Global Campus Africa

Awarded Theses 2018/2019

Chisomo Nyemba

Right to Data Privacy in the Digital Era

Critical Assessment of Malawi's Data Privacy Protection Regime

HRDA, The Master's Programme in Human Rights and Democratisation in Africa

CHISOMO NYEMBA

RIGHT TO DATA PRIVACY IN THE DIGITAL ERA: A CRITICAL ASSESSMENT OF MALAWI'S DATA PRIVACY PROTECTION REGIME

FOREWORD

The Global Campus of Human Rights is a unique network of more than one hundred participating universities around the world, seeking to advance human rights and democracy through regional and global cooperation for education and research. This global network is promoted through seven Regional Programmes which are based in Venice for Europe, in Sarajevo/Bologna for South East Europe, in Yerevan for the Caucasus, in Pretoria for Africa, in Bangkok for Asia-Pacific, in Buenos Aires for Latin America and the Caribbean, and in Beirut for the Arab World.

Every year each regional master's programmes select the best master thesis of the previous academic year that is published online as part of the GC publications. The selected seven GC master theses cover a range of different international human rights topics and challenges.

The Global Campus Awarded Theses of the academic year 2018/2019 are:

• Begalieva, Nuriza, *From Democracy to Autocracy? Growing Threats to Civil Society and Media in Kyrgyzstan*, Supervisor: Arusyak Aleksanyan, Yerevan State University. Master's Programme in Human Rights and Democratisation in the Caucasus (CES), coordinated by Yerevan State University.

• El-Hawary, Nouran *Refugees ad Migrant Access to Health in Transit Countries: Politics of Adaptability, Enactment of Slow Death and Inevitability of Pain: an Ethnography of Poor Urban Neighborhood in Rabat (Morocco),* Supervisor: Jeremy Gunn, International University of Rabat (UIR). Arab Master's Programme in Democracy and Human Rights (ARMA), coordinated by Saint Joseph University (Lebanon).

• Ferizović, Jasenka *Prosecution of Crimes of Appropriation of Private Property before the ICTY and the IRMCT*, Supervisor: Hans-Joachim Heintze, Ruhr Unversity Bochum. European Regional Master's Programme in Democracy and Human Rights in South East Europe (ERMA), coordinated by University of Sarajevo and University of Bologna

• Frías Sampaio, Emmanuel, *Politics of Memory of the Recent Past in Brazil: The Federal Government's Role in Constructing Collective Memory Between 2003 and 2016,* Supervisor. Ana De Maio, University of Buenos Aires. Master's Programme in Human Rights and Democratisation in Latin American and the Caribbean (LATMA), coordinated by National University of San Martin (Argentina)

• Guzmán Torán, Juan José, *When the Forest Screams. The Rights of Nature and Indigenous Rights as a Mutually Reinforcing Resistance Platform for the Indigenous Peoples of the Ecuadorian Amazon*, Supervisor: Felipe Gómez Isa, University of Deusto Bilbao. European Master's Programme in Human Rights and Democratisation (EMA), coordinated by Global Campus of Human Rights Headquarters.

• Hasanah, Mahesti *Between the Domination of Transnational Companies and Its Discourse on Business and Human Rights: Contract Farming and Banana Small Farmers in the Davao Region (The Philippines)*, Supervisor: Ryan Jeremiah D. Quan, Manila University. Master's Programme in Human Rights and Democratisation in Asia Pacific (APMA), coordinated by Mahidol University.

• Nyemba, Chisomo *Right to Data Privacy in the Digital Era: a Critical Assessment of Malawi's Data Privacy Protection Regime,* Supervisor: Akinola E Akintayo, University of Lagos. Master's Programme in Human Rights and Democratisation in Africa (HRDA), coordinated by Centre for Human Rights, University of Pretoria.

This publication includes the thesis *Right to Data Privacy in the Digital Era: a Critical Assessment of Malawi's Data Privacy Protection Regime* written by Chisomo Nyemba and supervised by Akinola E Akintayo, University of Lagos.

BIOGRAPHY

Chisomo Nyemba was born and raised in Malawi. She is a legal practitioner. She obtained a Bachelor of Laws (Honours) Degree from the University of Malawi in 2014 and a master's degree in Human Rights and Democratisation from the University of Pretoria in South Africa in 2019. In all her endeavors, Chisomo is largely driven by a desire to make a difference for those who are less privileged. Further, she believes in using the law as a tool for bringing positive and lasting change.

ABSTRACT

The proliferation of information communication technology (ICT) and consequent increase in the processing of personal data threaten the right to data privacy and related human rights. Although Malawi has comparatively been slow in ICT growth and usage, personal data is now being collected and processed at an unprecedented scale. The processing of personal data is likely to increase as the ICT infrastructure grows and technology becomes more sophisticated. This paper examines whether the right to data privacy, particularly of vulnerable people, is adequately and effectively protected in the digital era in the context of Malawi, a developing country currently classified as one of the poorest countries in the world. This paper demonstrates how the risks of infringement of data privacy may be heightened for the poor and vulnerable. Further, the poor and the vulnerable may not be able to avert or mitigate against adverse consequences in case of infringements of the right to data privacy. Therefore, the paper argues that, despite having laws under which the right to data privacy can be protected, the laws are inadequate and ineffective in view of the threats posed by ICT and prevalent vulnerabilities in Malawi. The paper recommends the promulgation of a more robust, comprehensive and effective data privacy protection law that adequately takes into account the vulnerabilities in Malawi.

ACKNOWLEDGEMENTS

Completing this thesis has been possible because of the assistance from various people and organisations. I am deeply grateful to the Centre for Human Rights, University of Pretoria, and its dedicated team for making the LLM journey worthwhile and transformative. I also sincerely appreciate the European Union for the financial assistance that enabled me to pursue the LLM.

My profound gratitude to my supervisor, Dr Akinola Akintayo, for providing guidance, timely feedback and for stretching my intellectual abilities. I am very grateful for the excellent supervision. I am also thankful to the University of Lagos, Faculty of Law, for ensuring that I had a conducive environment for my research.

To my mom, dad, siblings and family, thank you for always encouraging and supporting me to pursue my dreams.

Thank you to all my friends, classmates, colleagues and everyone who has supported me throughout my studies. May God's grace abound in your lives.

TABLE OF ABBREVIATIONS

AIA	Access to Information Act
AU	African Union
CCTV	Closed-circuit television
CERT	Computer Emergency Response Team
ET Act	Electronic Transactions and Cyber Security Act
EU Charter	Charter of Fundamental Rights of the European Union
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information communication technology
MACRA	Malawi Communications and Regulatory Authority
MalTIS	Malawi Traffic Information System
NSA	National Statistics Act
PPIA	Protection of Personal Information Act
SALRC	South Africa Law Review Commission
USA	United States of America

TABLE OF CONTENTS

1.

INTRODUCTION

1.1 Background

There is an exponential growth in the collection of personal data facilitated by information and communication technologies (ICTs) which inevitably threaten privacy and sanctity of personal data. In view of the threats, a human right to control the processing of personal data and to safeguard the interests of the person to whom the information pertains (the data subject) has emerged which is referred to as the right to data privacy.[1] Personal data is generally information in respect of or about an individual.[2] The data or information does not have to be secret or private.[3] Although personal data collection by private entities and the government is not new,[4] technology imperils data privacy more. This is because technology helps in the collection of more data with relative ease, facilitates storage of huge amounts of data and makes it easier to alter and transfer data at the click of a button.[5] Furthermore, breaches and violations can occur subtly, without the data subject's knowledge or consent.[6]

[1] The term 'right to data privacy' is preferred to 'right to data protection' in this study. However, the terms are used interchangeably in various works and laws so the term 'data protection' may be employed in this study when quoting laws or literature that use that terminology. On why the term data privacy is preferred see Lee Andrew Bygrave, 'Privacy and Data Protection in an International Perspective' (2010) 56 Scandinavian Studies in Law 166, 168.

[2] Maria Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? "Reconstructing" a Not So New Right' (2013) 3 International Data Privacy Law 88, 89.

[3] Lukman Adebisi Abdulrauf, 'The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa' (LLD thesis, University Of Pretoria 2015) 21.

[4] Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and United States* (Cornell UP 1992) 18.

[5] Alex Boniface Makulilo (ed), *African Data Privacy Laws* (Springer 2016) 3.

[6] Rachel K Zimmerman, 'The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century' (2000) 4 Journal of Legislation and Public Policy 439, 441.

Therefore, unregulated data processing can facilitate human rights violations, including infringement of the rights to privacy, dignity, security of person, discrimination and property.[7] Personal data is increasingly being used for identity theft,[8] phishing scams,[9] fraud,[10] money theft,[11] harassment and stalking of people.[12] Personal data can also be used to target people leading to massive human rights violations.[13] The genocide in Rwanda where thousands of Tutsi were killed based on their identification cards which indicated the holder's tribe is a case in point.[14] Thus, the need for laws to protect personal data in this technological era cannot be overemphasised. Although personal data protection developed in Western countries, developing countries including Malawi now have personal data privacy concerns because of the proliferation of ICT.[15]

[7] Giovanni Sartor, 'Human Rights in the Information Society: Utopias, Dystopias and Human Values' in Mario Viola de Azevedo Cunha and others, *New Technologies and Human Rights: Challenges to Regulation* (1st edn, Ashgate Publishing Limited 2013) 14-24; Pedro Ferreira, 'Angels and Demons: Data Protection and Security in Electronic Communications' in Mario Viola de Azevedo Cunha and others, *New Technologies and Human Rights: Challenges to Regulation* (1st edn, Ashgate Publishing Limited 2013) 203-216.

[8] See generally Esma Aimeur and David Schonfeld, 'The Ultimate Invasion of Privacy: Identity Theft' (Ninth Annual International Conference on Privacy, Security and Trust 2011) <www.site.uottawa.ca/~nelkadri/CSI5389/Papers/8-Aimeur_and_Schonfeld_PST2011.pdf> accessed 1 September 2019.

[9] The Tunisian government used phishing scripts to get personal information and passwords of users on Twitter, Facebook, Gmail and Yahoo in order to spy on private communications and delete unfavourable posts. See Alex Comninos, 'Twitter Revolutions and Cyber Crackdowns: User-Generated Content and Social Networking in the Arab Spring and Beyond' (Association for Progressive Communications (APC) June 2011) <www.apc.org/sites/default/files/AlexComninos_MobileInternet.pdf> accessed 1 September 2019 10.

[10] Mark Button and Cassandra Cross, *Cyber Frauds, Scams, and Their Victims* (Routledge 2017) 43-45.

[11] ibid.

[12] Shandre Sissing and Johan Prinsloo, 'Contextualising the Phenomenon of Cyber Stalking and Protection from Harassment in South Africa' (2013) 2 Acta Criminologica: Southern Africa Journal of Criminology 15, 19-20.

[13] For example, China is using technology to monitor, control and target people. See Xiao Qiang, '"Dataveillance" in Xi Jinping's "Brave New China"' (*Power3.0*, 26 April 2018) <www.power3point0.org/2018/04/26/dataveillance-in-xi-jinpings-brave-new-china/> accessed 1 September 2019; Steven Feldstein, 'The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression' (2019) 30 Journal of Democracy 40, 45.

[14] *Prosecutor v Jean-Paul Akayesu* Case ICTR-96-4-T (International Criminal Tribunal for Rwanda) [123].

[15] See generally James Wiley, 'The Globalisation of Technology to Developing Countries' (*Digital Commons*, 4 August 2009) <http://digitalcommons.providence.edu/glbstudy_students/3> accessed 18 August 2019; Jimmy Kainja, 'Privacy and Personal Data Protection: Challenges and Trends in Malawi' (CIPESA September 2018) <https://cipesa.org/?wpfb_dl=300> accessed 20 August 2019 13-15.

This thesis analyses whether the extant data privacy protection framework in Malawi adequately and effectively protects the right to data privacy in view of ICT-facilitated threats. The analysis focuses on the right to data privacy of the poor and vulnerable based on the hypothesis that socioeconomic vulnerabilities heighten the risks for and violations of the right. Vulnerability can result from a person's 'natural characteristics' or as a 'result of marginalization and stigmatization'.[16] Vulnerable people are more susceptible to a decline in wellbeing or harm when society experiences shocks or disruptions.[17] I identify the following vulnerabilities as increasing risks to data privacy in Malawi: poverty, illiteracy, digital illiteracy, lack of education, gender and disability.

At the outset, it is important to explain the nexus between the right to data privacy and the traditional right to privacy. One view is that data privacy is a subcategory of the right to privacy.[18] Another view is that the right to data privacy protects distinct and broader interests than the right to privacy by generally regulating processing of personal data even when it is willingly disclosed and is not private.[19] I agree with the latter view as data privacy goes beyond protecting traditional interests of privacy. This paper thus approaches data privacy as a self-standing right which is closely related to the right to privacy but protects broader interests. However, it refers to the right to data privacy as a subset of privacy when quoting literature or laws that regard it as such.

1.2 Research problem

The government and private entities in Malawi are increasingly using ICT to collect and process personal data thereby threatening the right to data privacy.[20] Notwithstanding the threats, data privacy protection

[16] Siri Gloppen and Fidelis Edge Kanyongolo, 'Courts and the Poor in Malawi: Economic Marginalization, Vulnerability, and the Law' (2007) 5 International Journal of Constitutional Law 258, 261.

[17] ibid.

[18] Daniel Solove, '"I've Got Nothing To Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745, 754; Roger Clarke, 'Introduction to Dataveillance and Information Privacy, Definition of Terms' (*Roger Clarke*, 24 July 2016) <www.rogerclarke.com/DV/Intro.html#InfoPriv> accessed 14 October 2019; Kainja (n 15) 8.

[19] Orla Lynskey, 'Deconstructing Data Protection: The "Added Value" of a Right to Data Protection in the EU Legal Order' (2014) 63(3) International and Comparative Law Quarterly 569, 579.

[20] Kainja (n 15) 13-15.

has not received much attention from scholars and law makers in Malawi. Further, data subjects do not really understand the importance of personal data protection.[21] As such, there is a high risk of violations of the right to data privacy in Malawi. The risks may be heightened because of prevalent poverty, wealth and education inequalities, predominant digital illiteracy, gender disparities and inadequate protection of persons with disabilities. The increased use of ICT in processing personal data in Malawi and the rate at which they are becoming more sophisticated necessitates an examination of whether the legal framework adequately and effectively protects people's data privacy rights. Consequently, this study assesses the adequacy and efficacy of data privacy laws with due regard to contexts and vulnerabilities in Malawi. Such an assessment will help in the formulation of a robust data privacy legal regime suitable in the contexts of Malawi.

1.3 Research questions

The main research question addressed by this study is: Having regard to the contexts within which ICT utilisation and data processing activities are taking place in Malawi, is the legal framework for protecting data privacy rights adequate and effective?

The following sub-questions will help answer the main question:

a. What theories underpin and explain the interplay between law and technology, and their impact in society, particularly on vulnerable people?

b. What is the scope and extent of data privacy protection offered by Malawi's extant legal framework?

c. Having regard to the peculiar contexts of ICTs and data processing operationalisations in Malawi, is the current legal framework adequate and effective to protect data privacy rights, especially of the poor and vulnerable?

d. What lessons can Malawi learn from comparative foreign laws to bolster its data privacy protection regime?

[21] Kainja (n 15) 30.

1.4 Methodology

This study employs a desk-based research methodology. Primary sources relied on include human rights and data privacy protection instruments, acts, bills and case law. The study also uses secondary sources including books, journal articles, reports by the government and nongovernmental organisations, conference papers, commentaries and dissertations. In addition, comparative legal research is conducted in order to draw lessons from foreign jurisdictions on data privacy protection to guide necessary law reforms in Malawi.

1.5 Literature review

Personal data protection has attracted the interest of scholars, policy makers and law makers in many countries. Concerns relating to misuse of personal data facilitated by computerised systems were initially raised and documented in the 1960s and 1970s, and authoritative texts on the subject were written by Westin and Miller.[22] They both approached personal data protection as a right to information privacy. Shortly thereafter, Rule examined in detail how personal data was being collected and processed and the adverse effect it had on people.[23] The concerns led to the promulgation of data protection laws and regulations in the United States of America (USA) and Europe from the 1970s onwards.[24] However, as noted by Makulilo, data privacy protection has been largely overlooked and literature on the subject is underdeveloped in Africa despite the increase in personal data processing facilitated by ICT.[25] Nonetheless, some literature is available on Africa in general and Malawi is surveyed below.

Literature examined here is grouped into three categories. The first category discusses the challenges to data privacy resulting from

[22] Alan Westin, *Privacy and Freedom* (Bodley Head 1970); Arthur Miller, *The Assault on* Privacy: *Computers, Data Banks and Dossiers* (UMP 1971) discussed in Bygrave (n 1) 167.

[23] James Rule, *Private Lives and Public Surveillance (*1973) quoted in Adam Warren, James Dearnley and Charles Oppenheim, 'Sources of Literature on Data Protection and Human Rights' (2001) 2 Journal of Information, Law and Technology 1, 3.

[24] ibid.

[25] Alex Boniface Makulilo, 'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) International Data Privacy Law 163, 176.

the increased use of ICTs by government and private entities. As Banisar noted, there is an increase in the use of ICTs in Africa and this raises data privacy concerns.[26] He cited various technologies as raising concerns, including identification cards systems which collect personal information with no guarantee of safety. He also expressed concerns about the emergence of DNA databases, biometric systems, body scanners, advanced communications technologies, advanced technologies owned by governments for intercepting communications and collection of information of users of various services including SIM card holders.[27] He reported that there is a rise in fraud and identity theft as a result of inadequate security of databases. In addition to the challenges identified above, Fombad and Abdulrauf assert that data privacy is being threatened in Africa by internet activities.[28] The preceding literature is however generalised and not specific to the challenges in Malawi.

