privacy Law Review* 34.

Bruin B 'The Liberal Value of Privacy' (2010) *Law and Philosophy* 505.

Busch C 'Implementing Personalized Law: Personalized Disclosures in Consumer Law and Data Privacy Law' (2019) *University of Chicago Law Review* 309.

Cath C 'Governing artificial intelligence: ethical, legal and technical opportunities and challenges (2018) *Philosophical Transactions of the Royal Society* 2.

Chirwa D 'In search of philosophical justifications and suitable models for the horizontal application of human rights' (2008) *African Human Rights Law Journal* 294.

Chirwa D 'The Doctrine of State Responsibility as a Potential Means of Making Private Actors Accountable for Human Rights' (2004) *Melbourne Journal of International Law* 1.

Citron D and Solove D 'Privacy Harms' (2011) *GW Law School Public Law and Legal Theory Paper No. 2021-1, GW Legal Studies Research Paper No. 2021-11* 3.

Citron D and Solove D 'Privacy Harms' (2022) *Boston University Law Review* 793.

Cohen J 'What Privacy is For' (2013) *Harvard Law Review* 1904.

Coleman D 'Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws' (2019) *Michigan Journal of Race & Law* 417.

Corlett J 'The Nature and Value of the Moral Right to Privacy' (2002) *Public Affairs Quarterly* 329.

Costa-Cabral F and Lynskey O 'Family ties: the intersection between data protection and competition in EU Law' (2017) *Common Market Law Review* 11 .

Couldry N and Mejias U, 'Data colonialism: rethinking big data's relation to the contemporary subject' (2018) *Television and New Media* 336.

Crain M and Nadler A 'Political Manipulation and Internet Advertising Infrastructure' (2019) *Journal of Information Policy* 370.

Dale W 'The Making and Remaking of Commonwealth Constitutions' (1993) *The International and Comparative Law Quarterly* 67.

De Hert P and Gutwirth S 'Privacy, data protection and law enforcement: Opacity of the individual and transparency of power' (2006) *Privacy and the criminal law* 61.

De Hert P 'Data Protection as Bundles of Principles, General Rights, Concrete Subjective Rights and Rules: Piercing the Veil of Stability Surrounding the Principles of Data Protection' (2017) *European Data Protection Law Review* 160.

Draper N and Turow J 'The corporate cultivation of digital resignation' (2019) *New Media & Society* 1824.

Du Plessis L 'The Status and Role of Legislation in South Africa as a Constitutional Democracy: Some Exploratory Observations' (2011) *Potchefstroom Electronic Law Journal* 14(4).

Dubber M 'Historical Analysis of Law' (1998) *Law and History Review* 159.

Eberle E 'The Right to Information Self-Determination' (2001) *Utah Law Review* 965.

Fan M 'The Public's Right to Benefit from Privately Held Consumer Big Data' (2021) *NYU Law Review* 35.

Feehily R 'Commercial mediation: commercial conflict panacea or an affront to due process and the justice ideal?' (2015) *The Comparative and International Law Journal of Southern Africa* 317.
Feinberg J 'In Defence of Moral Rights' (1992) *Oxford Journal of Legal Studies* 149.

Gerver M 'Consent for Data on Consent' (2015) *Ethical Theory and Moral Practice* 799.

Ghosh D and Couldry N 'Digital Realignment Rebalancing Platform Economies from Corporation to Consumer'(2020) *M-RCBG Associate Working Paper Series* 6.

Gill A and Jaiswal A 'Data Surveillance: Need for A Policy To Achieve Equilibrium Between State And Individual Interest' (2018) *Nirma University Law Journal* 57.

Giurgiu A and Larsen T, 'Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?' (2016) *European Data Protection Law Review* 342.

Gligorijević J 'Children's privacy: the role of parental control and consent' (2019) *Human Rights Law Review* 201.

Grochowski M, Jabłonowska A, Lagioia F, and Sartor G 'Algorithmic Transparency and Explainability for EU Consumer Protection: Unwrapping the Regulatory Premises' (2021) *Critical Analysis of Law* 43.

