PRIVACY AND DATA PROTECTION IN EHEALTH IN AFRICA

AN ASSESSMENT OF THE REGULATORY FRAMEWORKS THAT GOVERN PRIVACY AND DATA PROTECTION IN THE EFFECTIVE IMPLEMENTATION OF ELECTRONIC HEALTH CARE IN AFRICA: IS THERE A NEED FOR REFORM AND GREATER REGIONAL COLLABORATION IN REGULATORY POLICYMAKING?

by

Beverley Alice Townsend
BA LLB LLM Higher Dip. in Tax Law LLM (with distinction)

BNTBEV001

Thesis presented for the degree of DOCTOR OF PHILOSOPHY in the Faculty of Law UNIVERSITY OF CAPE TOWN

Date of submission: March 2017

Supervisor: Professor Alistair Price, University of Cape Town

DECLARATION

"This thesis has been submitted to the Turnitin module (or equivalent similarity and originality checking software) and I confirm that my supervisor has seen my report and any concerns revealed by such have been resolved with my supervisor."

Name: Beverley Alice Townsend

Student number: BNTBEV001

Signature: Signed by candidate

Date: 24/02/2017

ABSTRACT

This thesis examines and evaluates the legal protection of privacy and personal data in South Africa and across Africa in the electronic health care industry, that is, where medical services are provided to individuals by way of networked technological platforms including mobile telephones. This thesis presents a critical understanding of, and pragmatic solution to, the questions that lie at the intersection of the following: an individual's right to privacy and data protection, cultural disparities when defining privacy, the emergence of electronic health care, the sensitivity of health related data, the need for health care in areas, where lack of resources and lack of accessibility are often commonplace, and the introduction of networked technologies within the health care system as a solution.

Firstly, eHealth services and applications are described. Secondly, notions of privacy and data protection are considered. Thirdly, the prevailing legal determinants that form the basis of African and South African data protection regulatory measures are ascertained. Fourthly, selected illustrations are presented of the practical implementation of eHealth services and certain recent influencers within the digital environment, which may inform the future eHealth privacy regulatory framework. Finally, criticisms of the Malabo Convention are presented and recommendations advanced.

As there is limited guidance with regard to policymaking decisions concerning privacy and data protection in the implementation of eHealth in developing countries, possibilities for reform are suggested. These will allow a more careful balance between, on the one hand, the normative commitment to providing accessible health care using electronic means and, on the other, the rights to privacy and data protection of the user, which require safeguarding within an African context.

In proposing a solution, it is argued that adequate privacy regulation of electronic health must (1) be sensitive to societal and cultural differences in what is considered private, (2) be responsive to rapid technological transformation in healthcare industries, and (3) build user confidence in data protection in this context, to enable nascent electronic health initiatives to reach their potential in Africa.

It is proposed that the adoption of an accepted social imperative protected by a powerful triumvirate of ethical constraints, effective legal provisions and regulations, and operational necessities, is possible. Greater regulatory collaboration across the

continent is called for based on harmonised domestic and international laws, national policies, and industry codes of conduct that are sensitive to local conditions and challenges.

ACKNOWLEDGEMENTS

I am most grateful to my supervisor, Professor Alistair Price, for his support, guidance and encouragement. It was a huge honour and pleasure to learn from him. I wish to thank my family for their love and never-ending belief in me, sometimes against insurmountable odds. In particular, I wish to thank my husband, Craig, for his unwavering confidence in me and for being my greatest inspiration. My darling children, Alice and Elizabeth, I thank for their devotion and patience.

TABLE OF CONTENTS

LIST OF ACRONYMS

AFAPDP	- Association francophone des autorités de protection des données personnelles
AIDS	- Acquired Immune Deficiency Syndrome
ART	- Anti Retroviral Treatment
ATA	- American Telemedicine Association
CJEU	- Court of Justice of the European Union
DOH	- Department of Health
DOTS	- Directly Observed Treatment Short Course
EAC	- East African Community
ECA	- Economic Commission of Africa
ECCAS	- Economic Community of Central African States
ECOWAS	- Economic Community of West African States
ECT	- Electronic Communications and Transactions Act 25 of 2002
ECHR	- European Court of Human Rights
EMS	- Emergency Medical Services
EPR	- Electronic Patient Record
EU	- European Union
GSMA	- Groupe Speciale Mobile Association
HIV	- Human Immunodeficiency Virus
HPCSA	- Health Professions Council of South Africa
ICESR	- International Covenant on Economic and Social Rights
ICT	- Information and Communications Technology
IT	- Information Technology
ITU	- International Telecommunication Union
LAN	- Local Area Network
MRC	- Medical Research Council
NESC	- National e-Health Steering Committee
NHC	- National Health Council
NHI	- National Health Insurance
NHIS/SA	- National Health Information System of South Africa
OAU	- Organization of African Unity