The second category of literature examines the state of data privacy laws. As recently as 2004, Bygrave stated that there was no country in Africa with omnibus legislation on data privacy.[29] However, there has been a significant change since then. As pointed out by Greenleaf, 25 African countries currently have data privacy legislation as at January 2019.[30] Malawi is listed as one of the countries with legislation on data privacy and the Electronic Transactions and Cyber Security Act (the ET Act) enacted in 2016 is specified as the primary law.[31] The adequacy of the ET Act to protect data privacy is not assessed by Greenleaf. Kainja also acknowledged the existence of legislation in Malawi providing for some

[26] David Banisar, 'Linking ICTs, the Right to Privacy, Freedom of Expression and Access to Information' (2010) 16 East African Journal of Peace & Human Rights 124.

[27] Also see Chikaodili Juliet Hemeson, 'Directive on Consumer Data for SIM Card Registration in the Telecommunications Sector: An African Perspective' (*SSRN*, 8 January 2012) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1982033> accessed 19 August 2019 7-8.

[28] Charles Manga Fombad and Lukman Adebisi Abdulrauf, 'The African Union's Data Protection Convention 2014: A Possible Cause for Celebration in Human Rights in Africa?' (2016) 8 Journal of Media Law 67, 69-72.

[29] Lee Bygrave, 'Privacy Protection in a Global Context: A Comparative Overview' (2004) 47 Scandinavian Studies in Law 320, 343.

[30] Graham Greenleaf, 'Global Data Privacy Laws 2019: 132 National Laws and Many Bills' (2019) 157 Privacy Laws & Business International Report <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593> accessed 22 August 2019; Graham Greenleaf, 'Global Tables of Data Privacy Laws and Bills' (2019) Supplement to 157 Privacy Laws & Business International Report <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3380794> accessed 22 August 2019.

[31] Greenleaf, 'Global Tables of Data Privacy Laws and Bills' ibid 9.

aspects of data privacy protection, namely the ET Act, Communications Act, Access to Information Act (the AIA) and the National Statistics Act (the NSA).[32] However, Kainja argued that the laws are inadequate.[33] Kainja's analysis on the inadequacy of the existing laws is very brief. He implores academics to engage with and write more on the subject. This study has taken up the challenge and undertakes an in-depth analysis of the adequacy and effectiveness of the current legal regime vis-à-vis the workings of ICT in contexts of Malawi with a view to assessing the limitations of the current regime and proposing appropriate reform of the laws.

The third category of literature is on formulating effective and adequate legal protection of the right to data privacy in Malawi. Kainja suggests that a comprehensive law on data privacy protection must be enacted in Malawi but he does not offer guidance on the contents of the law.[34] Further, Kainja does not take into account vulnerable people in proposing how effective data protection can be achieved. Both the text of the law and the context within which the law operates must be considered for effective data privacy protection. The context matters as argued by Dominique who for example, expresses doubt that constitutional reforms in Chad can lead to constitutionalism in contexts of domination by the president and his party.[35] This study examines the contexts within which personal data is being processed in Malawi in order to devise context sensitive proposals on data privacy protection. The study also draws lessons from comparative foreign laws.

1.6 Scope and limitation of study

This dissertation is limited in scope and by some factors as follows. First, the study approaches data privacy and threats to personal data as a human rights issue and not as a commercial issue. As such, the study is not concerned with protection of personal data for example for

[32] Kainja (n 15) 9-11.
[33] ibid 18.
[34] ibid.
[35] Sioudina Mandibaye Dominique, 'Reforming the Content, Rather than Context, of the Chadian Constitution: Old Wine in a New Bottle?' (*ConstitutionNet,* 9 May 2018) <http://constitutionnet.org/news/reforming-content-rather-context-chadian-constitution-old-wine-new-bottle> accessed 6 September 2019.

the enhancement of trade or business growth,[36] but as a fundamental entitlement of everyone.[37]

Second, this study does not cover all types of ICTs. ICT is a broad term covering computer-based resources whether networked or independent and includes communication devices like phones, computer hardware and software applications, and services like broadcasting and distance learning.[38] This study focuses on 'privacy-destroying technologies' which 'facilitate the acquisition of raw data and (…) allow one to process and collate that data'.[39] These include computer systems, databases, phones and some platforms on the internet.

Third, the study is limited by the dearth of literature on data privacy protection in Malawi. The study will therefore draw from generalised literature, as applicable.

1.7 Structure of chapters

The dissertation is divided into six chapters. Chapter one provides the background and explains the research problem that justifies the need for this study. Thereafter, the research questions, methodology of research, literature review and limitations of the study are discussed. Chapter two is the theoretical take-off point of the study and discusses the theories elucidating the interplay between technology and law as well as the impact of the interplay on society, especially on vulnerable members. Chapter three enunciates the scope of the relevant legal framework for data privacy protection in Malawi. Chapter four undertakes an assessment of the adequacy of the extant data privacy legal frameworks

[36] An example of that perspective is Deloitte, 'Privacy is Paramount: Personal Data Protection in Africa' (*Deloitte*, 2017) <www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf> accessed 8 October 2019.

[37] Celestine Nyamu-Musembi and Andrea Cornwall, 'What is the "Rights-Based Approach" All About? Perspectives from International Development Agencies' (Institute of Development Studies working paper series 234 2004) <http://opendocs.ids.ac.uk/opendocs/handle/123456789/4073#.Vc2TC7Vu6Wg> accessed 15 October 2019; Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP 2014) 223.

[38] Government of Malawi, 'National ICT Master Plan 2014-2031' (*Malawi Diaspora*, 2014) <www.malawidiaspora.gov.mw/images/National-ICT-Master-Plan.pdf> accessed 8 October 2019 ix.

[39] Michael Froomkin, 'The Death of Privacy?' (2000) 52(5) Stanford Law Review 1461, 1468.

in view of the contexts, vulnerabilities and threats posed by ICTs and data processing activities in Malawi. This is in order to identify the gaps and areas requiring reform in the frameworks. Chapter five examines relevant comparative foreign laws to tease out how other jurisdictions have dealt with challenges of data privacy protection in order to deduce learning points for the reform of Malawi's data privacy protection regime for a more robust and effective regime. Chapter six concludes the dissertation by summarising the findings of the study and making appropriate recommendations.

2.

THEORETICAL FRAMEWORK

2.1 Introduction

The previous chapter sets out the background of the study and delineates the research agenda. To guide the research, this chapter explores theories on the role and impact of technology in society, particularly on vulnerable people. Specifically, the instrumental, substantive and synthetic theories of technology and law are discussed. Subsequently, the theoretical basis of this study is identified and discussed.

2.2 The instrumental theory

As the name suggests, instrumental theorists view technology as an instrument or tool capable of being used for any purpose by anyone.[40] According to them, technology is neutral, impartial and can be used to achieve various ends.[41] A plain example is a knife as a tool, it can be used to 'cook, kill or cure'.[42] Instrumentalists also regard technology as apolitical and usable in any social context, with costs of its transfer being the only hindrance to use in some contexts.[43] Further, they opine that technology works universally according to its technical architecture and is not influenced by economic, cultural or other contexts.[44] In addition, they state that efficiency of technology is measured similarly in every context thus buttressing its neutrality.[45]

[40] Andrew Feenberg, *Transforming Technology: A Critical Theory Revisited* (OUP 2002) 5-6.
[41] ibid.
[42] Rajab Ali, 'Technological Neutrality' (2009) 14(2) Lex Electronica <www.lex-electronica.org/en/auteur-e-s/ali-rajab/> accessed 8 October 2019 6.
[43] Feenberg (n 40) 5-6.
[44] ibid; Arthur Cockfield and Jason Pridmore, 'A Synthetic Theory of Law and Technology' (2007) 8(2) Minnesota Journal of Law Science and Technology 475, 501.
[45] Feenberg (n 40) 5-6.

In presenting technology as neutral, this theory underlines the agency of human beings in choosing whether to and how to use technology.[46] Instrumentalists state that the adoption, use and discard of technology is determined by the people and the law should simply provide a legal framework to foster and encourage development of technology.[47] Instrumentalists focus on how technology can be used for efficiency but they do not usually critically examine the underlying forces and negative impacts of technology.[48] They are disinterested in questions that require more than a surface analysis of technology.[49]

Instead, instrumentalists consider the proliferation of technology as necessary for social good.[50] This view is more prevalent today as the use of technology is viewed as a means to achieve what is beneficial for society, like economic growth and increase in incomes and living standards, while all other concerns are relegated to the background.[51]

Instrumentalists however acknowledge that there may be instances where other concerns or interests are advanced to limit the use of technology, for example protection of the environment.[52] Their view is that such interests are traded off at the expense of more efficiency.[53] The above views of instrumentalists are however challenged by substantive theorists who disagree that technology is a contexts neutral tool.

2.3 The substantive theory

Substantive theorists view technology as more than just a neutral tool and assert that it can substantively impact on society to the detriment of individuals and the society.[54] Substantive theorists lift the veil of ostensibly neutral technologies in order to determine the underlying determinants and impacts on society.[55] These theorists have thus analysed technologies and revealed how they have been used beyond

[46] Cockfield and Pridmore (n 44) 480.
[47] ibid 504.
[48] Cockfield and Pridmore (n 44) 482.
[49] Langdon Winner, 'Technology Today: Utopia or Dystopia' (1997) 64(3) Social Research 989, 1006.
[50] ibid 991.
[51] ibid.
[52] Richard Heeks, *Information and Communication Technology For Development* (1st edn, Routledge 2017) 318-352.
[53] Feenberg (n 40) 6.
[54] Cockfield and Pridmore (n 44) 483.
[55] ibid.

their purported purposes to disadvantage some sections of society.[56] One of the examples given by Winner relates to the deliberate design of low overpasses in Long Island in the USA to prevent buses serving less well-to-do communities from accessing places reserved for the rich.[57] The apparent purpose of the bridges was for transportation but it also had exclusionary effects on poor and black people who usually used public buses.[58] The undesirable effects of technology can be as a result of deliberate engineering as was the case with the Long Island overpasses but it can also be unintentional, arising from neglect or disregard.[59] For example, global practices signalling the exclusionary effect of technologies on persons with disabilities results from the fact that technologies are often designed without due regard to their needs but without any deliberate intention to marginalise them.[60]

Substantive theorists argue that technology is increasingly autonomous and people are merely objects used in technological processes.[61] Thus technology is structuring the world, shaping the way of life and has become indispensable.[62] They assert that technology is 'an independent, self-controlling, self-determining, self-generating, self-propelling, self-perpetuating and self-expanding force'.[63] Choice on whether to use and how to use them becomes an illusion as the choice is predetermined by technology.[64] From that understanding, human autonomy and human choice have no place in controlling the use and impacts of technology.

Technology is also seen as a means of domination and perpetuation of advantage of the elite, the privileged, the capitalists and the males.[65] Feminists state that men design technology for themselves and control it with the result that it furthers the disadvantage and marginalisation of women.[66] Technology is also seen as exclusionary in access, use and control to the benefit of the rich and privileged resulting in a digital

[56] Langdon Winner, 'Do Artifacts Have Politics' (1980) 109(1) Modern Technology: Problem or Opportunity? 121.
[57] ibid 123-125.
[58] ibid.
[59] ibid 125.
[60] See generally Jonathan Lazar and Michael Ashley Stein (eds), *Disability, Human Rights and Information Society* (University of Pennsylvania Press 2017).
[61] Feenberg (n 40) 6-8.
[62] ibid 14.
[63] Ali (n 42) 3.
[64] Feenberg (n 40) 14.
[65] Cockfield and Pridmore (n 44) 485.
[66] Cynthia Cockburn, *Machinery of Dominance: Women, Men and Technical Know-How* (PP 1985) quoted in Cockfield and Pridmore ibid 493.

divide.[67] Further, technology is viewed as the means to further capitalist powers.[68] The substantive theory therefore illustrates that politics and contexts behind technology are influential and it is important to dig beneath the surface to understand how technology affects society and people as this is not always obvious. However, the substantive theory of law and technology has been criticised for ignoring the power of human agency and for postulating that human agency has been overridden by technology.[69]

2.4 The synthetic theory

The synthetic theory is a middle ground between instrumental and substantive theories and is elucidated by Cockfield and Pridmore. In line with the views of instrumentalists, the synthetic theory recognises the importance of human agency.[70] At the same time, it takes on board the perspectives of substantive theorists that technology is not simply a neutral tool and it can be used to disadvantage and exclude the vulnerable.[71] It advocates for analyses of technology and law that are contextual and foster 'socially optimal technological developments'.[72]

Technology can be disruptive and traditional legal principles may not adequately deal with its adverse impacts. The synthetic theory proposes a method of legal analysis in such instances.[73] To illustrate how the analysis should proceed, Cockfield and Pridmore use an example of the first case of wiretapping without a warrant before the USA Supreme Court in 1928.[74] The accused was convicted mainly based on evidence obtained using a wiretap by the police without a warrant. The police were not required to get a warrant as it was only needed under the law in cases of physical searches of a house. The wiretap was done without a physical search of the house but using technology that enabled the police to hear conversations remotely.

[67] See generally Pippa Norris, *Digital Divide: Civic Engagement, Information Society and the Internet Worldwide* (CUP 2001).
[68] Cockfield and Pridmore (n 44) 494.
[69] ibid 498.
[70] ibid 500.
[71] ibid.
[72] Ibid.
[73] ibid 503-507.
[74] *Olmstead v United States* [1928] 277 United States 438 discussed by Cockfield and Pridmore (n 44) 506-507.

To determine how to approach this scenario, two steps are proposed under the synthetic theory.[75] First, the rights and interests that are traditionally protected under the law must be identified. In the example used by Cockfield and Pridmore, they identified the right to privacy as the traditional right.[76] Second, the effect of technology on the interest or right should be examined in a manner which is 'contextual, forward-looking, and less deferential to traditional doctrine and precedents'.[77] This requires a critical analysis of the 'substantive impact' of technology on people and their legal interests, beyond the obvious purpose of the technology.[78] The wiretapping in the case was meant to help in the fight against crime but its substantive impact on people was the invasion of privacy which had to be protected.[79] Thus the synthetic theory can aid in identification of rights threatened by technology as well as in the formulation of contextual and pre-emptive laws whose principles can depart from traditional doctrines.[80]

This study adopts the synthetic theory as its theoretical take off point because aspects of both instrumental and substantive theories are relevant for the analysis in the study. In line with the instrumental theory, this dissertation recognises that the fate of people is not entirely in the hands of technology and the value of human agency is acknowledged. The substantive theory is also relevant as this study does not see technology as a neutral tool. Rather, the study engages in a contextual and critical analysis of the substantive impact of technology with a view to ensuring optimum legal protection.

2.5 Conclusion

This chapter discussed the three theories of law and technology which explain the intersection between technology, law and society. The instrumental theory holds a simplistic view of technology as a neutral tool that can be used for various ends in any context. It ignores the contextual nature of the dynamics and impacts of technology on individuals and society. The substantive theory on the other hand exposes

[75] Cockfield and Pridmore (n 44) 503.
[76] ibid 503-507.
[77] ibid.
[78] ibid.
[79] ibid.
[80] ibid.

how technology is political and can have adverse effects on society and vulnerable people. However, the theory underestimates the power of human agency in controlling the impacts of technology. In view of the shortcomings of both theories, a synthetic theory of law and technology was developed based on a synthesis of elements of instrumental and substantive theories. The synthetic theory thus provides a framework for critical and contextual analysis of law and technology, while recognising the role of human agency. This chapter adopts the synthetic theory of law and technology as a framework for critical and contextual analysis of the impact of ICT on data privacy in contexts of vulnerabilities in Malawi. The next chapter examines the scope of protection generally guaranteed by Malawi's data privacy regime. This paves the way for the assessment of the adequacy and effectiveness of the regime in addressing threats arising from the particular contexts of ICT and data processing activities in the country in chapter four of the dissertation.

3.

MALAWI'S LEGAL FRAMEWORK FOR DATA PRIVACY PROTECTION

3.1 Introduction

As shown by the theoretical discussion in chapter two, technology can negatively impact on society and disadvantage vulnerable people hence legal frameworks for protection against the negative impacts must be contextual and formulated critically. This chapter examines the general scope and extent of data privacy protection deducible from Malawi's legal framework. Analysis in this chapter sets the stage for the assessment in the next chapter of the adequacy and effectiveness of the specific protections provided by the framework. The relevant legal framework comprises of applicable international and regional human rights instruments, the constitution, common law and acts of parliament. The applicable international and regional instruments are the International Covenant on Civil and Political Rights[81], the African Charter on the Rights and Welfare of the Child,[82] and the African Union Convention on Cyber Security and Personal Data Protection.[83] Malawi is a dualist state and therefore treaties are only enforceable domestically if incorporated in the law by municipal statutes.[84] The above-mentioned

[81] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171.

[82] African Charter on the Rights and Welfare of the Child (adopted 11 July 1990, entered into force 29 November 1999) CAB/LEG/24.9/49.

[83] African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014) EX.CL/846(XXV).

[84] Republic of Malawi (Constitution) Act No 20 of 1994 (Malawian Constitution), s 211; Reyneck Matemba, 'Incorporation of International and Regional Human Rights Instruments: Comparative Analyses of Methods of Incorporation and the Impact that Human Rights Instruments Have in a National Legal Order' (2011) 37(3) Commonwealth Law Bulletin 435, 438-439.

instruments have not been domesticated. As a result of the constraints of space, the scope of protections under the instruments are not discussed and the discussion below is restricted to applicable domestic norms.

3.2 The constitution

The Constitution of the Republic of Malawi (Malawian Constitution) is the supreme law in Malawi.[85] Section 21 of the Malawian Constitution states that everyone 'shall have the right to personal privacy' then it lists examples of conduct that would infringe on the right including interception of private communication.

Although the list of what the right to privacy entails is not exhaustive, the right has been construed narrowly by the courts in relation to information to cover only confidential or sensitive information.[86] There is however room for seeking protection of data privacy under section 21 as it is written in wide terms and the courts are enjoined to interpret the Malawian Constitution in line with international law norms.[87] However, adoption of such interpretation would be at the discretion of the court. The right to privacy can be limited according to sections 44(1) and 44(2) of the Malawian Constitution where such limitation is reasonable, in line with 'international human rights standards' and if 'necessary in an open and democratic society'.

3.3 The common law

As a relic of colonialism, the English common law is part of Malawi's legal system according to section 200 of the Malawian Constitution. Under the common law, privacy is not protected as an independent tort.[88] However, the common law has developed some remedies that can serve to protect data privacy rights, albeit to a limited extent.