Hafner-Burton E, Heifer L, and Fariss C 'Emergency and Escape: Explaining Derogations from Human Rights Treaties' (2011) *International Organization* 673.

Hallborg R 'Principles of Liberty and the Right to Privacy' (1985) *Law and Philosophy* 175.

Hartzog W and Selinger E 'Surveillance as Loss of Obscurity' (2015) *Washington and Lee Law Review* 1343.

Hedeen T 'Coercion and Self-determination in Court-Connected Mediation: All Mediations Are Voluntary, But Some Are More Voluntary than Others' (2005) *The Justice System Journal* 273.

Hu M 'Algorithmic Jim Crow' (2017) *Fordham Law Review* 633.

Huscroft G, Miller B, and Webber G 'Proportionality and the Rule of Law: Rights, Justification, Reasoning' (2014) *Cambridge University Press* 21.

Hutchinson and N Duncan N 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) *Deakin Law Review* 83.

Kang J 'Information Privacy in Cyberspace Transactions' (1998) *Stanford Law Review* 1193.

Kilovaty I 'Psychological Data Breach Harms' (2021) *North Carolina Journal of Law & Technology* 1.

King J and Stephan A 'Regulating Privacy Dark Patterns In Practice—Drawing Inspiration From California Privacy Rights Act' (2021) Georgetown Law Technology Review 26.

Kulhari S 'Data Protection, Privacy and Identity: A Complex Triad' in *Building-Blocks of a Data Protection Revolution* (2018) 23.

Lipton J 'Mapping Online Privacy' (2009) *Case Research Paper Series in Legal Studies: Working Paper* 09.

Lyon D 'State and Surveillance' (2019) in CIG *Governing Cyberspace during a Crisis in Trust* 1.

Macnish K 'An Eye for an Eye: Proportionality and Surveillance' (2015) *Ethical Theory and Moral Practice* 529.

Makulilo A 'Privacy and Data Protection in Africa: A State of the Art' (2012) *International Data Privacy Law* 163.

Malala J 'Consumer Law and Policy in Kenya' (2018) *Journal of Consumer Policy* 355.

Martin A 'Mobile Money Platform Surveillance' (2019) *Surveillance & Society* 213.

Marx G 'A Tack in the Shoe: Neutralizing and Resisting the New Surveillance' (2003) *Journal of Social Issues* 369.

Mavedzenge J 'The Right to Privacy v National Security in Africa: Towards a Legislative Framework which Guarantees Proportionality in Communications Surveillance' (2020) *African Journal of Legal Studies* 360.

McQuoid-Mason D 'Consumer Protection and the Right to Privacy' (1982) *Comparative and International Law Journal of Southern Africa* 135.

Mhlambi M 'From Rationality to Relationality: Ubuntu as an Ethical & Human Rights Framework for Artificial Intelligence Governance' (2020) *Carr Center Discussion Paper* 9.

Milberg S, Smith H and Burke S 'Information Privacy: Corporate Management and National Regulation' (2000) *Organization Science* 35.

Moreham N 'Privacy in Public Spaces' (2006) *The Cambridge Law Journal* 606.

Musila G 'The right to an effective remedy under the African Charter on Human and Peoples' Rights' (2006) *African Human Rights Law Journal* 442.

Neethling J 'The Concept Of Privacy In South African Law'(2005) *South African Law Journal* 18.

O'Callaghan L 'The Intersection between Data Protection and Competition Law: How To Incorporate Data Protection, as a Non-Economic Objective, into EU Competition Analysis' (2018) *Trinity College Law Review* 109.

Ohlhausen H and Okuliar A 'Competition, Consumer Protection, and the Right [Approach] to Privacy' (2015) *Antitrust Law Journal* 121.

Perninan B 'The Origin of Privacy as a Legal Value: A Reflection on Roman and English Law' (2012) *American Journal of Legal History* 183.

Philbeck T and Davis N 'The Fourth Industrial Revolution' (2019) *Journal of International Affairs* 17.

Posner R 'Privacy, Surveillance, and Law' (2008) *The University of Chicago Law Review* 245.

Rengel A 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace' (2014) *Groningen Journal of International Law* 2.