OECD	- Organization for Economic Cooperation and Development
PAIA	- Promotion of Access to Information Act No.2 of 2000
POPI	- Protection of Personal Information Act No. 4 of 2013
SADC	- Southern African Development Community
SMS	- Short Message Service
UN	- United Nations
UNCITRAL	- United Nations Commission on International Trade Law
UNCTAD	- United Nations Conference on Trade and Development
UNESCO	- United Nations Educational, Scientific and Cultural Organization
UNICEF	- United Nations International Children's Emergency Fund
WHA	- World Health Assembly
WHO	- World Health Organization
WMA	- World Medical Association

CHAPTER 1: STATING THE PROBLEM

O my body, make of me always a man who questions!

Black Skin, White Masks. Frantz Fanon

I INTRODUCTION

The provision of health care in Africa today faces many challenges, including a shortage of health care resources, an increased burden of disease, a large proportion of the population living in rural areas, and a lack of education and primary health care.[1] Illness and death in developing countries are often due to health conditions that are preventable and for which medical solutions are known and easily implemented.[2] Advances in information communication technology over the past few years have provided an alternative and attractive method of health care delivery in the form of electronic health (eHealth).

Although increasing in popularity and of enormous benefit, eHealth has created potential ethical and legal challenges to regulators, both internationally and in Africa. Safeguarding privacy is an issue plaguing the successful implementation of eHealth.[3]

As there is limited guidance to direct regulatory decisions with regard to privacy and data protection in the implementation of eHealth in developing countries[4], the intention of this thesis is to arrive at a clearer understanding of the broader legal narrative, while suggesting possibilities for regulatory reform, which may allow greater inclusion and collaboration in adequately safeguarding privacy rights within the African region.

---

[1] WHO 'World Health Statistics: 2012' (2012); M Mars and C Seebregts 'Country Case Study for eHealth: South Africa' (2008) *Rockefeller Foundation* at 1.

[2] A Le Roux 'Telemedicine: A South African legal perspective' (2008) (1) *TSAR* at 99 and M Kekana, B Mkhize and P Noe 'The practice of telemedicine and challenges to the regulatory authorities.' (2010) 3 (1) *South African Journal of Bioethics and Law* at 33.

[3] C Erwell 'Telemedicine: overcoming obstacles on the road to global health care' (2003) *International Trade Law Journal* 68 at 69; S Fox and L Rainie 'The online health care revolution' *Pew Internet & American Life Project: Online Report* (2000) at 1.

[4] N Leon *et al.* 'Applying a framework for assessing the health system challenges to scaling up mhealth in South Africa' (2013) 12 *BMC Medical Informatics and decision making* at 123.

II THE PREDICAMENT: THE DIGITAL ENVIRONMENT AND EHEALTH DATA PROTECTION

This thesis commences by stating the predicament arising in privacy and data protection brought about by the recent emergence of health care applications in the digital order within Africa.

The predicament is set out as follows. Firstly, strides in technological development and wider use of the electronic environment have advanced new threats to its users. The rights to privacy and data protection have been placed at risk by emerging technological processes. These emerging threats cannot be easily and suitably overcome by historical legal remedies and require additional and/or alternative resolution measures. The question is how are these potential violations to privacy rights to be safeguarded against in the provision of much-needed eHealth in developing countries, such as those found in Africa?

In light of the borderless nature of the threat, the inference drawn is that any resolution cannot be achieved in isolation. The challenges lie in the disparity between the evolving norms both internationally and regionally, the significant and rapid acceleration of technological progress, and the practical incorporation of such norms at a national level.

Within this context, the aim is to provide a pragmatic solution that is appropriate within an African context by the proposed engagement of legal, regulatory and policymaking measures. Insight is thus provided in this thesis, aimed at informing regulatory governance and ensuring that the delicate balance between the normative commitment to provide adequate and accessible health care, on the one hand, and the right to privacy and data protection of the user, on the other, is safeguarded within a uniquely African context.

For illustrative purposes, the position of privacy and data protection within South Africa is considered. South Africa is a useful example of how data protection regulation may be implemented on a domestic level and is used as a case study as it mirrors many of the issues found within the African region as a whole. Consideration of the position found in South Africa is a worthwhile endeavour as privacy is protected by a multi-facetted approach, that is, by virtue of the law of delict, by means of a protected right of privacy enshrined in the Constitution, and by provisions in

general or specific privacy and data protection legislation. These means of protection run concurrently within the legal system and, rather than existing independently, their convergence and mutual interaction can serve to strengthen any consequential privacy protection. South Africa is, however, merely used to illustrate certain challenges experienced in the domestic implementation of data protection regulation within a health care environment and is not an attempt to provide a complete solution within the country itself or within the African continent as a whole.