[85] Malawian Constitution, s 10(1).

[86] For example, see *Kimu v Access Malawi Limited and others* Commercial Case 54 of 2011 (unreported); *Gwanda v S* Constitutional Cause 5 of 2015 (unreported).

[87] Malawian Constitution, s 11(2)(c).

[88] Raymond Wacks, 'Why There Will Never Be an English Common Law Privacy Tort' in Andrew Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (CUP 2006) 154.

A person can seek remedies for breach of confidence under the law of contract or under equity.[89] Initially breach of confidence only protected the unauthorised disclosure of confidential information by a person in a position of trust or under a contractual obligation to maintain confidence.[90] The law has however been modified by the courts in England and Wales over time and an action of breach of confidence can now be commenced in respect of information which one would reasonably expect to be kept private, and not just confidential information.[91] Further, if the information is private, an obligation of confidence is imposed regardless of the relationship between parties.[92] Malawian courts have not developed the law similarly but they are likely to follow suit as developments of the common law in England and Wales are highly persuasive to the courts in Malawi.[93] An action for breach of confidence can therefore protect data privacy only to the extent that the information concerned is private. The action is also restricted to unauthorised disclosures.[94]

The law of torts can also be relied on to protect data privacy. For example, the tort of trespass to property can protect against collection of personal information through unlawful interference with storage devices.[95] A cause of action can also lie in defamation if disclosure of personal information harms the data subject's reputation.[96] The tort of negligence can also be relied on in cases of damage resulting from negligent handling of personal information as a data controller arguably has a duty of care towards a data subject.[97] However, these remedies do not protect all the interests protected under the right to data privacy.[98]

[89] Tanya Aplin, 'The Development of the Action of Breach of Confidence in a Post-HRA Era' (2007) 1 Intellectual Property Quarterly 19.
[90] ibid.
[91] ibid.
[92] ibid.
[93] *Kishindo v Kishindo* Civil cause 397 of 2013 (unreported) 6-8.
[94] Wacks (n 88) 166.
[95] Lukman Adebisi Abdulrauf, 'The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa' (LLD thesis, University Of Pretoria 2015) 128.
[96] ibid.
[97] An action in negligence is premised on a defendant owing a claimant a duty of care and breach of the duty by the defendant resulting in suffering or damage to the claimant. See *Thomson v Lujeri Tea Estate* Personal injury case 95 of 2015 (unreported).
[98] Abdulrauf (n 95) 128.

3.4 Statutory protection of data privacy

Malawi does not have consolidated or single legislation on the right to data privacy but it has various statutes which can be relied on to protect the right. The relevant statutes are discussed below.

3.4.1 The National Statistics Act

Section 10 of the NSA permits the collection of personal data by the National Statistics Organisation for purposes of compiling statistics about the country.[99] Section 13 of the NSA generally prohibits the disclosure of information obtained by the organisation. Statistical data can be disclosed under section 14 of the NSA only if it is accurate and the confidentiality of the participants is protected. The act is only applicable in relation to personal information obtained for purposes of compiling statistics for the country. It is also limited to protection against disclosure and publication of inaccurate data. Other interests of data privacy are not protected for example, the collection of personal information is not restricted to strictly necessary information.

3.4.2 The Communications Act

Section 176(2) of the Communications Act criminalises unlawful interception, interference, disclosure or modification of electronic data, including personal data, by any person not authorised under the act.[100] An employee, licensee or agent of an entity with a communication licence can be criminally liable for disclosing information about a user obtained through electronic communication services under section 177 of the Communications Act. This may have general deterrent effects and help in minimising data privacy violations.[101] However, it does not grant data subjects enforceable rights. The investigation and prosecution in such matters against the alleged offender rests with the state through the Director of Public Prosecutions.[102]

[99] National Statistics Act Chapter 27:01 Laws of Malawi (NSA).

[100] Communications Act Chapter 68:01 Laws of Malawi.

[101] Punishments generally have a deterrent effect as stated in Esther Gumboh, 'Examining the application of deterrence in sentencing in Malawi' (2017) 20 Potchefstroom Electronic Law Journal 1, 7.

[102] Malawian Constitution, s 99 as read with the Criminal Procedure and Evidence Code Chapter 8:01 Laws of Malawi, s 76(1).

3.4.3 The Access to Information Act

The AIA provides for the right of access to information kept by public bodies and private bodies specified in the act (collectively referred to as information holders).[103] Under its section 20, seemingly confidential information of a person requested by a third party shall not be disclosed by information holders before determining whether the information is in fact confidential and whether disclosure would be harmful. Section 29 of the AIA mandates information holders to not disclose personal information 'unreasonably'. Personal information is defined in section 2 as 'information about an identifiable individual' and examples are listed including information relating to race, language, education, medical, address and biometrics. The AIA is relevant to protection of data privacy only to the extent that it prohibits unreasonable disclosure of personal data and controls disclosure of confidential information. However, it is only applicable to information holders where a request for information is made under the act.

3.4.4 The Electronic Transactions and Cyber Security Act

The ET Act came into force on 1 June 2017 and its objectives are stated as follows:[104]

> An Act to make provision for electronic transactions; for the establishment and functions of the Malawi Computer Emergency Response Team (MCERT); to make provision for criminalizing offences related to computer systems and information communication technologies; and provide for investigation, collection and use of electronic evidence; and for matters connected therewith and incidental thereto.

One of the 'matters connected therewith and incidental thereto' is personal data protection. The title of the ET Act shows that its focus is broadly on electronic transactions and its objectives are multifarious. The ET Act contains 104 provisions on various matters including formation of electronic transactions; liability for online service providers;

[103] Access to Information Act 13 of 2017 (16 February 2017) Malawi Gazette Supplement (AIA).

[104] According to the long title of the Electronic Transactions and Cyber Security Act Chapter 74:02 Laws of Malawi.

electronic commerce; consumer protection; management of domain names; electronic-government transactions and cybercrimes. Only four sections contain direct provisions on data privacy.[105] The scope of the ET Act is therefore broad as it covers issues in commercial law, criminal law, law of evidence and human rights. From the onset, data privacy protection was not the focus of the act as the objective in the initial bill was 'to set up a responsive ICT legal framework that can facilitate competition, development of ICT and the participation of (…) Malawi in the information age and economy'.[106] This confirms Makulilo's sentiments that protection of data privacy in African statutes is usually a secondary aim as the main concern is facilitating commerce.[107]

As stated earlier, only four sections in chapter VII of the ET Act deal with data protection and privacy. The first is section 71 which stipulates the duties of a data controller in relation to the processing of personal data. According to section 2 of the ET Act, a data controller is a person who collects, keeps, controls or processes data. Personal data is defined in section 2 of the ET Act as 'any information relating to an individual who may be directly identified' or may be indirectly 'identified by reference to an identification number or one or several elements related to his physical, physiological, genetic, psychological, cultural, social, or economic identity'.

A data controller is required under the said section 71 to collect personal data for 'specified, explicit and legitimate purposes' and to process it in line with the purposes for which it was obtained, lawfully and fairly. Further, personal data collected must be accurate, updated, sufficient, relevant and not more than required for the purposes. The data controller is mandated to delete or modify data which is inaccurate, incomplete or no longer necessary, as applicable.

The processing of personal data is permitted only in six circumstances according to section 71(2) of the ET Act. First, if consented to by the data subject unambiguously.[108] Consent is defined in section 2 as 'any freely given specific and informed indication by a data subject, of his wishes, by agreement, to his personal data being collected, processed

[105] The ET Act (ibid), ss 71-74.

[106] The E-Bill, art 2(1). See Parliament of Malawi, 'E-Bill' (*biz-file*, 2012) <https://biz-file.com/f/1210/Malawi_E-Bill_Draft_2012.doc> accessed 14 October 2019.

[107] Alex Boniface Makulilo, 'Myth and Reality of Harmonization of Data Privacy Policies in Africa' (2015) 31 Computer Law & Security Review 78, 79.

[108] The ET Act (n 105), s 71(2)(a).

or stored'. Second, where it is required for pre-contractual steps at the direction of the data subject or 'performance of a contract' binding on the data subject.[109] Third, where it is required under the law which the data controller is obliged to comply with.[110] Fourth, if it is required for purposes of protecting the 'vital interests of the data subject'.[111] Fifth, if required for tasks 'carried out in the public interest or in the exercise of official authority vested in a data controller or in a third party to whom the data is disclosed'.[112] Sixth, if necessitated by 'legitimate interests' of a data controller, or 'a third party to whom the data is disclosed' subject to 'the interests or fundamental rights and freedoms of the data subject'.[113]

Section 72 of the ET Act is on the rights of a data subject. The data subject has a right to obtain from the data controller information on whether his or her data is being processed, why it is being processed, the data being processed and other parties to whom the data is disclosed. A data subject can object to further processing of his or her personal data and if the objection is justifiable, the data controller is required to stop the processing. A data subject is empowered to demand that his or her personal data be modified, deleted or blocked if it is being processed in contravention of the ET Act.

Duties are imposed on a data controller in section 73 of the ET Act. A data controller is obliged to inform a data subject whose data has been collected: 'the identity of the data controller and of his representative';[114] to what end the data is being processed; his or her right to access and make corrections to the data; and his or her right to challenge the processing of personal data. Section 74 mandates a data controller to put in place 'appropriate technical and organizational measures for the protection of personal data', especially when the data is transmitted over a network.[115]

The ET Act criminalises unauthorised interference, access and disclosure of data,[116] and use of electronic communication to infringe on

[109] The ET Act (n 105), s 71(2)(b).
[110] ibid s 71(2)(c).
[111] ibid s 71(2)(d).
[112] ibid s 71(2)(e).
[113] ibid s 71(2)(f).
[114] ibid s 73(a).
[115] ibid s 74(1).
[116] ibid s 84.

the right to privacy.[117] Any victim of the crimes is entitled to complain to the monitoring authority who initiates assessment of the complaint and, if the complaint is 'relevant and reasonable', instigates further investigations.[118] The authority responsible for implementation of the act is the Malawi Communications and Regulatory Authority (MACRA) established under the Communications Act and its unit, the Computer Emergency Response Team (CERT), is responsible for monitoring cyber security.[119] However, the CERT is not operative yet.[120] According to section 5(1) of the Communications Act, MACRA is subject to the general direction of the minister on how to execute its duties. MACRA is also responsible for various duties relating to communications services in Malawi and its members are appointed by the president.[121]

3.5 Conclusion

This chapter reviewed the scope and extent of the protection given to data subjects under Malawi's current data privacy regime. Specifically, the Malawian Constitution, common law and some acts of parliament were examined. It has been noted that, although the constitution protects the right to privacy, it has been narrowly interpreted by the courts and currently pertains to private information. However, the text of the constitution is not restrictive and the right can be interpreted to include data privacy protection if the courts are minded to being progressive and proactive. As to the common law, several causes of actions were identified as relevant for data protection but their scope is limited. Regarding statutes, some statutes have provisions that offer protection to data privacy rights. It is however evident from the discussion that the ET Act has the most elaborate provisions on data privacy as opposed to other statutes which are limited in scope. The next chapter seeks to answer the question of whether the legal framework adequately and effectively addresses risks arising from prevalent ICT use in contexts of vulnerabilities in Malawi.

[117] The ET Act (n 105), s 87.
[118] ibid s 96.
[119] ibid ss 5 and 6.
[120] Jimmy Kainja, 'Privacy and Personal Data Protection: Challenges and Trends in Malawi' (CIPESA September 2018) <https://cipesa.org/?wpfb_dl=300> accessed 20 August 2019 13.
[121] The Communications Act (n 100), s 8.

4.

ADEQUACY AND EFFICACY OF MALAWI'S DATA PRIVACY LEGAL FRAMEWORK

4.1 Introduction

The previous chapter has confirmed the existence of legal protections of data privacy rights in Malawi. This chapter analyses whether the extant legal framework is adequate and effective for protecting data privacy in light of the increase in personal data processing activities facilitated by ICT in the contexts of the vulnerabilities in Malawi. The chapter commences with a discussion of the socioeconomic context and vulnerabilities in Malawi. Then the levels of ICT penetration and use in Malawi are discussed. Thereafter, risks to data privacy associated with uses of ICT in the contexts of Malawi are identified and the adequacy as well as effectiveness of the current legal framework to avert those risks are examined.

4.2 Socioeconomic context of Malawi

Located in South-Eastern Africa over an area of 118,480 square kilometres,[122] Malawi is classified as a poor country.[123] As at 2018, Malawi had a total population of about 17,563,749.[124] It is estimated

[122] Government of Malawi, 'The Malawi Growth and Development Strategy (2017-2022)' (*UNDP*, November 2017) <www.undp.org/content/dam/malawi/docs/UNDP_Malawi_MGDS)%20III.pdf> accessed 9 September 2019 1.

[123] World Bank, 'The World by Income and Region' (*The World Bank Data Topics*, 2017) <http://datatopics.worldbank.org/world-development-indicators/the-world-by-income-and-region.html> accessed 23 August 2019.

[124] National Statistical Office (NSO), '2018 Malawi Population and Housing Census Report' (NSO Malawi 2019) <www.nsomalawi.mw/images/stories/data_on_line/demography/census_2018/2018%20Malawi%20Population%20and%20Housing%20Census%20Main%20Report.pdf> accessed 23 August 2019 4.

that the population will grow rapidly to 19,400,000 by 2022 and the socioeconomic situation of the country will worsen as a result.[125] Various poverty reduction strategies and economic reforms have been implemented in the country with the hope of alleviating poverty but with no significant success.[126] Climate change, floods, droughts, electricity supply shortages, increased imports and reduced exports, macro-economic instability and corruption have stifled economic growth.[127] Although Malawi is generally classified as poor, some groups of people in the country are particularly vulnerable.

4.3 Vulnerabilities and intersectionality

4.3.1 Poverty

It is estimated that 50.7% of the people in Malawi live below the poverty line[128] and lack the means to purchase food with sufficient calories for adequate nutrition and other basic expenditures.[129] 25% live in ultra-poverty and do not have sufficient income to buy adequate food.[130] Indications from a poverty analysis suggest that the statistics underestimate the actual levels of poverty as 74% of Malawians are believed to be poor and unable to adequately fend for themselves.[131] Poverty levels have not really changed even in the years when economic growth was registered at an average rate of 6.1% annually between 2008 and 2014.[132] This is shown by the fact that despite the economic growth, the percentage of Malawians classified as poor only slightly decreased

[125] Government of Malawi, 'The Malawi Growth and Development Strategy (2017-2022)' (n 122) 1.

[126] Blessings Chinsinga, 'Decentralisation and Poverty Reduction in Malawi – A Critical Appraisal' in Gordon Crawford and Christof Hartmann, *Decentralisation in Africa* (Amsterdam UP 2008) 77.

[127] Peter Engbo Rasmussen, '2018 African Economic Outlook: Malawi' (AFDB 2018) <www.afdb.org/fileadmin/uploads/afdb/Documents/Generic-Documents/country_notes/Malawi_country_note.pdf> accessed 23 September 2019 1.

[128] ibid 14.

[129] ibid.

[130] ibid.

[131] ibid 8-9.

[132] Richard Mussa, 'Poverty and Inequality in Malawi: Trends, Prospects, and Policy Simulation' (MPRA 2017) <https://mpra.ub.uni-muenchen.de/75979/1/MPRA_paper_75979.pdf> accessed 27 September 2019 3.

by 0.8% in the six years between 2008 and 2014.[133] The benefits of economic growth have only been experienced by the rich while the conditions of the poor have largely stagnated.[134]

4.3.2 Inequalities in income, education and digital literacy

The gap between the rich and the poor is wide in Malawi.[135] Inequitable distribution of income was identified as a challenge in 2000 and the government committed to achieving fair and equitable distribution of income by 2020.[136] However, the inequalities persist as shown by the Gini coefficient value.[137] The most recent Gini coefficient value for Malawi is 44.7.[138] This shows that inequalities are increasing as the Gini coefficient in 2004 was 39.[139] Inequalities in access to education are also prevalent as statistics show that households with higher income levels are more educated than those with lower income.[140] High income households are also more digitally literate and have better access to ICTs than poor households.[141]

[133] World Bank and National Statistics Office of Malawi, 'Methodology for Poverty Measurement in Malawi (2016/17)' (World Bank 2018) <http://documents.worldbank.org/curated/en/575101534874113572/Methodology-for-Poverty-Measurement-in-Malawi> accessed 27 September 2019 16.

[134] Mussa (n 132) 4.

[135] See generally Richard Mussa and Winford Henderson Masanjala, 'A Dangerous Divide: The State of Inequality in Malawi' (Oxfam 2015) <www-cdn.oxfam.org/s3fs-public/file_attachments/rr-inequality-in-malawi-261115-en.pdf> accessed 27 September 2019.

[136] National Economic Council, 'Vision 2020: the National Long-Term Development Perspective for Malawi' (CEPA 2000) <https://cepa.rmportal.net/Library/government-publications/Vision%202020-%20The%20National%20Long%20Term%20Development%20Perspective%20for%20Malawi.pdf> accessed 26 September 2019 75.

[137] The Gini coefficient value measures levels of inequalities with 0 signifying ideal equality and 100 representing high inequalities. See World Bank, 'World Development Indicators 2013' (World Bank 2013) <https://openknowledge.worldbank.org/handle/10986/13191> accessed 26 September 2019 36.

[138] World Bank, 'GINI Index' (*World Bank*, 2017) <https://data.worldbank.org/indicator/si.pov.gini> accessed 26 September 2019.

[139] Mussa (n 132) 4.

[140] See generally National Statistical Office, 'Survey on access and usage of ICT services in Malawi' (Open Africa 2019) <https://open.africa/dataset/access-and-use-of-ict-services-survey/resource/11219fa2-ec00-4370-9e59-aa6f8cf37bad> accessed 3 August 2020.

[141] ibid 19.