Richards N 'The Dangers of Surveillance' (2013) *Harvard Law Review* 1934.

Robinson G 'Data protection reform, passenger name record and telecommunications data retention: -Mass Surveillance Measures in the E. U. and the Need for a Comprehensive Legal Framework' (2012) *Critical Quarterly for Legislation and Law* 394.

Roos A 'Core principles of data protection law' (2006) *The Comparative and International Law Journal of Southern Africa* 103.

Roos A 'Privacy in the Facebook Era: A South African Legal Perspective' (2012) *South African Law Journal* 375.

Roos A 'Privacy in the Facebook Era: A South African Legal Perspective' (2012) *The South African Law Journal* 375.

Roth P 'Adequate Level of Data Protection in Third Countries Post-Schrems and under the General Data Protection Regulation' (2017) *Journal of Law, Information and Science* 49.

Rubenfeld, J 'The Right of Privacy' (1989) *Harvard Law Review* 737.

Rule J 'Toward Strong Privacy: Values, Markets, Mechanisms, And Institutions' (2004) *University of Toronto Law Journal* 183.

Sajo A, 'Independent Regulatory Authorities as Constitutional Actors: A Comparative Perspective' (2007) *Annales Universitatis Scientiarum Budapestinensis de Rolando Eotvos Nominatae* 5.

Schwartz P and Solove D 'Reconciling Personal Information in the United States and European Union' (2014) *California Law Review* 877.

Selinger E and Hartzog W 'Surveillance as Loss of Obscurity' (2015) *Washington and Lee Law Review* 1343.

Sircar N and Maleche A 'Assessing a Human Rights-Based Approach to HIV Testing and Partner Notification in Kenya: A Qualitative Study to Examine How Kenya's Policies and Practices Implement a Rights-Based Approach to Health' (2020) *Health and Human Rights Journal* 167.

Solove D 'A Taxonomy of Privacy' (2006) *University of Pennsylvania Law Review* 477.

Solove D 'Conceptualizing Privacy' (2002) *California Law Review* 1087.

Solove D 'Privacy Self-Management and the Consent Dilemma' (2013) *Harvard Law Review* 1880.

Solove D 'The Limitations of Privacy Rights' (2022) *George Washington University Law School, Legal Studies Research Paper Series 1.*

Solove D 'The Myth of the Privacy Paradox' (2021) *The George Washington Law Review* 1.

Steeves V and Piñero V 'Privacy and Police Powers: Situating the Reasonable Expectation of Privacy Test' (2008) *Canadian Journal of Criminology and Criminal Justice* 263.

Sun N 'Applying Siracusa: A Call for a General Comment on Public Health Emergencies' (2020) *Health and Human Rights* 387.

Szydlo M 'Case Law, Principles underlying independence of national data protection authorities: Commission v. Austria' (2013) *Common Market Law Review* 50.

Taylor-Sakyi K (2016) 'Big Data: Understanding Big Data' ArXiv 1.

Tschider C 'Meaningful Choice: A History of Consent and Alternatives to the Consent Myth' (2021) *North Carolina Journal of Law & Technology* 617.

Tschider C 'AI's Legitimate Interest: Towards A Public Benefit Privacy Model' (2021) *Houston Journal of Health Law & Policy* 125.

Ünver H 'Politics of Digital Surveillance, National Security and Privacy' (2018) *Centre for Economics and Foreign Policy Studies* 1.

Vidović M, 'Schrems V Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities'(2015) *Croatian Yearbook of European Law & Policy* 259.

Warren S. D. & Brandeis L. D. 'The Right to Privacy' (1890) *Harvard Law Review* 193.

Williams B, Brooks , and Shmargad Y 'How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications' (2018) *Journal of Information Policy* 78.

Woolman S 'South Africa's Aspirational Constitution and our Problems of Collective Action' (2016) *South African Journal on Human Rights* 156.

Woolman S 'Understanding South Africa's Aspirational Constitution as Scaffolding' (2016) *New York Law School Law Review* 283.

Zitzke E 'Decolonial Comparative Law: Thoughts from South Africa' (2022) *Rabel Journal of Comparative and International Private Law* 190.