The argument postulated in this thesis is that contemporary digital and health care expansion precludes the adherence to suppositions of strict self-reliance and detachment. The proposition is that an exercise in slavish adherence to autonomous self-determination by sovereign nations may very well prove ineffectual. Rather, a multi-layered approach combining various regulatory measures is a more viable solution. It is suggested further that an overly simplistic generalisation about Africa may be averted by way of a layered approach to regulation.

III THE STRUCTURE OF THE ARGUMENT

Firstly, this thesis examines and defines eHealth services and applications and the essence of privacy and data protection in Chapters 2 and 3. The prevailing legal determinants forming the basis of African and South African data protection regulatory measures are ascertained in Chapters 4 and 5. Chapter 6 sets out selected illustrations of the practical implementation of eHealth services and identifies certain recent influencers, or drivers, within the digital environment, which may inform future eHealth privacy and data protection regulatory frameworks. Chapters 7, 8 and 9 present criticisms of the Malabo Convention and possible solutions and recommendations.

IV SCOPE AND DESCRIPTION OF THE TERMS 'AFRICA' AND 'AFRICAN'

The purpose of this thesis is not to analyse class structures across 55 African nation-states as to do so is not feasible. Instead, the thesis assesses and proposes

improvements to the regional and national regulation of privacy and data protection in the context of eHealth provision within the African continent as a whole.[5]

In this thesis, 'Africa' is used to describe the 55 sovereign states that have ratified or acceded to the Constitutive Act of the African Union. This is done primarily as I seek to understand the influence of certain regional and sub-regional data protection instruments, specifically those of the African Union and its most recently promulgated Convention on Cyber Security and Personal Data Protection ('the Malabo Convention'). I acknowledge that it is problematic to treat Africa as a single homogeneous entity as it is a continent of great diversity. As stated by Ryszard Kapuściński when describing Africa: *'The continent is too large to describe. It is a veritable ocean, a separate planet, a varied, immensely rich cosmos. Only with the greatest simplification, for the sake of convenience, can we say "Africa". In reality, except as a geographical appellation, Africa does not exist*'.[6] However, this thesis addresses a shared problem in the region of Africa, and for reasons of necessity, generalisations where justified by the available facts are unavoidable. Importantly, the solution the thesis proposes is a regional effort to tackle the problem identified in the thesis, including harmonising regional laws which can then be adopted by states with appropriate modifications taking account of varying conditions in particular countries.

'African' is used to denote people who originated on the African continent. Using the phrase an 'African perspective' is not meant to imply that it is the perspective of all indigenous people, but only to designate the normative thought common amongst those people in Africa. Likewise, using the term 'Western' denotes the normative thought of those in the West, that is, predominately in Europe and America. Using a geographical term to connote a certain idea does not suggest that all people in that geographical area accept the idea or perspective, nor that no one outside of that area does. It merely means that the idea or perspective is prevalent in that area to a noticeable extent, relative to other places in the world. The importance of privacy and protecting personal data is the foundation on which the thesis's argument is

[5] Africa is a vast continent consisting of 55 sovereign states recognised by either the AU or the UN or both, 9 territories and 2 *de facto* independent states with limited recognition. The member states of the African Union are the 55 sovereign states that have ratified or acceded to the Constitutive Act of the African Union.

[6] Ryszard Kapuściński writes of Africa in his book *The Cobra's Heart:* extracted from the author's book *The Shadow of the Sun* (2007).

built. The raison d'être of the thesis's argument is to assess and make proposals regarding the protection of privacy and personal data in African societies.

V ARGUMENT

In this thesis, I shall argue that:

(a) with the emergence and increased accessibility of the Internet and, particularly, social media, the development of mobile (mHealth) and electronic health (eHealth) is an inevitability;[7]

(b) a health care crisis looms in many developing countries, including in South Africa, and eHealth as a potential platform for the distribution of health care services provides an attractive, alternative or complementary solution;[8]

(c) various legal barriers to the implementation of eHealth exist, including more specifically violations of one's right to privacy and data protection;

(d) the right to privacy is an elusive concept worthy of debate;

(e) in exploring the notion of privacy, the cultural and contextual sensitivities that arise in certain countries and the great influence and importance of traditional indigenous laws should be considered;

(f) recent international developments in data protection regulatory frameworks make valuable contributions to the debate;

(g) the regulatory framework within the African region governing data protection is documented in this thesis;

(h) emerging trends in medical and technological development, although hugely beneficial to the service delivery of health care in developing countries, have created additional regulatory challenges, with regard to cross-jurisdictional data mobility and data protection;

---

[7] 'eHealth' is electronic health and 'mHealth' is mobile health; both are defined in greater detail in Chapter 2.