Poor people get little or no benefit from the formal justice system as compared to the privileged because of various barriers.[142] These barriers include lack of awareness of legal rights and remedies; illiteracy; direct and indirect costs of prosecuting a court case; long distances between homes and courts; inability to comprehend the court's official language which is English; institutional and economic challenges of legal aid departments and organisations that offer free legal assistance; and the court's restrictive application of the rules on *locus standi* which shuts out public interest litigation.[143]

4.3.3 Gender disparities

Gender inequalities remain stark in Malawi as reported by the World Economic Forum which assessed levels of gender disparities in 144 countries and ranked Malawi poorly.[144] Female headed households are the majority at 57% and they are poorer than male-headed households.[145] More men are digitally literate and have more access to ICTs like mobile phones as 52% of men own phones as opposed to 33% of women.[146] Malawi is a patriarchal society where women are seen as subordinates to men and gender disparities perpetuate male dominance.[147] The subordinate status of women usually translates into coercive control by their male partners who monitor their technologies and coerce them into divulging mobile phones and social media passwords.[148]

[142] Siri Gloppen and Fidelis Edge Kanyongolo, 'Courts and the Poor in Malawi: Economic Marginalization, Vulnerability, and the Law' (2007) 5 International Journal of Constitutional Law 258, 273-282.

[143] ibid.

[144] World Economic Forum, *The Global Gender Gap Report* (World Economic Forum 2017) <www3.weforum.org/docs/WEF_GGGR_2017.pdf> accessed 11 October 2019 222-223.

[145] Ministry of Finance, Economic Planning and Development, 'Economic Development Document for Malawi' (*IMF*, May 2017) <www.imf.org/en/Publications/CR/Issues/2017/07/05/Malawi-Economic-Development-Document-45037> accessed 9 September 2019 5.

[146] Calum Handforth and Matthew Wilson, 'Digital Identity Country Report: Malawi' (GSMA 2019) <www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report.pdf> accessed 26 September 2019 14.

[147] Elizabeth Mkandawire, 'Socialisation of Malawian Women and the Negotiation of Safe Sex' (Msc thesis, University of Pretoria 2012) 6.

[148] Saskia van Veen, Bethan Cansfield and Sandrine Muir-Bouchard, '"Let's stop thinking its normal": Identifying patterns in social norms contributing to violence against women and girls across Africa, Latin America and the Caribbean and the Pacific' (Oxfam 2018) <www-cdn.oxfam.org/s3fs-public/file_attachments/rr-lets-stop-thinking-normal-evaw-social-norms-251118-en.pdf> accessed 12 October 2019 27.

4.3.4 Marginalisation of persons with disabilities

Persons with disabilities are marginalised and disadvantaged in Malawi. Statistics show that Malawi has 10.4% persons with disabilities with 49% having an eyesight impairment, 24% having a hearing impairment, 27% having leg mobility limitations and 9% having speaking difficulties.[149] Persons with disabilities lack adequate education and 35% of them have never enrolled in school.[150] They also have lower income levels as discrimination against them in employment persists.[151] Persons with disabilities are less digitally literate.[152] Analysis of the impact of ICT use and data processing in Malawi must take account of these contexts and vulnerabilities.

4.4 ICT and data processing activities in Malawi

Malawi, like other countries, is striving to harness the power of technology to achieve efficiency, effectiveness and transformation in various sectors. Malawi has specifically set out to be 'a technologically driven middle-income economy' by 2020.[153] Though some progress has been made, it is doubtful that the 2020 goal will be achieved. Telecom coverage is at 85% of the country.[154] However, only 51.7% of the households have a mobile phone, 33% have a radio, 11.8% have a television and 16.4% have access to the internet.[155] 22 internet service providers are licenced but only 10 are active and they have few customers relative to the size of the population.[156] The government is however working to increase ICT accessibility, use and affordability.[157]

[149] National Statistical Office, '2018 Malawi Population and Housing Census Report' (n 124) 28.

[150] Alister Munthali, 'A Situation Analysis of Persons with Disabilities in Malawi' (*Medbox*, 2011) <www.medbox.org/pdf/5e148832db60a2044c2d2a29> accessed 12 October 2019 16.

[151] ibid 19-20.

[152] CIPESA, 'Placing ICT Access for Persons with Disabilities at the Centre of Internet Rights Debate in Kenya' (*CIPESA*, 11 September 2019) <https://cipesa.org/2019/09/placing-ict-access-for-persons-with-disabilities-at-the-centre-of-internet-rights-debate-in-kenya/> accessed 12 October 2019.

[153] National Economic Council (n 136) 27.

[154] Government of Malawi, 'The Malawi Growth and Development Strategy (2017-2022)' (n 122) 45.

[155] National Statistical Office, 'Survey on access and usage of ICT services in Malawi' (n 140) 37.

[156] Government of Malawi, 'The Malawi Growth and Development Strategy (2017-2022)' (n 122) 45.

[157] Government of Malawi, 'Malawi Economic Recovery Plan' (*Resakss*, 2013) <www.resakss.org/sites/default/files/Malawi%202012%20Malawi%20Economic%20Recovery%20Plan.pdf> accessed 9 September 2019 14-15; Government of Malawi ibid 44-46.

Although ICT growth has hitherto been slow in Malawi, there is an upward trajectory of utilisation of the technology by the government, the private sector and individuals. The increase in ICT use and data processing activities is highlighted next. The illustrations are not exhaustive but are only aimed at showing that use of ICT is increasing and will only increase further alongside risks posed by its increased usage.

4.4.1 Collection and processing of personal data by the government

ICT has simplified the collection and processing of personal data. Initially, these were done using pen and paper; a process that was time consuming, error-prone, expensive and cumbersome.[158] To overcome these hurdles, ICT has been adopted by the government of Malawi. The collection of data by the government is not new, but ICT has enabled the collection on a larger scale with increases in associated risks.[159]

Various government departments collect and process personal data. For example, the National Registration Bureau collects personal data, including biographic and biometric data, for issuing national identity cards, identity cards for non-nationals, marriage registration certificates and death certificates.[160] The collected data is stored in a national identity system.[161] The national identity cards have smartcard chips that can be used to install 'multiple, custom-built applications' without the knowledge of the identity card holder.[162] The identity card can be linked to other systems using the chip and the personal data therein can be used for purposes other than the purposes for which they were collected.[163] The system is currently linked to other government systems.[164] The system has also been integrated with the system of a commercial bank, FDH Bank, without the consent of the data subjects

[158] Neil Palmer, 'ICT for Data Collection and Monitoring and Evaluation' (FAO June 2012) <www.fao.org/3/aq003e/aq003e.pdf> accessed 7 October 2019 1.

[159] Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and United States* (Cornell UP 1992), 18.

[160] National Registration Act Chapter 24:01 Laws of Malawi

[161] Handforth and Wilson (n 146) 5, 8.

[162] ibid 7.

[163] ibid.

[164] Jimmy Kainja, 'Are Malawians Sleep-Walking into a Surveillance State?' (*CIPESA*, 12 August 2019) <https://cipesa.org/2019/08/are-malawians-sleep-walking-into-a-surveillance-state/> accessed 10 October 2019.

and the bank will be able to access and process information from it.[165] Other banks are expected to link their systems to the national identity system soon.[166] There is no indication that there was an assessment of the necessity of integrating the systems and that specific measures have been put in place to avert data privacy risks.

Some government departments equally collect personal data for the issuance of official documents. For a birth certificate to be issued: the name, biographic details and details about the place of birth of the child; biographic details of the mother and father; and details about any other children of the mother are collected.[167] The Department of Immigration also collects information on place of origin and biographic and biometric details for purposes of issuing passports.[168] The Department of Road Traffic collects similar information which is stored in the Malawi Traffic Information System (MalTIS) before issuing licences, other related permits and registering vehicles.[169] The MalTIS is linked to the Malawi Revenue Authority's system for purposes of checking whether relevant taxes have been paid for registered vehicles.[170] Similarly, the National Statistical Office collects wide ranging personal information in order to compile statistics about the country.[171] The government also initiated mandatory SIM card registration resulting in collection of personal data of mobile phone subscribers.[172]

In addition, the government has created a universal beneficiary register which is currently intended to facilitate identification of beneficiaries of social programmes, management of social cash transfers and payments for public works programmes.[173] The plan is to extend

[165] James Nthondo, 'FDH Bank Integrates Malawi National ID System Through NRB System' (*Nyasa Times*, 8 June 2019) <www.nyasatimes.com/fdh-bank-integrates-malawi-national-id-system-through-nrb-system/> accessed 12 October 2019.

[166] ibid.

[167] Handforth and Wilson (n 146) 6.

[168] Department of Immigration and Citizenship Services, 'Passport Process' (*The Department of Immigration and Citizenship Services*, 2018) <www.immigration.gov.mw/passports/passport-process/> accessed 11 October 2019.

[169] A new electronic system was introduced in 2015 and the features are explained by Nation Online, 'Benefits of the New System' (*The Nation*, 1 July 2015) <https://mwnation.com/benefits-of-the-new-system-2/> accessed 11 October 2019.

[170] Kondwani Makanda, Thokozani Felix Vallent and Hyunsung Kim, 'Remarks on National Cyber Security for Underdeveloped and Developing Countries: Focused on Malawi' (2017) 6(7) American Journal of Engineering Research 257, 259 <www.ajer.org/papers/v6(07)/ZG0607257260.pdf> accessed 11 October 2019.

[171] National Statistics Act Chapter 27:01 Laws of Malawi (NSA).

[172] This was done under the Communications Act (n 100), s 92.

[173] Handforth and Wilson (n 146) 11.

its use to farm input subsidy programmes, village savings and loan programmes, microfinance, legal aid services for the poor, health services and education bursaries.[174] The collection and storage of data in all these systems are mainly technology based.

4.4.2 Collection of personal data by private entities and individuals

The private sector is also collecting and storing a myriad of personal information in Malawi. For example, people are required to provide personal data to companies before they can access products or services like insurance policies.[175] Commercial banks also require customers to fill mandatory 'know your customer' forms.[176] Personal data is also gathered through electronic transactions like internet banking and use of surveillance technologies in shops and offices. Further, most banks have central databases where they store customers' personal information accessible by all their branches unlike in the past when such information was kept only at the branch hosting the customer's account.[177] Most private companies are subsidiaries of or affiliated to international corporations outside Malawi and some of them transfer personal data abroad or integrate database systems with foreign companies.[178]

Individuals are also able to collect personal data using technology. For example, one can use a cell phone to collect personal data, including pictures and videos.[179] People are also sharing a lot of personal data on

[174] Kathy A Lindert and others, 'Rapid Social Registry Assessment: Malawi's Unified Beneficiary Registry' (World Bank November 2018) 31 <http://documents.worldbank.org/curated/en/363391542398737774/Rapid-Social-Registry-Assessment-Malawis-Unified-Beneficiary-Registry-UBR> accessed 26 September 2019.

[175] For example, see the form of one of the leading insurance companies in Malawi, NICO Life Insurance Company Limited, 'Personal Details for New Policy Application' (*NICO Life*) <www.nico-life.com/index.php/download-forms/individual-products/12-personal-details-for-new-policy-application/file> accessed 1 September 2019.

[176] National Bank of Malawi, 'Know Your Customer Detail Update Form' (*National Bank of Malawi*) <https://natbank.co.mw/forms/download-forms/know-your-customer-kyc-detail-update-form/188-know-your-customer-kyc-detail-update-form/file> accessed 1 September 2019.

[177] Johanna Vroegop, 'The Status of Bank Branches' (1990) 5(11) Journal of International Banking Law 445.

[178] For example, Liberty Health Malawi acknowledges in their privacy statement that sometimes they process personal information in other countries and some of the countries may have inadequate data protection laws. See Liberty Health, 'Privacy statement' (*Liberty Health*) <www.libertyhealth.net/malawi/en/privacy-statement/> accessed 16 October 2019.

[179] Michelle Caswell, 'Instant Documentation: Cell-Phone-Generated Records in the Archives' (2009) 72 The American Archivists 133, 133-135.

social media which can easily be downloaded or stored by others. It has been observed that many people in Malawi share sensitive personal data on social media.[180] In addition, hacking applications for the phone have been developed that enable one to monitor another person's social media private conversations, messages, emails, internet browsing history and GPS locations.[181]

4.4.3 Surveillance technologies

Various technologies are being used to survey people in public spaces, shops, offices and to monitor their telecommunications. Surveillance is 'the systematic investigation or monitoring of the actions or communications of one or more persons'.[182] The proclaimed purposes of surveillance in public spaces are public safety and security but they infringe on people's right to privacy.[183] The use of closed-circuit television (CCTV) cameras by the government in public spaces is not wide spread in Malawi but they have been installed in some public spaces like hospitals.[184] The government is also reported to have found partners in India to assist in installation of CCTV cameras with facial recognition in public places.[185] The use of CCTV cameras in Malawi is common in shops, banks and offices. Footages captured are meant to be used for identification of suspects who commit crimes within the premises.[186] Some employers also monitor their employees at work

[180] Kainja (n 120) 12.

[181] Easyapns, 'How to Monitor Someone's Whatsapp Messages from Mobile' (*Easyapns*, 17 December 2018) <www.easyapns.com/monitor-someones-whatsapp-messages/> accessed 12 October 2019.

[182] Roger Clarke, 'Introduction to Dataveillance and Information Privacy, Definition of Terms' (*Roger Clarke*, 24 July 2016) <www.rogerclarke.com/DV/Intro.html#InfoPriv> accessed 14 October 2019.

[183] Anna Tsiftsoglou, 'Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy' in Christina Akrivopoulou and Athanasios Psygkas (eds), *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices* (IGI Global 2011) 93.

[184] Arthur Chatora, 'Malawi Installs CCTV Cameras in Public Spaces to Fight Rampant Drugs Theft' (*This is Africa*, 10 November 2015) <https://thisisafrica.me/politics-and-society/malawi-installs-cctv-cameras-in-public-hospitals-to-fight-rampant-drugs-theft/> accessed 12 October 2019.

[185] Owen Khamula, 'Malawi to Have CCTV Cameras in Public Places: More Benefits from India-Africa Business Meeting' (*All Africa*, 27 March 2018) <https://allafrica.com/stories/201803270477.html> accessed 11 October 2019.

[186] For example see Tom Sangala, '3 Arrested for Mec Break-in' (*The Times*, 13 May 2019) <https://times.mw/3-arrested-for-mec-break-in/> accessed 11 October 2019.

using various technologies.[187] Although such monitoring is also done in white-collar jobs, low-wage workers like workers in retail shops, domestic workers and security guards are also usually monitored using privacy-intrusive measures like video recording and tracking using radio frequency devices.[188]

The government is also using a machine, the consolidated ICT regulatory management system popularly known in Malawi as the spy machine, to monitor conversations even though it is meant to regulate the telecommunications sector.[189] Further, the government is capable of monitoring and tracking people using registered SIM cards as the central database has personal information of the user and use of the SIM cards can be tracked.[190] The section below analyses the risks, how they are heightened by vulnerabilities and the adequacy and effectiveness of the law to address the risks.

4.5 Assessment of the adequacy and effectiveness of the Malawian data privacy legal framework in tackling contemporary challenges and risks

The expansive data processing activities highlighted above raise several data privacy concerns, risks and threats. The first is database safety and integrity of the data.[191] The ET Act appropriately mandates a data controller to ensure that personal data is secure, accurate and reliable. However, the security, reliability and accuracy of personal data in government systems is doubtful as illustrated by an assessment

[187] For example, some companies use a software named 'manage engine' to monitor what an employee is browsing on the internet and their downloads. See Allie Muhammed Kent, 'An Investigation on How Employee's Use of Internet at Workplace Has Impacted Employee's Performance – A Case Study of Telekom Networks Malawi Limited (TNM)' (Bsc thesis, Malawi College of Accountancy 2016) 20.

[188] Michele Estrin Gilman, 'The Class Differential in Privacy Law' (2012) 77(4) Brooklyn Law Review 1389, 1400-1403.

[189] Green Muheya, 'Malawi rolls out "spy machine": Macra can now listen to people's phone conversation' (*Nyasa Times*, 24 January 2018) <www.nyasatimes.com/malawi-roll-spy-machine/> accessed 23 September 2019.

[190] Ewan Sutherland, 'The Mandatory Registration of SIM Cards' (2010) (16)3 Computer and Telecommunications Law Review 61, 61–63; Privacy International, 'Africa: SIM Card Registration Only Increases Monitoring and Exclusion' (*Privacy International*, 5 August 2019) <www.privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion> accessed 16 October 2019.

[191] David Banisar, 'Linking ICTs, the Right to Privacy, Freedom of Expression and Access to Information' (2010) 16 East African Journal of Peace & Human Rights 126.

of the universal beneficiary register. After the universal beneficiary register was rolled out and information of about four million people had been collected, an assessment of the system was conducted by a team from the World Bank.[192] The assessment revealed that there is a risk of data breaches because the local server with all the collected personal information does not have firewall protection or other mechanisms to detect intrusions.[193] Further, even though some controls have been put in place like password control, the staff have not been given specific roles such that they can all access the system, share the data and modify the content thereby affecting its reliability and accuracy.[194] Apart from the staff directly implementing the system, the system can also be accessed by users responsible for managing social programmes. Access to personal data has not been restricted to specific users and it is not stated whether some data will be anonymised for other users.[195] There are no security sockets layer certificates for the encryption of data to protect the data and there are no measures to ensure adherence to data-sharing protocols.[196]

Section 74 of the ET Act requiring a data controller to put in place technical and organisational measures to protect the personal data can be used to oblige the government to adequately secure such systems. However, questions arise about who will request and ensure that the government puts in place security measures. Ordinarily, the data subjects should question how their personal data will be secured. However, the beneficiaries of universal beneficiary register are vulnerable people in need of social support who are likely to focus on the benefits because of desperation and they may not care about protection of data privacy. They may not even know the risks associated with personal data processing because of digital illiteracy.[197] The law is therefore not effective in the protection of their rights to data privacy as there is no mechanism or entity responsible for ensuring that their data privacy is protected.