Reports

Artificial intelligence and privacy, and children's privacy: Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci A/HRC/46/37

CIPESA "State of Internet Freedom in Africa 2021: Effects of State Surveillance on Democratic Participation in Africa" available at <SIFA 21 copy (cipesa.org)> last accessed 31st January 2022.

CIPIT "Data Protection in the Kenyan Banking Sector: A study of Publicly Available Data Policies of Commercial Banks operating in Kenya in Relation to a Set Data Protection Standard" (2021) < Data-Protection-in-the-Kenyan-Banking-Sector.pdf (strathmore.edu)> las accessed 8 September 2022.

CIPIT "Privacy and Data Protection Practices of Digital Lending Apps in Kenya" (2020) <https://cipit.strathmore.edu/privacy-and-data-protection-practices-of-digital-lending-apps-in-kenya-report/> last accessed 8 April 2021.

Communication Authority of Kenya "First Quarter Sector Statistics Report for the Financial Year 2020/2021 (July - September 2020)" - <https://ca.go.ke/wp-content/uploads/2020/12/Sector-Statistics-Report-Q1-2020-2021.pdf> last accessed 25 March 2021.

Communication Authority "Third Quarter Sector Statistics Report for The Financial Year 2021/2022"< Sector-Statistics-Report-Q3-2021-2022.pdf (ca.go.ke)> last accessed 27 June 2022.

UNCTAD "Data Protection and Privacy Legislation Worldwide" <Data Protection and Privacy Legislation Worldwide | UNCTAD> last accessed 6 September 2022.

Digital Future Society *Privacy First: A New Business Model for the Digital Era* (2020).

East African Community "Task Force on Cyberlaws published a Draft EAC Legal Framework for Cyberlaws" (2008) <http://repository.eac.int:8080/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?seq> last accessed 20 March 2021.

EDRi "How online ads discriminate: Unequal harms of online advertising in Europe" (2021)

European Digital Rights "How online ads discriminate: Unequal harms of online advertising in Europe" (2021) https://edri.org/wp-content/uploads/2021/06/EDRi_Discrimination_Online.pdf last accessed 26th July 2021.

Final Report of the Committee of Experts on Constitutional Review (2010).

Final Report of the Constitution of Kenya Review Commission (2005).

Forbrukerradet "Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy" (2018) available at < 2018-06-27-deceived-by-design-final.pdf (forbrukerradet.no)> 7 last accessed 23 March 2022.

KNBS "Kenya 2019 census report" <https://www.knbs.or.ke/?p=5621> last accessed 25 March 2021.

Kenya National Assembly "Official Hansard Record" < Kenya National Assembly Official Record (Hansard) - Google Books> last accessed 7th September 2022.

MoICT "Emerging Digital Technologies for Kenya - Exploration and Analysis" <http://www.ict.go.ke/blockchain.pdf> last accessed 3 April 2021.

Lekubu D 'Understanding 'Adequate Legal Protection' As A Requirement For Transborder Information Flows From South Africa' (2022) LLM Report: University of the Witwatersrand.

Marczak B, Scott-Railton J, McKune S, Razzak B, and Deibert R 'HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries' (2018).

Marczak B, Scott-Railton J, Rao S, Anstis S, and Deibert R 'Running in Circles Uncovering the Clients of Cyberespionage Firm Circles'(2020).

OECD *Data-Driven Innovation: Big Data for Growth and Well-Being* (2015).

Privacy International "Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya" https://www.privacyinternation al.org/sites/default/files/2017-10/track_capture_final.pdf last accessed 1 April 2021.

Safaricom "Annual Report 2021" available at < Safaricom at a glance – Safaricom> last accessed 17 March 2022.

Slaughter R, Kopec J, and Batal M 'Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission (2021) *ISP Digital Future Whitepaper* & *Yale Journal of Law and Technology Special Publication*.

*The EU Digital Markets Act: A Report from a Panel of Economic Exper*ts (2021)

The Panel for the Future of Science and Technology of the European Parliament 'A Governance framework for algorithmic accountability and transparency' (2019).

UK Information Commissioner's Office "Investigation into the use of data analytics in political campaigns: A report to Parliament" (2018) < https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf> last accessed 1 April 2021.

UN Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" 17 April 2013, A/HRC/23/40, available at: https://www.refworld.org/docid/51a5ca5f4.html last accessed 23 July 2022

Policy and working papers

African Union *African Union Data Policy Framework* (2022).

Article 29 Data Protection Working Party *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* Adopted on 9 April 2014 25.

CETS "Explanatory Report of Convention 108 as modified by the amending Protocol". Council of Europe Treaty Series - No. 22 < CETS 223 - Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (coe.int)>

EU "GDPR Recitals" available at <Recital 47 - Overriding Legitimate Interest - General Data Protection Regulation (GDPR) (gdpr-info.eu)> last accessed 22 September 2022.

Necessary and Proportionate "International Principles on the Application of Human Rights to Communications Surveillance" (2014) < EN Princples (necessaryandproportionate.org)> last accessed 1 April 2021.

Office of the UN High Commissioner for Human Rights (OHCHR), 'The Right to Privacy in the Digital Age. Report of the United Nations High Commissioner for Human Rights' (30 June 2014) UN Doc A/HRC/27/37 47 ('A/HRC/27/37').

The Panel for the Future of Science and Technology of the European Parliament 'A governance framework for algorithmic accountability and transparency' (2019).

UN Commission on Human Rights, "The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights", 28 September 1984, E/CN.4/1985/4, available at: https://www.refworld.org/docid/4672bc122.html last accessed 27 January 2022.

Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Working Document Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive Adopted by the Working Party on 24 July 1998

Legal instruments

Kenya

Births and Deaths Registration Act, Cap 149 Laws of Kenya.

Central Bank of Kenya (Amendment) Act, 2021.

Central Bank of Kenya Prudential Guidelines January 2013.

Children Act, 2022, No. 29 of 2022.

Citizenship and Immigration Act, No. 12 of 2011.

Civil Procedure Act, Cap 21 Laws of Kenya.

Computer Misuse and Cybercrimes Act, No. 5 of 2018.

Constitution of Kenya, 2010.

Constitutional (Amendment) Bill 2020.

Consumer Protection Act, No. 46 of 2012.

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

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

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

Data Protection Act, 2019.

Elections (Registration of Voters) Regulations, 2012, L.N. 126/2012, L.N. 73/2017.

Elections Act, No. 4 of 2011

Health Act No. 21 of 2017.

HIV AIDS and Control Act, 2003.

Kenya Citizenship and Immigration Act No 12 of 2011.

Kenya Defence Forces Act, No. 25 of 2012.

Kenya Information and Communication Act (KICA) Cap 411A of the Laws of Kenya

Kenya Information and Communications (Registration of Subscribers of Telecommunications Services) Regulations, 2014.

Kenya Information and Communications Act (Registration of SIM cards) Regulations, 2015
Kenya Revenue Authority Act, No. 2 of 1995.

Law Society of Kenya *Code of Standards of Professional Practice and Ethical Conduct* (June 2016)

Media Council Act, No. 46 of 2013.

National Intelligence Service Act, No. 28 of 2012.

National Police Service Act, Cap 84 Laws of Kenya.

ODPC "Alternative Dispute Resolution Framework & Guidelines" <Alternative Dispute Resolution Framework (ADR) – OFFICE OF THE DATA PROTECTION COMMISSIONER KENYA (odpc.go.ke)> las accessed 20 December 2022.

Penal Code, Cap. 63 Laws of Kenya.

Prevention of Terrorism Act, No. 30 2012

Private Security Regulation Act, No. 13 of 2016.

Proceeds of Crime and Anti-Money Laundering Act, No. 9 of 2009.

Refugees Act, No. 13 of 2006.

Registration of Persons Act Cap 107 Laws of Kenya.

Statistics Act Cap 112

European Union

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.

Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, 28 January 1981, ETS 108.

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal

offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

EU "Artificial Intelligence Act" Brussels, 21.4.2021, COM(2021) 206 final. 2021/0106(COD) available at < EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu)> last accessed 17 August 2022.