The second problem is that data collection activities by the government leave people with little or no choice of opting out as people need the services or documentation whose grant are contingent on disclosure of personal data. Human agency is overcome in such cases and even

[192] Lindert and others (n 174).
[193] ibid 57.
[194] ibid 57-58.
[195] ibid 58.
[196] ibid.
[197] Kainja (n 164) 30.

privacy-conscious individuals are forced to give their information. Such a scenario highlights and confirms the claims of substantive theorists that technology can force certain actions without leaving people with any choice. Thus, people's personal data can be exploited or denigrated without any opportunity on their part to avoid or mitigate the risks. The legal framework in Malawi does not address this concern as systems can be implemented without any data privacy risk assessment. Further, there is no mechanism to audit whether systems are respecting data privacy rights. Under the current legal framework, people can approach the court either for a pre-emptive remedy if the risks to their rights are foreseeable and irreparable or for damages in case of breaches. The rich and privileged would know about and would be able to pursue such court actions. However, the poor and vulnerable are likely to just suffer the consequences and not pursue any remedy in case of violations because of the various barriers to access to justice including lack of awareness, costs, distance to courts and formal barriers to public interest litigation.

The third risk is that ICT technicalities may hinder oversight and accountability. This is because technology is necessarily technical and scientific outside of the ken and competence of average citizens. The poor and vulnerable may not even have basic knowledge of ICT workings. Therefore, evaluation of ICT systems is sometimes required to be done by experts like the team from World Bank that evaluated the universal beneficiary system.[198] Under the extant legal regime, there is no requirement for the establishment of an oversight body with experts responsible for analysing whether the systems are technically secure. Therefore, the protection offered is inadequate and ineffective. Similarly, the risks are bound to disproportionately affect the poor who may not have access to any remedy in case of infringements.

The fourth risk is that technology databases can be used for discrimination and exclusion.[199] Technology with identity information can replicate or even enhance discrimination because it is 'codified, managed in complex inflexible structures, where the individual is merely a passive subject rather than an active participant'.[200] For example, it

[198] Lindert and others (n 174).

[199] Giovanni Sartor, 'Human Rights in the Information Society: Utopias, Dystopias and Human Values' in Mario Viola de Azevedo Cunha and others, *New Technologies and Human Rights: Challenges to Regulation* (1st edn, Ashgate Publishing Limited 2013) 15.

[200] Privacy International, 'ID, Identity and Identification' (*Privacy International*) <www.privacyinternational.org/what-we-do/id-identity-and-identification> accessed 16 October 2019.

has been alleged that employment and social goods in Malawi mainly benefit the tribe which the president is affiliated with to the exclusion of other tribes.[201] The ICT systems can therefore be used for targeted allocation and exclusions even though that is not their professed purpose. Further, history is awash with examples of human rights abuses based on profiling and identities which databases can facilitate with relative ease.[202] Information which poses higher risks and can be used to unfairly discriminate against or exclude a person is categorised as sensitive data.[203] The ET Act does not offer enhanced protection to sensitive data such that it can be processed like any other personal data. This deficiency can be exploited by the powerful and privileged for selective practices to the detriment of the less powerful and vulnerable.

The fifth problem is that personal data can be used beyond authorised purposes. As illustrated above, personal data collected for legitimate government purposes like issuing identity cards is being disclosed to commercial banks by integration of systems without the consent of data subjects. This is prejudicial to the data subjects because private banks are profit oriented and data privacy may not be their core interest. The ET Act does not adequately address this risk but it can actually facilitate it. This is because the provisions stipulating the circumstances in which processing of personal data is permissible are too wide, ambiguous and liable to abuse. For example, under section 71 of the ET Act a data controller can process personal data, even without the consent of the data subject, if it is in 'the vital interests' of the data subject; 'carried out in the public interest'; or necessary for 'legitimate interests pursued' of the data controller. These terms are not clear, are too broad and can be used to justify processing of data for other purposes and thereby trump data privacy rights. The only way to challenge unauthorised personal data processing under the Malawian legal framework would be via the

[201] Nyasa Times, 'Lomwe Becomes Buzz Word for Malawi's Employment, Business' (*Nyasa Times*, 3 August 2009) <www.nyasatimes.com/lomwe-becomes-buzz-word-for-malawis-employment-business/> accessed 12 October 2019.

[202] *Prosecutor v Jean-Paul Akayesu* Case ICTR-96-4-T (International Criminal Tribunal for Rwanda) [123]; Ethiopians of Eritrean origin were targeted for deportation, harassment and discrimination see Home Office, 'Country Information and Guidance Ethiopia: People of Mixed Eritrean/Ethiopian Nationality' (*Refworld*, 2016) <www.refworld.org/pdfid/57c6daf84.pdf> accessed 15 October 2019 4;

[203] Spiros Simitis, 'Revisiting Sensitive Data' (CoE 1999) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806845af> accessed 15 October 2019.

courts. The poor and vulnerable are likely not to challenge the data processing, even if their rights are violated, because of the barriers to access to justice identified above. The data controllers can therefore use ICT for their own ends without accountability. On the other hand, rich and privileged people can afford to challenge the processing of their personal data in court. The provisions are therefore not only inadequate but would serve to further disadvantage the poor and the vulnerable.

The sixth risk is that private entities can transfer personal data to other countries without adequate check and constraints. As stated above, Malawian companies have related parties in other jurisdictions who they share personal data with. There are no restrictions in the ET Act on cross border transfer of personal data. According to Fombad and Abdulrauf, 'it is customary' to include provisions on trans-border data exportation because the data is exposed to greater risks when exported.[204] If there are any breaches in a foreign country, the poor and vulnerable may be unable to obtain a remedy as complex issues of conflict of laws would arise and a lot of resources would be needed to pursue the claims.

The seventh risk is that personal data can be unfairly or unlawfully used. For example, it can be used for identity theft by impersonation, which is generally on the rise in Africa.[205] The stolen identity can be used for various purposes including obtaining social benefits, services, property, money, or any other valuable thing or benefit that the victim is entitled to.[206] The identity can also be used to commit fraud, to facilitate 'illegal migration, terrorism, espionage and to evade criminal sanctions or apprehension'.[207] Biometric information is of particular concern as it is 'inseparably linked' to a person and can be abused resulting in great harms.[208] These may include arrest for crimes committed by the identity thief, pain and suffering, rejection of claims

[204] Charles Manga Fombad and Lukman Adebisi Abdulrauf, 'The African Union's Data Protection Convention 2014: A Possible Cause for Celebration in Human Rights in Africa?' (2016) 8 Journal of Media Law 67, 86.

[205] Banisar (n 191) 126.

[206] OECD, 'The Scope of Online Identity Theft' in *OECD Online Identity Theft* (OECD Publishing 2009) 17.

[207] Fawzia Cassim, 'Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?' (2015) 18(2) Potchefstroom Electronic Law Journal 69, 72-73.

[208] United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (*UN Docs*, 3 August 2018) 5 <https://undocs.org/A/HRC/39/29> accessed 16 October 2019.

or benefits because of exhaustion by the identity thief and reputational harm imperilling prospects of employment.[209] As such, various rights including the right to security of person, property, privacy, economic development, autonomy and dignity would be threatened. The ET Act does not explicitly criminalise identity theft but interference with data. The law can therefore be used to punish the offenders but the provision is inadequate as there are no direct remedies for the victim. Further, the CERT which is responsible for monitoring cybercrimes is not operational. Furthermore, MACRA, which is the body charged with receiving complaints from victims of cybercrimes is inundated with other duties pertaining to the communications sector, is subject to the general direction of the minister and its members are appointed by the president as discussed above. The independence and efficiency of MACRA is therefore compromised.

The eighth risk is that unregulated data processing may undermine democratic processes in favour of the technologically powerful as political campaigns are now turning 'into sophisticated data operations' which can unfairly influence votes by swaying and suppressing voters.[210] In Zimbabwe and Kenya, there are reports that the ruling parties were sending personalised and targeted messages to prospective voters and they obtained the personal data from mobile network operators.[211] In Nigeria, it was alleged that the Communications Commission disclosed data of the electorate to the ruling party which enabled the party to target its campaigns.[212] The ET Act prohibits the disclosure of personal data but the exceptions are broad and unclear as already highlighted. Therefore, disclosure of such information can be justified based on the exceptions and the only recourse for data subjects would be the courts.

[209] Cassim (n 207) 75.

[210] Privacy International, 'Data and Elections' (*Privacy International*) <https://privacyinternational.org/learning-topics/data-and-elections> accessed 16 October 2019.

[211] Grace Mutung'u, 'The Influence Industry: Data and Digital Election Campaigning in Kenya' (*Our Data Our Selves*, June 2018) 11-13 <https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf> accessed 22 August 2019; Tawanda Karombo, 'Zimbabwe's First Ever Election Without Robert Mugabe Has Turned into a Data Privacy Minefield' (*Quartz Africa*, 11 July 2018) <https://qz.com/africa/1325485/zimbabwe-elections-whatsapp-sms-spam-data-privacy-concerns-for-mnangagwa-chimasa/> accessed 16 October 2019.

[212] Olugbenga Adanikin, '2019 election: How APC may have benefitted from NCC, INEC breach of voters' privacy' (*International Centre for Investigative Reporting*, 1 February 2019) <www.icirnigeria.org/2019-election-how-apc-may-have-benefited-from-ncc-inec-breach-of-voters-privacy/> accessed 16 October 2019.

As postulated above, this is ineffective protection for the poor and vulnerable and it marginalises them further.

The ninth risk is that stalking, harassment, infringement of privacy and intimidation are amplified by increased sharing of personal data online.[213] Women are particularly vulnerable to such risks in Malawi. For example, there have been instances of photos and videos of naked or partially clothed women being taken without their consent and circulated online in breach of their rights to dignity and privacy.[214] Remedies against such can either be criminal at the discretion of the state or civil. Vulnerable people are unlikely to pursue the civil remedy because of barriers to access justice.

Generally, vulnerable people who do not know the repercussions of personal data breaches are more likely to fall prey to the above dangers as they may not exercise due care and caution when divulging certain personal data. They would also face more threats because most of the technology is imposed on them, they may not be familiar with the risks and they may not do or be able to do anything to mitigate the risks. Inequalities in the country may also result in empowerment of the rich, literate, educated, male, persons without disability who may be able to exploit technologies and protect themselves from the adverse impacts while the vulnerable are further disempowered.[215] As illustrated above, the ET Act has many gaps and deficiencies that hinder it from protecting data privacy rights adequately and effectively. Examination of the adequacy of other laws in Malawi is done below.

The constitutional protection of the right to privacy also does not offer adequate protection against these serious threats because it has been construed narrowly by the courts as protecting against the unauthorised disclosure of private information. The information collected by the government and private entities is not always confidential or secret and it is initially disclosed by the data subject and as such, it would not be protected under the Malawian Constitution. Additionally, the right to

[213] Shandre Sissing and Johan Prinsloo, 'Contextualising the Phenomenon of Cyber Stalking and Protection from Harassment in South Africa' (2013) 2 Acta Criminologica: Southern Africa Journal of Criminology 15, 17.

[214] Rossalyn Warren, 'Cycle of Shame: Harassed in the Street, Then Again on Social Media' (*CNN*, 2018) <https://edition.cnn.com/2018/01/08/africa/malawi-cycle-of-shame-asequals/index.html> accessed 12 October 2019.

[215] Robert M Bichler, 'Southern Africa and the Digital Divide: A Malawian Case Study' (2008) 4(6) International Journal of Technology, Knowledge and Society 41, 46.

privacy is not absolute as it can be limited if reasonable, in line with 'international human rights standards' and if 'necessary in an open and democratic society'. A data controller can decide to process personal data under the guise of the exceptions and the only remedy of the data subjects would be via court action. This is problematic especially in Malawi where there are many barriers to the right of access to justice of the vulnerable.

The common law action for breach of confidence can only protect data privacy to the extent that the information concerned is private. However, personal data does not have to be private for it to be protected under data privacy rights.[216] Another limitation is that the action is restricted to unauthorised disclosure.[217]

Other statutes discussed in chapter three are limited in scope and cannot address the identified risks arising from the upsurge of ICT. The NSA cannot be applied in respect of personal data obtained through other means than during collection of data for statistical purposes. The AIA is relevant only to the extent that it prohibits unreasonable disclosure of personal data kept by the government and controls disclosure of confidential information. The Communications Act on the other hand only offers criminal remedies that are focused on the offender. Therefore, the effectiveness of the Communications Act in fostering data privacy protection in the country, beyond the general deterrent effect of punishment, is limited. Malawi's legal frameworks therefore fall short of adequate and effective protection of the right to data privacy.

4.6 Conclusion

This chapter contextually analyses the adequacy and effectiveness of the existing data privacy regime in Malawi. For a meaningful analysis, the chapter commenced with an exposé of the socioeconomic contexts, the different contexts of vulnerabilities and the levels of ICT in the

[216] Lukman Adebisi Abdulrauf, 'The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa' (LLD thesis, University Of Pretoria 2015) 21.

[217] Raymond Wacks, 'Why There Will Never Be an English Common Law Privacy Tort' in Andrew Kenyon and Megan Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (CUP 2006) 166.

country. It was also shown that ICT is a double-edged sword which can be used to benefit as well as imperil people's rights. The analysis was in line with the synthetic theory of law and technology. As demonstrated in the chapter, ICT is being used and a lot of personal data is being processed by the government and private entities in Malawi. Collection, retention, use and disclosure of personal data are sometimes being done unfairly, unlawfully and without the consent of the data subjects. The security of some of the systems is compromised and there are no measures to ensure that the data is accurate and reliable. Data privacy risks associated with the operationalisation of ICT include loss of dignity, identity theft, fraud, discrimination, exclusion, harassment and undermining of democratic processes. The rights to security of a person, property, economic development, privacy, autonomy and dignity are also threatened. The risks are more pronounced in Malawi because of prevalent vulnerabilities. Despite the dangers posed by rapid advances in ICT, Malawi's legal frameworks are lagging behind in efficacy and adequacy to address the challenges. Further, the supervisory and enforcement measures are ineffective especially for vulnerable people. The chapter thus underscores the need and urgency of formulating appropriate laws for the protection of data privacy within the contexts of Malawi. It has therefore become important to identify workable law reform approaches for Malawi in this regard. The next chapter looks at comparative jurisdictions for purposes of drawing lessons to address observed deficiencies and gaps.

5.

LESSONS FROM COMPARATIVE FOREIGN LAWS

5.1 Introduction

The preceding chapter established and demonstrated the necessity of reforming the data privacy protection framework of Malawi for it to respond more adequately to the data privacy challenges in the country. In formulating or reforming a law, it is sometimes useful to derive lessons from other jurisdictions but wholesale transplantation of the law should be avoided.[218] This chapter explores the data protection frameworks of other jurisdictions in order to draw lessons from their best features and avoid their shortcomings. Data privacy protection regimes differ,[219] so the regimes of the European Union (EU) and South Africa have been purposefully selected as comparators in this study. This chapter commences by justifying the selection of the EU and then evaluating EU's data privacy regime. Thereafter, the chapter discusses the choice of South Africa and examines South Africa's legislative framework. Insights will be drawn from both regimes to inform suggested reforms to the data privacy frameworks in Malawi.

[218] South Africa Law Reform Commission (SALRC), 'Privacy and Data Protection Report' (The Department of Justice and Constitutional Development , 2009) <www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf> accessed 2 October 2019 615; Alex Boniface Makulilo, 'Data Protection Regimes in Africa: Too Far from the European "Adequacy" Standard?' (2013) 3(1) International Data Privacy Law 42, 50.

[219] Beth Magnuson, Sarah Branam and Patrice Ettinger, 'Threading the Needle: Harmonising Global Privacy Practices' (presented at IAPP Global Privacy Summit 2019) 16-17 <https://iapp.my.salesforce.com/sfc/p/#1a000000HSGV/a/1P0000000HSl/6TfRQ7b.qUuXkLfSnbqtfGnHtPFrqOptcdTy.pqAfPc> accessed 18 October 2019.

5.2 Data privacy protection in the EU

5.2.1 Why the EU?

The EU has one of the most comprehensive data privacy protection regimes in the world and it is regarded as a trendsetter as well as catalyst of data privacy protection laws.[220] The main instrument for the protection of data privacy is the General Data Protection Regulation (GDPR) adopted in 2016 and effective from 2018.[221] The GDPR replaced the Data Protection Directive 95/46/EC (Directive).[222] Selection of the EU legal regime for lesson drawing in this study is hinged on three main factors: it is human rights centred;[223] it is one of the most comprehensive data privacy protection regimes; and it specifically addresses current and anticipated challenges posed by technologies.[224]

Nevertheless, the EU regime cannot be transplanted wholesale into Malawi because of some material differences. First, the GDPR is a regional instrument applicable in various countries in the EU and some provisions are specifically based on that setting. Second, the EU is generally more developed and its ICT is generally more advanced than in Malawi. The economic growth of EU countries is incomparable with that of Malawi.[225] Hence, a critical approach will be adopted in drawing applicable lessons so that only insights that aid in effective data privacy protection in Malawi, with regard to its contexts, influences lessons to be drawn.

[220] Alex Boniface Makulilo, 'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) International Data Privacy Law 163, 163.

[221] EU General Data Protection Regulation 2016/679 of 27 April 2016 of the European Parliament and of the Council 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 [2016] OJ L119/1 (GDPR).

[222] EU Directive 95/46/EC of 24 October 1995 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281/31 (Directive).

[223] Paul M Schwartz and Karl-Nikolaus Peifer, 'Transatlantic Data Privacy Law' [2017] The George Town Law Journal 106, 123.

[224] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2016) 28(1) Information & Communications Technology Law 65, 65-67.

[225] World Bank, 'European Union' (*World Bank*) <https://data.worldbank.org/region/european-union> accessed 20 October 2019.

5.2.2 The right to data privacy protection in the EU

The EU places a premium on the right to privacy and data protection. Article 7 of the Charter of Fundamental Rights of the European Union[226] guarantees the right to privacy as historically conceived. Article 8 of the EU Charter however guarantees 'the right to the protection of personal data' which confers rights of access and rectification, requires an independent authority to oversee compliance and mandates fair processing of personal data. The right to personal data protection is the cardinal basis of the GDPR as acknowledged in the preamble.[227] However, the right to personal data protection is not an absolute right and it must be proportionally balanced with other rights and interests.[228] The GDPR notes the increase in data processing resulting from technology proliferation in recital 6 but underlines the need for a 'stronger and more coherent data protection framework (…) backed by strong enforcement'.[229]

5.2.3 Scope of activities regulated under the GDPR

The GDPR regulates the processing of personal data. Article 4(1) of the GDPR defines personal data broadly as 'any information relating to an identified or identifiable person' and it lists examples of identifiers including a name, location, genetic identity and identification number. The definition of personal data is not restricted to data of an identified person but also an identifiable person because of the relative ease of linking personal information to identify a person using technology.[230]

Processing refers to an 'operation or set of operations which is performed on personal data or sets of personal data (…)'.[231] Various examples are listed including collection, alteration, transmission, deletion and storage. According to article 2(1), the GDPR applies to computerised processing and to manual processing if the personal data are 'part of a filing system or are intended to form part of a filing system'.