European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)

South Africa

Constitution, Act 108 of 1996.

Protection of Personal Information Act (POPIA) No. 4 of 2013.

Regulation of Interception of Communications and Provision of Communication-related information Act regulated communication surveillance, No. 70 of 2002.

International Instruments

African Union Convention on Cyber Security and Personal Data Protection, Adopted by the Twenty-Third Ordinary Session of the Assembly, Held in Malabo, Equatorial Guinea, 27th June 2014.

Convention on the Rights of Persons with Disabilities of 13 December 2006: U.N. Doc. A/RES/61/106.

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

Organization of African Unity (OAU), African Charter on Human and Peoples' Rights ("Banjul Charter"), 27 June 1981, CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982)

Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR).

Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3 (CRC).

Case law

Kenya

Aids Law Project v Attorney General & 3 others [2015] eKLR.

Association of Kenya Insurers (AKI) Suing through its Chairman Mr. Mathew Koech) v Kenya Revenue Authority & 2 others; Insurance Regulatory Authority (IRA) & another (Interested parties) (Petition 201 of 2020) [2021] KEHC 402 (KLR).

Attorney-General & 2 others v Ndii & 79 others; Prof. Rosalind Dixon & 7 others (Amici curiae) (Petition 12, 11 & 13 of 2021 (Consolidated)) [2022] KESC 8 (KLR).

C.O.M. v Standard Group Limited & another [2013] eKLR.

Communications Authority of Kenya v Okiya Omtata Okoiti & 8 others [2020] eKLR.

Cyprian Andama v Director of Public Prosecution & another; Article 19 East Africa (Interested Party) [2019] eKLR.

David Lawrence Kigera Gichuki v Aga Khan University Hospital [2014] eKLR.

David Ndii & others v Attorney General & others [2021] eKLR.

EG & 7 others v Attorney General; DKM & 9 others (Interested Parties); Katiba Institute & another (Amicus Curiae) [2019] eKLR.

Geoffrey Andare v Attorney General & 2 others [2016] eKLR.

Heiwua Auto Kenya Limited &3 Others V The Office Commanding Police Division Central Police Station & 3 Others[2010] eKLR.

Independent Electoral and Boundaries Commission & 4 others v David Ndii & 82 others; Kenya Human Rights Commission & 4 others (Amicus Curiae) [2021] eKLR.

J L N & 2 others v Director of Children Services & 4 others [2014] eKLR

Jacqueline Okuta & another v Attorney General & 2 others [2017] eKLR

James Opiyo Wandayi v Kenya National Assembly & 2 others [2016] eKLR

Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre & 2 others [2017] eKLR

JK v AAR Healthcare Kenya Ltd [2020] eKLR.

Katiba Institute & another vs. Attorney General & another [2017] eKLR.

Katiba Institute v Attorney General & 3 others; Kenya National Commission on Human Rights (Interested Party) [2019] eKLR.

Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 Others v Cabinet Secretary Ministry of Health & 4 Others [2016] EKLR.

Kenya Plantation and Agricultural Workers Union V James Finlay (K) Limited [2013] eKLR.

Mwangi & another v Naivasha County Hotel t/a Sawela Lodges (Petition E003 of 2021) [2022] KEHC 10975 (KLR) (19 July 2022) (Ruling).

N W R & another v Green Sports Africa Ltd & 4 others [2017] eKLR.

*Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (*Interested Parties) [2020] eKLR.

Okiya Omtatah Okoiti V Communication Authority of Kenya & 8 Others [2018] EKLR.

PAK & another v Attorney General & 3 others (Constitutional Petition E009 of 2020) [2022] KEHC 262 (KLR)

Republic v Firearms Licensing Board & another Ex parte Boniface Mwaura [2019] eKLR 50.

Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another (Exparte); Immaculate Kasait, Data Commissioner (Interested Party) (Judicial Review Application E1138 of 2020) [2021] KEHC 122 (KLR) (Judicial Review) (14 October 2021) (Judgment)

Roshanara Ebrahim v Ashleys Kenya Limited & 3 others [2016] eKLR.

Samura Engineering Limited & 10 others v Kenya Revenue Authority [2012] eKLR.

SKM v C. B. M & 3 others [2021] eKLR.

Standard Newspapers Limited & another v Attorney General & 4 others [2013] eKLR.

William Musembi and others v Moi Educational Centre Company Ltd and others SC Petition No.2 of 2018.

European Union

Big Brother Watch and Others V. The United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15)

Case of Von Hannover V. Germany (No. 2) (Applications nos. 40660/08 and 60641/08)

Digital Rights v. Ireland [2014] ECLI:EU:C:2014:238

European Commission v Hungary [2014] (Case C-288/12) ECLI:EU:C:2014:237, 51.

European Data Protection Supervisor (EDPS) v Republic of Austria [2012] (Case C-614/10) ECLI:EU:C:2012:631,37

Google and Alphabet v Commission Case T-612/17.

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González JUDGMENT OF 13. 5. 2014 — CASE C-131/12, 53.

H. K. v Prokuratuur Case C-746/18.

Maximillian Schrems v Data Protection Commissioner Case [2015] (Case C-362/14) ECLI:EU:C:2015:650.

Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA "Rīgas satiksme" Case C-13/16.

South Africa

AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others (CCT 278/19; CCT 279/19) [2021] ZACC 3 (4 February 2021).

Fose v Minister of Safety and Security (CCT14/96) [1997] ZACC 6; 1997 (7) BCLR 851; 1997 (3) SA 786 (5 June 1997) 69.

Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others (CCT1/00) [2000] ZACC 12; 2000 (10) BCLR 1079; 2001 (1) SA 545 (CC) (25 August 2000) 18.

Mistry v Interim National Medical and Dental Council of South Africa and Others (CCT13/97) [1998] ZACC 10; 1998 (4) SA 1127; 1998 (7) BCLR 880 (29 May 1998) 27.

S v Makwanyane and Another (CCT3/94) [1995] ZACC 3; 1995 (6) BCLR 665; 1995 (3) SA 391; [1996] 2 CHRLD 164; 1995 (2) SACR 1 (6 June 1995)

Other

Campbell v MGN Limited [2004] UKHL 22.

Katz v. United States 389 U.S. 347 (more) 88 S. Ct. 507; 19 L. Ed. 2d 576; 1967 U.S. LEXIS 2

R (Daly) vs. Secretary of State for Home Department (2001) 2 AC 532.

R v Oakes [1986] 1 SCR 103

Sir Dawda K Jawara v The Gambia Communication No. 147/95, 149/96 32.

U.S.A v Jones 132 S. Ct. 945 (2012).

Internet sources

Aaronson S "Inadequate data protection: A threat to economic and national security"'(2020) available at < Inadequate data protection: A threat to economic and national security | CEPR> last accessed 4 October 2022.

African Union "list of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection" < 29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf (au.int)> last accessed 6 September 2022.

Akinyi A "Laws, Policies and the Right to Privacy for People Living with HIV in Kenya" (2019) available at < Laws, Policies and the Right to Privacy for People living with HIV in Kenya (uonbi.ac.ke)> last accessed 9 March 2022

Bounie D, Dubus A, and Waelbroeck P "Selling Strategic Information in Digital Competitive Markets" (2018) available at < david bouie_ antoine dubus_patrick waelbroeck.pdf (europa.eu)> 2 last accessed 24 March 2022.

Brignull H, "What are dark patterns?" Available at < Dark Patterns> last accessed 22 March 2022

E Felten "What does it mean to ask for an "explainable" algorithm?" (2017) < What does it mean to ask for an "explainable" algorithm? (freedom-to-tinker.com)> last accessed 22 March 2022

European Commission "Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising" (2019) < https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770> last accessed 29 July 2022.

European Commission "Adequacy Decisions" Adequacy decisions | European Commission (europa.eu) last accessed 18 August 2022.

European Data Protection Board "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)" < edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf (europa.eu)> last accessed 21 December 2022.

Federal Trade Commission "FTC Sues Facebook for Illegal Monopolization Agency challenges Facebook's multi-year course of unlawful conduct" (2020) < https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization> last accessed 29 July 2022.