[226] Charter of Fundamental Rights of the European Union (signed 12 December 2007, took effect 1 December 2009) 2012/C 326/02 (EU Charter).
[227] GDPR (n 221), recital 1.
[228] ibid recital 2.
[229] ibid recital 7.
[230] ibid recital 26; Bart van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4(4) International Data Privacy Law 307, 309.
[231] GDPR (n 221), art 4(2).

Processing of personal data by authorities in relation to criminal offences or for public security are exempted from the regulation.[232] In addition, processing by a natural person for 'purely personal or household activity' is exempted from the provisions of the GDPR.[233] However, video surveillance for security to property, health or life does not qualify under the exception as a purely personal or household activity even if the camera is installed at a private house.[234]

5.2.4 Principles on processing of personal data

Article 5 of the GDPR elucidates principles on processing of personal data. The principles are similar to those contained in section 71 of the ET Act in Malawi on fairness, limitation to purpose, minimal processing, accuracy and security. The GDPR however outlines three additional principles. First, the GDPR requires that processing be done in a transparent manner.[235] Second, it limits the storage of personal data 'in an identifiable form for no longer than is necessary for the purposes for which the personal data are processed' except for archiving in the public interests, for research and for statistical records if appropriately secured.[236] Third, a duty of accountability is imposed on the controller to ensure and prove compliance with all the principles of personal data processing.[237] A controller is a person or entity with power to decide the purpose and 'means of processing of personal data', alone or with others.[238] Recital 39 also adds that personal data should only be processed 'if the purpose of the processing could not reasonably be fulfilled by other means'.

5.2.5 Lawful basis for processing personal data

The circumstances under which personal data processing is permissible under article 6 of the GDPR are similar to those in section 71(2) of the ET Act discussed in chapter three above. However, article 6(2) of the GDPR gives states discretion to devise specific provisions

[232] GDPR (n 221), art 2(2)(d).
[233] ibid art 2(2)(c).
[234] *František Ryneš v Úřad Pro Ochranu Osobních Údajů* (2014) ECLI:EU:C:2014:2428.
[235] GDPR (n 221), art 5(1)(a).
[236] ibid art 5(1)(e).
[237] ibid art 5(2).
[238] ibid art 4(7).

on when processing can be deemed 'necessary for compliance with a legal obligation' of a controller and 'necessary for the performance of a task carried out in public interest or in the exercise of official authority vested in the controller'.

The GDPR also contains further provisions on consent of a data subject. Consent must be 'freely given, specific, informed and unambiguous' indicated 'by a statement or by a clear affirmative action'.[239] If the consent is written in a declaration together with content relating to other matters, the consent should be 'clearly distinguishable from the other matters' and given in an 'intelligible and easily accessible form, using clear and plain language'.[240] The data subject should be at liberty to withdraw their consent easily. A child below 16 years old cannot validly give consent but it must be given by a parental figure.[241] The controller must ensure that the person consenting on behalf of the child is truly a parental figure.[242]

5.2.6 Processing of sensitive data

Article 9 of the GDPR prohibits processing of 'special categories of personal data' which is the term used to refer to sensitive data. Sensitive data includes data disclosing a person's race, ethnicity, political viewpoints, religious convictions, philosophical views, trade union affiliation, genetic information, biometrics, health information and information relating to a person's sex life or sexual orientation.[243]

Sensitive data can be processed in limited circumstances according to article 9(2) of the GDPR as follows: based on explicit consent of the data subject; if necessary for exercise of the controller's rights as employer; pursuant to the data subject's rights as an employee, social security beneficiary, social protection beneficiary or under a collective labour agreement; if the data subject is unable to consent and the processing is in their 'vital interests'; processing of details of members or former members or persons closely affiliated to a non-profit body acting pursuant to its legitimate activities; personal data disclosed publicly by

[239] GDPR (n 221), art 4(11).
[240] ibid.
[241] ibid art 8.
[242] ibid.
[243] ibid art 9.

the data subject; processing by courts in official capacity; for 'substantial public interests' under the law proportional to purposes and with respect to data protection rights; necessary for health reasons subject to proper safeguards; necessary for public health interests like prevention of serious health threats; and necessary for archiving in accordance with a law providing adequate protection to rights of data subjects. Article 10 proscribes processing of personal data on criminal convictions and offences except if done 'under the control of official authority' or under a law with adequate protection of data subject rights.

5.2.7 Rights of data subjects

The GDPR grants a wide array of rights to data subjects. All the rights in section 72 of the ET Act discussed in chapter 3 are included in the GDPR. The GDPR however guarantees rights beyond those. First, a data subject has a right to access their personal data and information pertaining to processing of that data under article 15 of the GDPR. Second, a data subject has a 'right to be forgotten' entitling them to deletion of personal data promptly by the controller upon request.[244] Upon such request, the controller is required to ensure that that the personal data is also erased by other controllers if it was disseminated further.[245] However, the right is subject to exceptions in order to balance it with other rights and interests like freedom of expression, public health and the freedom of information.[246] Third, article 20 of the GDPR stipulates that a data subject shall be entitled to collect their personal data for transmission to another controller if the processing is pursuant to a contract, their consent or done by automated means. This is known as the 'right to data portability' per the heading of article 20 of the GDPR. Fourth, a data subject is entitled to object to decisions being made based on automated processing.[247] The rights accorded to data subjects reveal the intention of the drafters for an individual to own and control their personal data.[248]

[244] GDPR (n 221), art 17.
[245] ibid art 17(2).
[246] ibid art 17(3).
[247] ibid art 22.
[248] van der Sloot (n 230) 315.

5.2.8 Duties of controllers

Seven duties of a controller stipulated in the GDPR are pertinent. One, a controller is required to implement measures in order to comply with the GDPR under article 24, including formulation of policies. Two, in designing and implementing a system, a controller is required to incorporate 'appropriate technical and organisational measures' to comply with the GDPR and protect rights of the data subject.[249] This is known as 'data protection by design and default'.[250] Three, a controller is allowed to engage another party (a processor) to process personal data only if they guarantee compliance with the GDPR and 'the rights of the data subject'.[251] Four, a controller is obliged to keep records of all its personal data processing activities.[252] Five, a controller is required to report to the supervisory authority any personal data breach promptly and if possible, within 72 hours of knowing about it.[253] Where such breach would pose 'a high risk to the rights and freedoms of natural persons' it shall be communicated to the data subject promptly.[254]

Six, a controller is obliged to conduct an assessment of the impact of intended data processing on personal data protection, especially by use of new technologies and if the processing carries high risks.[255] The assessment is for determining necessity, proportionality and whether adverse impacts have been adequately mitigated. Seven, a controller and a processor are required to have a data protection officer if they process data as a public authority or data processing is their main activity or sensitive data are extensively processed by them.[256] The data protection officer is responsible for ensuring compliance with the GDPR and collaborating with the supervisory authority, among other duties.[257] The duties imposed on the controller are consonant 'with the risk-based approach of the GDPR'.[258]

[249] GDPR (n 221), art 25(1).
[250] Per the heading ibid art 25.
[251] ibid art 28.
[252] ibid art 30.
[253] ibid art 33.
[254] ibid art 34.
[255] ibid art 35.
[256] ibid art 37(1).
[257] ibid art 39.
[258] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation: A Practical Guide* (1st edn, Springer 2017) 31.

5.2.9 Cross border transfers

Chapter V of the GDPR regulates cross border transfers of personal data. Such transfers are permissible if the receiving country provides 'an adequate level of protection' as determined by the European Commission.[259] The factors to be considered in determining adequacy are enumerated including the respect for human rights, state of rule of law, data privacy legal framework, existence of independent supervisory bodies and international treaty obligations binding the country.[260] In the absence of a decision on adequacy, trans border transfers are allowed if the controller has put in place 'appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available'.[261] The transfer can also be done if the conditions under article 49 of the GDPR are satisfied including consent of the data subject with full knowledge of the risks.

5.2.10 Supervisory body

Chapter VI of the GDPR requires the establishment of an independent supervisory body under the law responsible for monitoring compliance with the GDPR. Independence entails that it must be free from direct or indirect external influence.[262] The members are required to be knowledgeable, skilled and experienced for their roles.[263] Their appointment can be effected by the parliament, 'government, a head of state or independent body', as long as the appointment procedure is transparent.[264] The supervisory body shall have extensive powers including: to conduct public awareness; conduct investigations; give advice; enforce compliance; track pertinent ICT and commercial developments with an impact on personal data protection; encourage adoption of and review codes of conduct; resolve complaints lodged relating to data protection rights; conduct data protection audits; ban data processing and carry out other tasks for the protection of

[259] GDPR (n 221), art 45.
[260] ibid art 45(2).
[261] ibid art 46.
[262] ibid art 52.
[263] ibid art 53.
[264] ibid.

personal data.[265] Its services shall be rendered without charge to the data subject, unless the 'requests are manifestly unfounded or excessive' then a reasonable fee may be charged for administrative costs.[266] A data subject can commence judicial review proceedings against a supervisory authority's decision relating to him or her.[267]

5.2.11 Review of the GDPR

Article 97 of the GDPR requires the European Commission to review the GDPR regularly and submit reports to the European Parliament and Council at intervals of four years. The reports can include proposals for amendments particularly in view of changes in information technology.[268]

5.2.12 Critique of the GDPR

Despite being lauded as comprehensive and providing adequate protection to data privacy, some shortfalls of the GDPR have been identified. The main criticism is that it is too complicated,[269] not easy to understand, too lengthy, cumbersome and has high compliance and administrative costs.[270] It is reported that companies struggled to abide by the complex requirements because they could not fully understand the rules and exceptions.[271] This is problematic as failure to comply because of complexity of the rules would be against the objectives of the GDPR. Having examined the GDPR, the next section discusses the South African legal framework for purposes of drawing further insights.

[265] GDPR (n 221), arts 57 and 58.
[266] ibid art 57(3).
[267] ibid art 58(4).
[268] ibid art 97(5).
[269] Hoofnagle, van der Sloot and Borgesius (n 224) 98.
[270] EMOTA, 'Lessons from Europe and Data Protection' (United Nations Conference on Trade and Development 2017) <https://unctad.org/meetings/en/Presentation/dtl_eWeek2017p13_OliverHateley_en.pdf> accessed 18 October 2019.
[271] Philip Heijmans, 'Getting the Business Over Data Privacy' (*US News*, 1 August 2018) <www.usnews.com/news/best-countries/articles/2018-08-01/across-europe-new-data-privacy-law-still-leaves-confusion> accessed 20 October 2019.

5.3 South Africa's legal framework for data privacy protection

5.3.1 Why South Africa?

The data protection laws in South Africa provide useful insights to Malawi for various reasons. First, South Africa has one of the most comprehensive pieces of data privacy legislation in Africa which has been described as adequate for protection of personal data.[272] The principal data protection law in South Africa is the Protection of Personal Information Act (PPIA) which was enacted after extensive research and which drew insights from various jurisdictions around the world.[273] Second, both Malawi and South Africa are part of Southern African Development Community and African Union (AU) which have instruments on data privacy that may influence domestic law. Third, some provisions of the constitutions of both countries are similar, including the provision guaranteeing the right to privacy. Fourth, the PPIA prioritises human rights,[274] which is in line with the approach advocated for in this study.

5.3.2 The rights to data privacy in South Africa

Section 14 of the Constitution of South Africa provides for the right to privacy. Although the right to data privacy is not explicitly guaranteed, the courts have interpreted the right to privacy to include the right to protection of personal data.[275] The PPIA commences with a preamble that clearly recognises the constitutional right to privacy as the basis for protection of data privacy. The right is also granted to legal persons on the ground that they are equally impacted by data processing activities and deserve protection.[276]

[272] Makulilo (n 220) 222.
[273] Act 4 of 2013.
[274] Pamela Stein, 'South Africa's EU-style Data Protection Law' (2012) 10 Without Prejudice 48.
[275] Iain Currie and Johan De Waal, *The Bill of Rights Handbook* (6th edn, Juta 2013) 302-303.
[276] Definition of person under s 2 of the PPIA includes a juristic person. The reason was stated by SALRC (n 218) 83-84.

5.3.3 Data privacy protection under the PPIA: Points of departure from the GDPR

Similar to the GDPR, the PPIA contains extensive provisions on the rights of data subjects, duties of controllers and processors, principles of data processing, lawful grounds for processing personal data, processing of sensitive data, cross border transfers and establishment of a supervisory authority. The convergence is explicable on the basis that drafting of the PPIA was largely influenced by the EU's Directive and the GDPR which was in draft form at the time.[277] Therefore, the principles replicated in South Africa's framework from the EU will not be restated. However, the EU's framework was not the sole influence as drafters of the PPIA consulted widely in order to tailor the law to its contexts and considered relevant laws from other jurisdictions including the United Kingdom, Netherlands, New Zealand, Canada and Australia.[278] This section will therefore focus on the points of divergence of the PPIA from the GDPR.

Firstly, the PPIA mandates all entities to have an information officer, the equivalent of a data protection officer in the GDPR.[279] That is unlike the GDPR that places the requirement on specified entities. The officers are supposed to be registered with the regulator.[280]

Secondly, the PPIA establishes a supervisory body namely a regulator 'subject only to the Constitution' and accountable to the National Assembly.[281] Under section 60 a regulator may issue codes of conduct. Members of the regulator are appointed under section 42(2)(a) 'by the President on the recommendation of the National Assembly'. When security of personal data is compromised, the responsible party is mandated to inform the regulator and data subject as soon as reasonably possible.[282] The PPIA does not impose a requirement to report the breach in 72 hours like the GDPR.

Thirdly, some provisions in the GDPR are not included in the PPIA. For example, the right to be forgotten and the right to data portability are not included. These rights grant a data subject more control over their

[277] Stein (n 274) 48.
[278] SALRC (n 218) 615- 645.
[279] PPIA, s 56.
[280] ibid s 55(2).
[281] ibid s 39.
[282] ibid s 22.

personal data,[283] especially on the internet and the omission of the rights may lead to inadequate protection. As to duties of the controller, the controller is not required to implement privacy by design or to conduct data privacy impact assessments. These omissions may similarly result in inadequate protection of data privacy as they are meant to avert risks.

Fourthly, although the PPIA permits cross border transfers in limited circumstances like the GDPR, including that the third country should have an adequate level of data privacy protection, it does not give detailed guidance on how to determine adequacy. Section 72 simply states that an adequate level of protection shall 'uphold principles for reasonable processing of information that are substantially similar to the conditions for lawful processing'.

Fifthly, the PPIA does not provide for periodic review of the act. Section 40(1) however requires the regulator to monitor technological developments and to inform the minister of the developments. Further, the regulator can recommend amendments of the law to parliament.[284]

Sixthly, the PPIA is structured and drafted in a manner that aids in understanding an otherwise complex legislation in a relatively novel area. For example, rights of a data subject are outlined in the first part of the act and a data subject would not have to struggle in finding them which is commendable especially in contexts of lack of awareness.[285] Further, the PPIA provides a kind of summary of circumstances in which it would be lawful to process personal information in section 4 with cross reference to the section with details of the principle. The preamble is also short and easily comprehensible. Additionally, the duty of the regulator to raise awareness and educate is the first duty listed which emphasises the need in view of lack of awareness in African countries.[286]

Seventhly, the nomenclature in the PPIA is different from that adopted in the GDPR. An equivalent of a controller in the GDPR is a responsible party in the PPIA. Special categories of personal data in GDPR are simply special personal information. A data protection officer in the GDPR is an information officer in the PPIA. Lastly, a supervisory body in the GDPR is a regulator in the PPIA. This highlights the importance of purposefully selecting terminology.

[283] van der Sloot (n 230) 315.
[284] PPIA, s 40(1)(e)(ii).
[285] Lukman Adebisi Abdulrauf, 'The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa' (LLD thesis, University Of Pretoria 2015) 284.
[286] ibid 289.

5.4 Conclusion

This chapter examined the legal frameworks for protection of data privacy in the EU and South Africa. The EU was selected on account of its strict and comprehensive approach to data privacy protection. The analysis focused on the GDPR which is the main data privacy protection instrument in the EU. The GDPR contains detailed provisions on processing of personal data, exemptions from the regulations, rights of data subjects, duties of controllers and processors, cross border data transfers, and establishment of a supervisory body. It is fair to conclude that the GDPR does offer adequate and effective protection of data privacy. However, it is drafted in a manner that is difficult to understand, it is lengthy and compliance is resource intensive.

As for the South African legal framework, its main instrument for data privacy protection is the PPIA and it is similar to the GDPR in most of its content. However, some provisions of the GDPR are not replicated in the PPIA which makes it a bit less complicated but may lead to inadequate data privacy protection or cause uncertainties. The PPIA is more onerous than the GDPR in its requirement that every entity should have an information officer. Further, rights under the PPIA are granted to legal persons and not just natural persons. The PPIA is drafted in a manner that makes it easier to understand and that foregrounds rights of data subjects as well as the need for public awareness raising by the regulator. The next chapter concludes this study by summarising the findings of the research and making recommendations based on the insights from the legal frameworks of the EU and South Africa.

6.