Muigai G "Constitutional amendments and the constitutional Amendment process in Kenya (1964-1997) a study in the politics of the constitution" (2001) available at <Constitutional amendments and the constitutional Amendment process in Kenya (1964-1997) a study in the politics of the constitution (uonbi.ac.ke)> last accessed 7 March 2022

Muigua K "Court Sanctioned Mediation in Kenya-An Appraisal" (2015) available at <kmco.co.ke/wp-content/uploads/2018/08/Court-Sanctioned-Mediation-in-Kenya-An-Appraisal-By-Kariuki-Muigua.pdf> last accessed 5th May 2022

OHCHR "Status Ratification" < https://indicators.ohchr.org/> last accessed 21 March 2022.

Pillai A and Kohli R "A Case for a Customary Right to Privacy of an Individual: A Comparative Study on Indian and other State Practice" (2017) Oxford University Comparative Law Forum < https://ouclf.law.ox.ac.uk/a-case-for-a-customary-right-to-privacy-of-an-individual-a-comparative-study-on-indian-and-other-state-

practice/#C_Data_Privacy_as_an_emerging_norm_of_customary_international_law> last accessed 23 July 2022.

Raso F, Hilligoss H, Krishnamurthy V, Bavitz C, and Kim L "Artificial Intelligence & Human Rights Opportunities & Risks" (2018) *The Berkman Klein Center for Internet & Society Research Publication Series* available at https://cyber.harvard.edu/publication/2018/artificial-intelligence-human-rights last accessed 18 March 2022

United States Federal Trade Commission "Data Brokers: A Call for Transparency and Accountability" (2014) available at < Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission (May 2014) (ftc.gov)> 11 – 18 last accessed 24 March 2022.

Wheeler C "The Public Interest We Know It's Important, But Do We Know What It Means" AIAL FORUM No. 48. Available at < 2.pdf (austlii.edu.au)> last accessed 27 August 2022.

Press reports

Auchard E "Cambridge Analytica stage-managed Kenyan president's campaigns: UK TV" < https://www.reuters.com/article/us-facebook-cambridge-analytica-kenya-idUSKBN1GV300>.
BBC "Cambridge Analytica's Kenya election role 'must be investigated'" < https://www.bbc.com/news/world-africa-43471707> last accessed 23 March 2021.

Capital FM "Data Protection Office Probing 40 Digital Lenders Over Misuse Of Personal Data" <Data protection office probing 40 digital lenders over misuse of personal data - Capital Business (capitalfm.co.ke)> last accessed 14 December 2022.

Madowo L, "How Cambridge Analytica poisoned Kenya's democracy" (2018) < https://www.washingtonpost.com/news/global-opinions/wp/2018/03/20/how-cambridge-analytica-poisoned-kenyas-democracy/> last accessed 23 March 2021.

Nyabola N "Politics in the digital age: Cambridge Analytica in Kenya" < https://www.aljazeera.com/opinions/2018/3/22/politics-in-the-digital-age-cambridge-analytica-in-kenya> last accessed 23 March 2021.

Quantum Bog "Top 3 Reasons Why Metadata Is "The New Bacon"" (2017) https://blog.quantum.com/2017/08/15/top-3-reasons-why-metadata-is-the-new-bacon/ last accessed 29th July 2022.

The Star "Cambridge Analytica confirms involvement in Kenyan elections" < https://www.the-star.co.ke/news/2018-03-20-cambridge-analytica-confirms-involvement-in-kenyan-elections/> last accessed 23 March 2021.

The Star "Kenyans protest registration as party members without consent" < Kenyans protest registration as party members without consent (the-star.co.ke)> last accessed 20 June 2022.

Wall Street Journal "How Big Tech Got Even Bigger: Technology giants such as Alphabet, Amazon and Apple are more dominant than a year ago thanks to a greater reliance on their services during the pandemic. The forces propelling them to new heights are expected to outlast Covid-19." (6th February 2021) <https://www.wsj.com/articles/how-big-tech-got-even-bigger-11612587632>press last accessed 29th July 2022.