CONCLUSIONS AND RECOMMENDATIONS

6.1 Synopsis of conclusions

This study assessed the adequacy and effectiveness of Malawi's data privacy protection frameworks in responding to threats to data privacy rights in present-day realities of ICT proliferation and in the contexts of socioeconomic vulnerabilities in the country. The research agenda, the gap in literature and the scope of the study were detailed in chapter one. Chapter two identified the theoretical framework that underpins the research namely the synthetic theory which underlies critical and contextual legal analysis of substantive impacts of technology in society. Chapter three examined Malawi's data privacy protection frameworks and showed that they do offer some protection to data privacy. Chapter four then assessed the sufficiency and adequacy of the existing legal frameworks in addressing the challenges and dangers of ICT operationalisation in contexts of vulnerabilities in Malawi. To that end, the socioeconomic context, the nature of prevalent vulnerabilities and the scope of ICT utilisation in the country as well as its impact on people's rights, particularly the vulnerable, were discussed. That discussion set the scene for an analysis of the efficacy of the legal regime to address the impacts of ICT especially on vulnerable members of society. The chapter concluded that the legal framework is inadequate and ineffective. Chapter five explored the legal frameworks of the EU and South Africa for the identification of workable approaches and lessons for addressing the gaps and deficiencies in Malawi's data privacy protection frameworks. This chapter concludes the study by making recommendations for more robust and effective data privacy protection in Malawi below.

6.2 Recommendations

6.2.1 Recognition and constitutional entrenchment of the right to data privacy

The right to data privacy is important for individuals in contemporary times as infringements to the right have ripple effects and threaten other rights as illustrated in this study. The EU Charter explicitly recognises the right to data protection. In South Africa, the right to data privacy is protected under the constitutional right to privacy by virtue of judicial precedents. It is recommended that the right to data privacy be explicitly included in the Malawian Constitution, separate from the right to privacy because the interests it protects differ from those protected under the right to privacy. The South African approach of protecting data privacy as a subcategory of the right to privacy as interpreted by the courts is not preferred because the recognition, interpretation and scope of the right to data privacy may be at the discretion of a judge who may not adopt a favourable approach. Further, constitutional entrenchment would impose duties on the state to respect, protect and fulfil the right for everyone, including the poor and vulnerable who may not be able to secure protection on their own. Furthermore, once entrenched it would acquire a superior status over other laws and practices because the constitution is the supreme law of the country. However, amendment of the constitution is a rigorous process and may take some time. In the meantime therefore, the courts should recognise and develop the right to data privacy in the country.

6.2.2 Promulgation of a comprehensive data privacy law

A comprehensive law regulating the processing of personal data and protecting the right to data privacy is indispensable in light of the increase in data processing activities threatening and imperilling the rights of the people. The ET Act is a step in the right direction but it is inadequate as exemplified in this study. An extensive data privacy protection law should be formulated and it should be human rights centred. The preamble and object clause must clearly state that the act is for the protection of the right to data privacy. The content of the law must be determined after extensive comparative studies, wide

consultations and specific consideration of how best to protect the right to data privacy of the generality of the people and the vulnerable.

The following factors should be paramount in the act. First, personal information and data processing should be defined widely like it is done in the GDPR in light of technologies that easily piece information together and that are rapidly advancing such that we cannot contemplate how data will be processed in the future. Second, rights of data subjects should be included in the GDPR-style because they give adequate control over personal data. Third, detailed principles of data processing should be incorporated as done in both the GDPR and the PPIA to ensure that data processing is done fairly, lawfully, transparently, for a specified purpose, in line with purpose of collection, securely, on quality and reliable data, in an accountable manner and that the data is kept for no longer than necessary. Fourth, sensitive data should be accorded enhanced protection. This is particularly important as biometrics are being collected more and shared even with commercial entities without regard to the attendant risks.

Fifth, the provisions on when personal data can be lawfully processed should be unambiguous, clear and limited. Vague grounds like 'the vital interests' of the data subject; 'carried out in the public interest'; or necessary for 'legitimate interests' of the data controller should be clarified for example by specifying the criteria applicable, limiting circumstances in which those grounds can be relied on, restricting the types of processing and who the data can be transmitted to.

Sixth, cross border data transfers should be allowed in limited circumstances just like they are done under the GDPR and the PPIA. However, Malawi should learn from the GPDR and clearly encapsulate the criteria for determining whether another country has adequate levels of protection. Further, the determination of adequacy should be made by the regulator and it should be allowed to make blanket determinations in respect of countries or particular sectors within countries.

Seventh, specific duties should be imposed on controllers and processors in view of the power they yield when personal data is at their disposal. The duties can be modelled after the EU's and South Africa's risk-based approaches. However, the duties should be practicable for them to be effective. For example, in a small economy like Malawi, it may not be practical to require every entity processing personal data to have a data protection officer. Entities can therefore be allowed to designate an employee as responsible for executing duties of a data

protection officer on condition that he or she can ably execute the role considering his or her qualifications, other duties and the magnitude of data processing activities. The officers should be registered with the regulator who should have power to assess and approve or disapprove the suitability of the appointed officer. The above proposals would however be ineffective in the absence of a strong monitoring and enforcement mechanism.

In addition, it is crucial to have an independent regulator because of the lack of awareness, vulnerabilities and inequalities in Malawi. To ensure independence of the regulator, the act must clearly state that the regulator will be subject only to the constitution and the law, and that appointment of its members must be done in a specified and transparent manner for example by the parliament. The members must be adequately qualified and experienced for their roles. The regulator must have the primary duties of educating and raising awareness, ensuring compliance with the act, advising entities about requirements under the act, auditing data processing systems and handling complaints under the act. Its services must be provided free of charge, especially to the poor and vulnerable, its procedure must be simple and it must be adequately resourced. However, in terms of the constitution, the High Court would still have jurisdiction over matters within the jurisdiction of the regulator.[287] Considering that data privacy issues are novel and sometimes complicated because of technicalities, the act should require that independent experts be involved in all cases relating to data privacy breaches or threats in connection with ICT. The judiciary and lawyers should also be trained in data privacy protection. However, it is unlikely that the courts will be inundated with data privacy cases if the regulator is effective because of the costs and delays in courts. For profound impact, the regulator must be proactive and have powers to act on its own motion in order to protect the rights of the poor and vulnerable.

Furthermore, the proposed act must be drafted in a manner that is easy to understand and the terminology adopted should be simple. The other statutes with provisions relating to data privacy identified in chapter three must be amended and made subject to the proposed act to avoid inconsistencies. For example, the definition of personal information in the AIA is narrow and outdated hence it must be aligned

[287] Malawian Constitution, s 108.

with a more expansive definition in the proposed act. The proposed act must require the regulator to review it periodically, in intervals of not more than four years, and to recommend amendments to the Ministry of Justice and legislature.

6.2.3 Ratification and domestication of human rights treaties

Malawi should ratify the African Union Convention on Cyber Security and Personal Data Protection and domesticate it. It should also domesticate the International Covenant on Civil and Political Rights and the African Charter on the Rights and Welfare of the Child for enhanced protection of data privacy rights. Entities like the Legal Aid Department and organisations that offer *pro bono* services should be empowered and adequately resourced to be able to lodge cases before regional and international human rights bodies on behalf of the poor and vulnerable. The instruments should however be subject to the constitution and the act proposed above in case of inconsistencies.

6.2.4 Other general recommendations

Beyond the above recommendations, there is a need for concerted efforts in protection of data privacy rights in Malawi. First, the Malawi Human Rights Commission, civil society, human rights activists and human rights organisations must step up their efforts for the protection of rights to data privacy. They can collaborate with organisations working on data privacy issues world-wide like Privacy International.[288] Second, companies, organisations and government departments must develop adequate and comprehensive data privacy protection policies. Third, scholars should do more research on the right to data privacy. Various topics could be explored including: the need for a gendered data privacy law; data privacy in employment; data privacy on the internet; data privacy and public security; data privacy and healthcare; data privacy impact assessments; and data privacy and freedom of the press. To the best of my knowledge and after diligent research, I discovered that only one scholar has done research and written on the

[288] Privacy International does a lot of advocacy, research and litigation on issues pertaining to the right of privacy worldwide, including in Africa. See Privacy International, <https://privacyinternational.org/> accessed 29 September 2019.

right to data privacy in Malawi.[289] Research can be bolstered by the inclusion of a module or subject on the right to data privacy in law school as well as business schools because most businesses are now data driven. Fourth, ICT experts should develop and encourage the public to use technologies that enhance data privacy.

If the above suggestions are implemented, Malawi will undoubtedly be well on the way to becoming a data privacy compliant and respecting country for the security and betterment of the country and people.

[289] Jimmy Kainja, 'Privacy and Personal Data Protection: Challenges and Trends in Malawi' (CIPESA September 2018) <https://cipesa.org/?wpfb_dl=300> accessed 20 August 2019; Jimmy Kainja, 'Are Malawians Sleep-Walking into a Surveillance State?' (*CIPESA*, 12 August 2019) <https://cipesa.org/2019/08/are-malawians-sleep-walking-into-a-surveillance-state/> accessed 10 October 2019.

BIBLIOGRAPHY

BOOKS AND ARTICLES

Ali R, 'Technological Neutrality' (2009) 14(2) Lex Electronica <www.lex-electronica.org/en/auteur-e-s/ali-rajab/> accessed 8 October 2019

Aplin T, 'The Development of the Action of Breach of Confidence in a Post-HRA Era' (2007) 1 Intellectual Property Quarterly 19

Balkin JM, 'Critical legal theory today' in Mootz FJ (ed), *On Philosophy in American Law* (CUP 2009)

Banisar D, 'Linking ICTs, the Right to Privacy, Freedom of Expression and Access to Information' (2010) East African Journal of Peace & Human Rights 124

Bennett C, *Regulating Privacy: Data Protection and Public Policy in Europe and United States* (Cornell UP 1992)

Bernal P, *Internet Privacy Rights: Rights to Protect Autonomy* (CUP 2014)

Bichler RM, 'Southern Africa and the Digital Divide: A Malawian Case Study' (2008) 4(6) International Journal of Technology, Knowledge and Society 41

Brickhill J and Leeve YV, 'Transformative Constitutionalism – Guiding Light or Empty Slogan' (2015) Acta Juridica 141

Button M and Cross C, *Cyber Frauds, Scams, And Their Victims* (Routledge 2017)

Bygrave LA, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (1998) 6 International Journal of Law and Information Technology 247

— 'Privacy and Data Protection in an International Perspective' (2010) 56 Scandinavian Studies in Law 166

— 'Privacy Protection in a Global Context: A Comparative Overview' (2004) 47 Scandinavian Studies in Law 320

Cassim F, 'Protecting Personal Information in the Era of Identity Theft: Just How Safe is Our Personal Information from Identity Thieves?' (2015) 18(2) Potchefstroom Electronic Law Journal 69

Caswell M, 'Instant Documentation: Cell-Phone-Generated Records in the Archives' (2009) 72 The American Archivists 133

Chinsinga B, 'Decentralisation and Poverty Reduction in Malawi – A Critical Appraisal' in Crawford G and Hartmann C, *Decentralisation in Africa* (Amsterdam UP 2008)
Cockfield A and Pridmore J, 'A Synthetic Theory of Law and Technology' (2007) 8(2) Minnesota Journal of Law Science and Technology 475
Currie I and De Waal J, *The Bill of Rights Handbook* (6th edn, Juta 2013)
Feenberg A, *Transforming Technology: A Critical Theory Revisited* (OUP 2002)
Feldstein S, 'The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression' (2019) 30 Journal of Democracy 40
Ferreira P, 'Angels and Demons: Data Protection and Security in Electronic Communications' in de Azevedo Cunha MV and others, *New technologies and Human Rights: Challenges to Regulation* (1st edn, Ashgate Publishing Limited 2013)
Fombad CM and Abdulrauf LA, 'The African Union's Data Protection Convention 2014: A Possible Cause for Celebration in Human Rights in Africa?' (2016) 8 Journal of Media Law 67
Froomkin AM, 'The Death of Privacy?' (2000) 52(5) Stanford Law Review 1461
Gilman ME, 'The Class Differential in Privacy Law' (2012) 77(4) Brooklyn Law Review 1389
Gloppen S and Kanyongolo FE, 'Courts and the Poor in Malawi: Economic Marginalization, Vulnerability, and the Law' (2007) 5 International Journal of Constitutional Law 258
Gumboh E, 'Examining the Application of Deterrence in Sentencing in Malawi' (2017) 20 Potchefstroom Electronic Law Journal 1
Heeks R, *Information and Communication Technology for Development* (1st edn, Routledge 2017)
Heyns C and Viljoen F, *The Impact of the United Nations Human Rights Treaties on the Domestic Level* (Springer 2002)
Hoofnagle CJ, van der Sloot B and Borgesius FZB, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2016) 28(1) Information & Communications Technology Law 65
Kairys D, 'Introduction' in Kairys D (ed), *The Politics of Law: A Progressive Critique* (3rd edn, Basic Books 1998)
Kennedy DW, 'The International Human Rights Regime: Still Part of the Problem?' in Dickinson R and others (eds), *Examining Critical Perspective on Human Rights* (CUP 2012)
Lazar J and Stein MA (eds), *Disability, Human Rights and Information Society* (University of Pennsylvania Press 2017)
Lynskey O, 'Deconstructing Data Protection: The "Added Value" of a Right to Data Protection in the EU Legal Order' (2014) 63(3) International and Comparative Law Quarterly 569
Makanda K, Vallent TF and Kim H, 'Remarks on National Cyber Security for Underdeveloped and Developing Countries: Focused on Malawi' (2017) 6(7) American Journal of Engineering Research 257
Makulilo AB (ed), *African Data Privacy Laws* (Springer 2016)

Makulilo AB, 'Privacy and Data Protection in Africa: A State of the Art' (2012) 2(3) International Data Privacy Law 163
— 'Data Protection Regimes in Africa: Too Far from the European 'Adequacy' Standard?' (2013) 3(1) International Data Privacy Law 42
— 'Myth and Reality of Harmonization of Data Privacy Policies in Africa' (2015) 31 Computer Law & Security Review 78
— 'The Quest for Information Privacy in Africa' (2018) 8 Journal of Information Policy 317
Matemba R, 'Incorporation of International and Regional Human Rights Instruments: Comparative Analyses of Methods of Incorporation and the Impact that Human Rights Instruments Have in a National Legal Order' (2011) 37(3) Commonwealth Law Bulletin 435
Mutua M, 'Human Rights in Africa: The Limited Promise of Liberalism' (2008) 51(1) African Studies Review 17
Norris P, *Digital Divide: Civic Engagement, Information Society and the Internet Worldwide* (CUP 2001)
OECD, 'The Scope of Online Identity Theft' in *OECD Online Identity Theft* (OECD Publishing 2009)
Rabinowitz V, 'The Radical Tradition in the Law' in Kairys D (ed), *The Politics of Law: A Progressive Critique* (3rd edn, Basic Books 1998)
Sartor G, 'Human Rights in the Information Society: Utopias, Dystopias and Human Values' in de Azevedo Cunha MV and others, *New Technologies and Human Rights: Challenges To Regulation* (1st edn, Ashgate Publishing Limited 2013)
Schwartz P and Peifer KN, 'Transatlantic Data Privacy Law' [2017] The George Town Law Journal 106
Sissing S and Prinsloo J, 'Contextualising the Phenomenon of Cyber Stalking and Protection from Harassment in South Africa' (2013) 2 Acta Criminologica: Southern Africa Journal of Criminology 15
Sloot B van der, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4(4) International Data Privacy Law 307
Solove DJ, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San Diego Law Review 745
Stein P, 'South Africa's EU-style Data Protection Law' (2012) 10 Without Prejudice 48
Sutherland E, 'The Mandatory Registration of SIM Cards' (2010) (16)3 Computer and Telecommunications Law Review 61
Taub N and Schneider EM, 'Women's Subordination and the Role of Law' in Kairys D (ed), *The Politics of Law: A Progressive Critique* (3rd edn, Basic Books 1998)
Tsiftsoglou A, 'Surveillance in Public Spaces As a Means of Protecting Security: Questions of Legitimacy and Policy' in Akrivopoulou C and Psygkas A (eds), *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices* (IGI Global 2011)
Tzanou M, 'Data protection as a Fundamental Right Next to Privacy? "Reconstructing" A Not So New Right' (2013) 3 International Data Privacy Law 88

Viljoen F, *International Human Rights Law in Africa* (2nd edn, OUP 2012)
Voigt P and Von Dem Bussche A, *The EU General Data Protection Regulation: A Practical Guide* (Springer 2017)
Vroegop J, 'The Status of Bank Branches' (1990) 5(11) Journal of International Banking Law 445
Wacks R, 'Why There Will Never be an English Common Law Privacy Tort' in Kenyon A and Richardson M (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (CUP 2006)
Warren A, Dearnley J and Oppenheim C, 'Sources of Literature on Data Protection and Human Rights' (2001) 2 Journal of Information, Law and Technology 1
Williams L, 'Welfare and Legal Entitlements: The Social Roots of Poverty' in Kairys D (ed), *The Politics of Law: A Progressive Critique* (3rd edn, Basic Books 1998)
Williams LA, 'The Legal Construction of Poverty: Gender "Work" and the "Social Contract"' (2011) 22 Stellenbosch Law Review 463
Winner L, 'Do Artifacts Have Politics' (1980) 109(1) Modern Technology: Problem or Opportunity? 121
— 'Technology Today: Utopia Or Dystopia' (1997) 64(3) Social Research 989
Zalnieriute M, 'An International Constitutional Moment for Data Privacy in the Times of Mass Surveillance' (2015) 23 International Journal of Law and Information Technology 99
Zimmerman RK, 'The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century' (2000) 4 Journal of Legislation and Public Policy 439

OFFICIAL DOCUMENTS

African Union

African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) CAB/LEG/67/3
African Charter on the Rights and Welfare of the Child (adopted 11 July 1990, entered into force 29 November 1999) CAB/LEG/24.9/49
African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014) EX.CL/846(XXV)

European Union

Charter of Fundamental Rights of the European Union (signed 12 December 2007, took effect 1 December 2009) 2012/C 326/02
EU Directive 95/46/EC of 24 October 1995 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L281/31.
EU General Data Protection Regulation 2016/679 of 27 April 2016 of the European Parliament and of the Council 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 [2016] OJ L119/1.

MALAWI

Access to Information Act 13 of 2017 (16 February 2017) Malawi Gazette Supplement
Communications Act Chapter 68:01 Laws of Malawi
Criminal Procedure and Evidence Code Chapter 8:01 Laws of Malawi
Electronic Transactions and Cyber Security Act Chapter 74:02 Laws of Malawi
National Registration Act Chapter 24:01 Laws of Malawi
National Statistics Act Chapter 27:01 Laws of Malawi
Republic of Malawi (Constitution) Act No. 20 of 1994

SOUTH AFRICA

Constitution of the Republic of South Africa 1996
Protection of Personal Information Act 4 of 2013

UNITED NATIONS

Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III)
International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

CASE LAW

EUROPEAN UNION
František Ryneš v Úřad pro ochranu osobních údajů (2014) ECLI:EU:C:2014:2428

INTERNATIONAL CRIMINAL TRIBUNAL FOR RWANDA
The Prosecutor v Jean-Paul Akayesu (1998) Case ICTR-96-4-T

MALAWI
Gwanda v S Constitutional cause 5 of 2015 (unreported)
Kimu v Access Malawi Limited and others Commercial case 54 of 2011 (unreported)
Kishindo v Kishindo Civil cause 397 of 2013 (unreported)
Thomson v Lujeri Tea Estate Personal injury case 95 of 2015 (unreported)
Zimba v The Republic Miscellaneous criminal application 1 of 2004 (unreported)

UNITED STATES OF AMERICA
Olmstead v United States [1928] 277 United States 438

INTERNET SOURCES

Adanikin O, '2019 Election: How APC May Have Benefitted From NCC, INEC Breach Of Voters' Privacy' (*International Centre for Investigative Reporting*, 1 February 2019) <www.icirnigeria.org/2019-election-how-apc-may-have-benefited-from-ncc-inec-breach-of-voters-privacy/> accessed 16 October 2019

Aimeur E and Schonfeld D, 'The Ultimate Invasion of Privacy: Identity Theft' (Ninth Annual International Conference on Privacy, Security and Trust 2011) <www.site.uottawa.ca/~nelkadri/CSI5389/Papers/8-Aimeur_and_Schonfeld_PST2011.pdf> accessed 1 September 2019

Chatora A, 'Malawi Installs CCTV Cameras in Public Spaces to Fight Rampant Drugs Theft' (*This is Africa*, 10 November 2015) <https://thisisafrica.me/politics-and-society/malawi-installs-cctv-cameras-in-public-hospitals-to-fight-rampant-drugs-theft/> accessed 12 October 2019

CIPESA, 'Placing ICT Access for Persons with Disabilities at the Centre of Internet Rights Debate in Kenya' (*CIPESA*, 11 September 2019) <https://cipesa.org/2019/09/placing-ict-access-for-persons-with-disabilities-at-the-centre-of-internet-rights-debate-in-kenya/> accessed 12 October 2019

Clarke R, 'Introduction to Dataveillance and Information Privacy, Definition of Terms' (*Roger Clarke*, 24 July 2016) <www.rogerclarke.com/DV/Intro.html#InfoPriv> accessed 14 October 2019

Comninos A, 'Twitter Revolutions and Cyber Crackdowns: User-Generated Content and Social Networking in the Arab Spring and Beyond' (Association for Progressive Communications (APC) June 2011) <www.apc.org/sites/default/files/AlexComninos_MobileInternet.pdf> accessed 1 September 2019

Deloitte, 'Privacy is Paramount: Personal Data Protection in Africa' (*Deloitte*, 2017) <www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf> accessed 8 October 2019

Department of Immigration and Citizenship Services, 'Passport Process' (*The Department of Immigration and Citizenship Services*, 2018) <www.immigration.gov.mw/passports/passport-process/> accessed 11 October 2019

Dominique SM, 'Reforming the Content, Rather than Context, of the Chadian Constitution: Old Wine in a New Bottle?' (*ConstitutionNet,* 9 May 2018) <http://constitutionnet.org/news/reforming-content-rather-context-chadian-constitution-old-wine-new-bottle> accessed 6 September 2019

Easyapns, 'How to Monitor Someone's Whatsapp Messages from Mobile' (*Easyapns*, 17 December 2018) <www.easyapns.com/monitor-someones-whatsapp-messages/> accessed 12 October 2019

EMOTA, 'Lessons from Europe and Data Protection' (United Nations Conference on Trade and Development 2017) <https://unctad.org/meetings/en/Presentation/dtl_eWeek2017p13_OliverHateley_en.pdf> accessed 18 October 2019

Greenleaf G, 'Global Data Privacy Laws 2019: 132 National Laws and Many Bills' (2019) 157 Privacy Laws & Business International Report <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593> accessed 22 August 2019

— 'Global Tables of Data Privacy Laws and Bills' (2019) Supplement to 157 Privacy Laws & Business International Report <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3380794> accessed 22 August 2019

Government of Malawi, 'Malawi Economic Recovery Plan' (*eisourceboook*, 2013) <www.eisourcebook.org/cms/June%202013/Malawi,%20Economic%20Recovery%20Plan%202012.pdf> accessed 9 September 2019

— 'National ICT Master Plan 2014-2031' (*Malawi Diaspora*, 2014) <www.malawidiaspora.gov.mw/images/National-ICT-Master-Plan.pdf> accessed 8 October 2019

— 'The Malawi Growth and Development Strategy (2017-2022)' (*UNDP*, November 2017) <www.undp.org/content/dam/malawi/docs/UNDP_Malawi_MGDS)%20III.pdf> accessed 9 September 2019

Handforth C and Wilson M, 'Digital Identity Country Report: Malawi' (GSMA 2019) <www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report.pdf> accessed 26 September 2019

Heijmans P, 'Getting the Business Over Data Privacy' (*US News*, 1 August 2018) <www.usnews.com/news/best-countries/articles/2018-08-01/across-europe-new-data-privacy-law-still-leaves-confusion> accessed 20 October 2019

Hemeson CJ, 'Directive on Consumer Data for SIM Card Registration in the Telecommunications Sector: An African Perspective' (*SSRN*, 8 January 2012) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1982033> accessed 19 August 2019

Home Office, 'Country Information and Guidance Ethiopia: People of Mixed Eritrean/Ethiopian Nationality' (*Refworld*, 2016) <www.refworld.org/pdfid/57c6daf84.pdf> accessed 15 October 2019

Kainja J, 'Privacy and Personal Data Protection: Challenges and Trends in Malawi' (CIPESA September 2018) <https://cipesa.org/?wpfb_dl=300> accessed 20 August 2019

— 'Are Malawians Sleep-Walking into a Surveillance State?' (*CIPESA*, 12 August 2019) <https://cipesa.org/2019/08/are-malawians-sleep-walking-into-a-surveillance-state/> accessed 10 October 2019

Karombo T, 'Zimbabwe's First Ever Election Without Robert Mugabe Has Turned into a Data Privacy Minefield' (*Quartz Africa*, 11 July 2018) <https://qz.com/africa/1325485/zimbabwe-elections-whatsapp-sms-spam-data-privacy-concerns-for-mnangagwa-chimasa/> accessed 16 October 2019

Khamula O, 'Malawi to Have CCTV Cameras in Public Places: More Benefits from India-Africa Business Meeting' (*All Africa*, 27 March 2018) <https://allafrica.com/stories/201803270477.html> accessed 11 October 2019

Liberty Health, 'Privacy statement' (*Liberty Health*) <www.libertyhealth.net/malawi/en/privacy-statement/> accessed 16 October 2019

Lindert KA and others, 'Rapid Social Registry Assessment: Malawi's Unified Beneficiary Registry' (World Bank November 2018) <http://documents.worldbank.org/curated/en/363391542398737774/Rapid-Social-Registry-Assessment-Malawis-Unified-Beneficiary-Registry-UBR> accessed 26 September 2019

Magnuson B, Branam S and Ettinger P, 'Threading the Needle: Harmonising Global Privacy Practices' (presented at IAPP Global Privacy Summit 2019) <https://iapp.my.salesforce.com/sfc/p/#1a000000HSGV/a/1P0000000HSl/6TfRQ7b.qUuXkLfSnbqtfGnHtPFrqOptcdTy.pqAfPc> accessed 18 October 2019

Ministry of Finance, Economic Planning and Development, 'Economic Development Document for Malawi' (*IMF*, May 2017) <www.imf.org/en/Publications/CR/Issues/2017/07/05/Malawi-Economic-Development-Document-45037> accessed 9 September 2019

Muheya G, 'Malawi rolls out "spy machine": Macra can now listen to people's phone conversation' (*Nyasa Times*, 24 January 2018) <www.nyasatimes.com/malawi-roll-spy-machine/> accessed 23 September 2019

Munthali A, 'A Situation Analysis of Persons with Disabilities in Malawi' (*Medbox*, 2011) <www.medbox.org/a-situation-analysis-of-persons-with-disabilities-in-malawi/download.pdf> accessed 12 October 2019

Mussa R, 'Poverty and Inequality in Malawi: Trends, Prospects, and Policy Simulation' (MPRA 2017) <https://mpra.ub.uni-muenchen.de/75979/1/MPRA_paper_75979.pdf> accessed 27 September 2019

Mussa R and Masanjala WH, 'A Dangerous Divide: The State of Inequality in Malawi' (Oxfam 2015) <www-cdn.oxfam.org/s3fs-public/file_attachments/rr-inequality-in-malawi-261115-en.pdf> accessed 27 September 2019

Mutung'u G, 'The Influence Industry: Data and Digital Election Campaigning in Kenya' (*Our Data Our Selves*, June 2018) <https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-kenya.pdf> accessed 22 August 2019

Nation Online, 'Benefits of the New System' (*The Nation*, 1 July 2015) <https://mwnation.com/benefits-of-the-new-system-2/> accessed 11 October 2019

National Bank of Malawi, 'Know Your Customer Detail Update Form' (*National Bank of Malawi*) <https://natbank.co.mw/forms/download-forms/know-your-customer-kyc-detail-update-form/188-know-your-customer-kyc-detail-update-form/file> accessed 1 September 2019

National Economic Council, 'Vision 2020: the National Long-Term Development Perspective for Malawi' (CEPA 2000) <https://cepa.rmportal.net/Library/government-publications/Vision%202020-%20The%20National%20Long%20Term%20Development%20Perspective%20for%20Malawi.pdf> accessed 26 September 2019

National Statistical Office, 'Survey on Access and Usage of ICT Services in Malawi' (MACRA June 2015) <www.macra.org.mw/wp-content/uploads/2014/09/Survey_on-_Access_and_Usage_of_ICT_Services_2014_Report.pdf> accessed 18 August 2019

— '2018 Malawi Population and Housing Census Report' (NSO Malawi 2019) <www.nsomalawi.mw/images/stories/data_on_line/demography/census_2018/2018%20Malawi%20Population%20and%20Housing%20Census%20Main%20Report.pdf> accessed 23 August 2019

NICO Life Insurance Company Limited, 'Personal Details for New Policy Application' (*NICO Life*) <www.nico-life.com/index.php/download-forms/individual-products/12-personal-details-for-new-policy-application/file> accessed 1 September 2019

Nthondo J, 'FDH Bank Integrates Malawi National ID System Through NRB System' (*Nyasa Times*, 8 June 2019) <www.nyasatimes.com/fdh-bank-integrates-malawi-national-id-system-through-nrb-system/> accessed 12 October 2019

Nyamu-Musembi C and Cornwall A, 'What is the "Rights-Based Approach" All About? Perspectives from International Development Agencies' (Institute of Development Studies working paper series 234 2004) <http://opendocs.ids.ac.uk/opendocs/handle/123456789/4073#.Vc2TC7Vu6Wg> accessed 15 October 2019

Nyasa Times, 'Lomwe Becomes Buzz Word for Malawi's Employment, Business' (*Nyasa Times*, 3 August 2009) <www.nyasatimes.com/lomwe-becomes-buzz-word-for-malawis-employment-business/> accessed 12 October 2019

Palmer N, 'ICT for Data Collection and Monitoring and Evaluation' (FAO June 2012) <www.fao.org/3/aq003e/aq003e.pdf> accessed 7 October 2019

Parliament of Malawi, 'E-Bill' (*biz-file*, 2012) <https://biz-file.com/f/1210/Malawi_E-Bill_Draft_2012.doc> accessed 14 October 2019

Privacy International, 'Africa: SIM Card Registration Only Increases Monitoring and Exclusion' (*Privacy International*, 5 August 2019) <www.privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion> accessed 16 October 2019.

— 'Data and Elections' (*Privacy International*) <https://privacyinternational.org/learning-topics/data-and-elections> accessed 16 October 2019

— 'ID, Identity and Identification' (*Privacy International*) <www.privacyinternational.org/what-we-do/id-identity-and-identification> accessed 16 October 2019

Qiang X, '"Dataveillance" in Xi Jinping's "Brave New China"' (*Power3.0*, 26 April 2018) <www.power3point0.org/2018/04/26/dataveillance-in-xi-jinpings-brave-new-china/> accessed 1 September 2019

Rasmussen PE, '2018 African Economic Outlook: Malawi' (AFDB 2018) <www.afdb.org/fileadmin/uploads/afdb/Documents/Generic-Documents/country_notes/Malawi_country_note.pdf> accessed 23 September 2019

Sangala T, '3 Arrested for Mec Break-in' (*The Times*, 13 May 2019) <https://times.mw/3-arrested-for-mec-break-in/> accessed 11 October 2019

Simitis S, 'Revisiting Sensitive Data' (1999) <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806845af> accessed 15 October 2019

South Africa Law Reform Commission, 'Privacy and Data Protection Report' (The Department of Justice and Constitutional Development 2009) <www.justice.gov.za/salrc/reports/r_prj124_privacy%20and%20data%20protection2009.pdf> accessed 2 October 2019

United Nations High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age' (*UN Docs*, 3 August 2018) <https://undocs.org/A/HRC/39/29> accessed 16 October 2019

United Nations Human Rights Committee, 'General Comment 16: Article 17 (right to privacy), the right to respect of privacy, family home and correspondence, and protection of honour and reputation' (1988) 8 April 1988, HRI/GEN/1/Rev.9 (Vol. I) <www.refworld.org/docid/453883f922.html> accessed 15 October 2019

Veen S van, Cansfield B and Muir-Bouchard S, '"Let's Stop Thinking Its Normal": Identifying Patterns in Social Norms Contributing to Violence Against Women and Girls Across Africa, Latin America and the Caribbean and the Pacific' (Oxfam 2018) <www-cdn.oxfam.org/s3fs-public/file_attachments/rr-lets-stop-thinking-normal-evaw-social-norms-251118-en.pdf> accessed 12 October 2019

Warren R, 'Cycle of Shame: Harassed in the Street, Then Again on Social Media' (*CNN*, 2018) <https://edition.cnn.com/2018/01/08/africa/malawi-cycle-of-shame-asequals/index.html> accessed 12 October 2019

Wiley J, 'The Globalisation of Technology to Developing Countries' (*Digital Commons*, 4 August 2009) <http://digitalcommons.providence.edu/glbstudy_students/3> accessed 18 August 2019

World Bank, 'World Development Indicators 2013' (World Bank 2013) <https://openknowledge.worldbank.org/handle/10986/13191> accessed 26 September 2019

— 'Digitizing Malawi for a Brighter Digital Future' (*World Bank*, 5 June 2017) <www.worldbank.org/en/news/press-release/2017/06/05/digitizing-malawi-for-a-brighter-digital-future> accessed 8 October 2019

— 'GINI Index' (*World Bank*, 2017) <https://data.worldbank.org/indicator/si.pov.gini> accessed 26 September 2019

— 'The World by Income and Region' (*The World Bank Data Topics*, 2017) <http://datatopics.worldbank.org/world-development-indicators/the-world-by-income-and-region.html> accessed 23 August 2019

— 'European Union' (*World Bank*) <https://data.worldbank.org/region/european-union> accessed 20 October 2019

— and National Statistics Office of Malawi, 'Methodology for Poverty Measurement in Malawi (2016/17)' (World Bank 2018) <http://documents.worldbank.org/curated/en/575101534874113572/Methodology-for-Poverty-Measurement-in-Malawi> accessed 27 September 2019

World Economic Forum, *The Global Gender Gap Report* (World Economic Forum 2017) <www3.weforum.org/docs/WEF_GGGR_2017.pdf> accessed 11 October 2019

OTHER SOURCES

Abdulrauf LA, 'The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa' (LLD thesis, University Of Pretoria 2015)

Enyew AB, 'Regulatory Regime on the Protection of Privacy and Personal Information in Ethiopia' (LLM thesis, University of Oslo 2009)

Kent AM, 'An Investigation on How Employee's Use of Internet at Workplace has Impacted Employee's Performance – A Case Study of Telekom Networks Malawi Limited (TNM)' (Bsc thesis, Malawi College of Accountancy 2016)

Makulilo AB, 'Protection of Personal Information in Sub-Saharan Africa' (Dr Jur thesis, University of Bremen 2012)

Mkandawire E, 'Socialisation of Malawian Women and the Negotiation of Safe Sex' (Msc thesis, University of Pretoria 2012)

Global Campus of Human Rights

Monastery of San Nicolò
Riviera San Nicolò, 26
I-30126 Venice Lido (Italy)

www.gchumanrights.org

Global Campus of Human Rights

The Global Campus of Human Rights is a unique network of more than one hundred participating universities around the world, seeking to advance human rights and democracy through regional and global cooperation for education and research. This global network is promoted through seven Regional Programmes which are based in Venice for Europe, in Sarajevo/Bologna for South East Europe, in Yerevan for the Caucasus, in Pretoria for Africa, in Bangkok for Asia-Pacific, in Buenos Aires for Latin America and the Caribbean, and in Beirut for the Arab World.

The Global Campus Awarded Theses

Every year each regional master's programmes select the best master thesis of the previous academic year that is published online as part of the GC publications. The selected seven GC master theses cover a range of different international human rights topics and challenges.

The present thesis - *Right to Data Privacy in the Digital Era: a Critical Assessment of Malawi's Data Privacy Protection Regime* written by **Chisomo Nyemba** and supervised by Akinola E Akintayo, University of Lagos - was submitted in partial fulfillment of the requirements for the Master's Programme in Human Rights and Democratisation in Africa (HRDA), coordinated by Centre for Human Rights, University of Pretoria.

This document has been produced with the financial assistance of the European Union and as part of the Global Campus of Human Rights. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or of Global Campus of Human Rights