[8] See L Schoeman 'Embracing e-government: In search of accountable and efficient governance objectives that improve service delivery in the South African health sector' (2007) 42 (5) *Journal of Public Administration* 183 at 184.

(i) it is therefore necessary to advance a range of approaches, which may wholly or partially transform the existing regulatory environment into one that is better suited to a technologically enabled health system;

(j) the law within South Africa can be used as an illustration of an effective African position regarding data protection developments. This is because South African law is an approach that can be duplicated or emulated in other African countries;

(k) the Malabo Convention, although positive in many respects, fails to address the rapid development of eHealth with regard to the protection of sensitive medical data and issues of consent in developing countries;

(l) a means of protecting an individual's right to privacy and to control the use of their personal information is to adopt a multidisciplinary and multifaceted approach to data protection regulation;[9]

(m) while it is imperative, on the one hand, to remain part of the international information community and to ensure that data can be freely and easily exchanged, it is necessary, on the other hand, to appreciate the difficulty of implementing internationally adopted eHealth privacy regulations mindlessly within an African context;

(n) the determination is to provide a solution that is appropriate, equitable and beneficial to developing countries whilst upholding human rights;

(o) additionally, it is acknowledged that there exists a need for greater standardisation and harmonisation of data protection laws within the African region, which would require greater co-operation between African nations;

(p) and finally, on a practical and doctrinal level, it is proposed that there is a need for a more collaborative, inclusive, pragmatic regional approach to policymaking.

VI METHODOLOGY

This thesis relies on research conducted using published materials. These include international organisations treaties, declarations, resolutions, recommendations; policy documents, statements and guidelines; reports of investigations; submissions

[9] See A Roos 'Core principles of data protection law' (2006) 39 *CILSA* at 102.

and proposals to the organisations; minutes and reports of meetings; Special Rapporteur reports; General Comments; and reported cases. Domestic government materials including statutes, regulations, policy documents, and reported cases. Non-governmental organisation reports; policy documents; public statements and press briefings were considered. The main secondary sources relied upon include books, journals, newspaper and online articles, research reports and theses.

VII CONCLUSION

In this chapter, I have set out the predicament and argument to be presented in this thesis. The structure of the argument to be followed has been outlined. In Chapter 2, I shall describe the nature, scope and benefit of eHealth.

CHAPTER 2: DEFINITION AND BENEFIT OF E-HEALTH

Science never solves a problem without creating ten more.[1]

George Bernard Shaw

[1] 'The doctor's dilemma' (2003) 32 (6) *International Journal of Epidemiology* 910–5.

I INTRODUCTION

Chapter 2 begins by defining the concept of eHealth. The nature and scope of eHealth and its benefits are examined in greater detail. Thereafter, the health care position of developing countries and the challenges faced are discussed, specifically with regard to what has been described as a health care crisis.[2] As equitable access to health care should be a highly desirable goal of most states, the merits of alternative, or supplementary, methods of addressing health care delivery are explored.

By referring to the examples of the Ebola outbreak in West Africa and the use of mobile text messages, two potentially conflicting themes are explored: the right to privacy and data protection, on the one hand, and the right to access health care through the promising phenomenon of eHealth, on the other. Finally, a barrier to the development of eHealth is examined, that is, safeguarding user privacy and data protection.

II EHEALTH DEFINED

When Archbishop Tutu[3] was asked whether eHealth could narrow the divide in social inequality across the world, he responded:

> '[t]echnology is a major driving force of our civilisation …[w]hat we need is a paradigm shift from information and communications technologies for health to a greater emphasis on information and communications technologies for development, which benefit health but also have an effect on education, agriculture, commerce, governance and other social determinants of health. What the poor and the vulnerable people need is not only good lives but good health as well'.[4]

In the following sections, eHealth, mHealth (i.e. mobile health), telemedicine and cyber-medicine will be described in turn. Although no universally accepted

---

[2] 'Reforming healthcare in South Africa' (2011) Report 18 *Centre for Development and Enterprise* at 7.

[3] Archbishop Desmond Tutu speaking at the Global eHealth Ambassadors Program of the International Society for Telemedicine and eHealth.

[4] WHO 'The bigger picture for e-health' (2012) 90 (5) *Bulletin of the World Health Organization* 321–400.

definition exists,[5] eHealth (or electronic health) is a broad term encompassing the use of all information and communications technologies with the aim of delivering health care services and information from a distance.[6] eHealth is thus an overarching concept incorporating mHealth, telemedicine, and cyber-medicine.

The objective of eHealth is to optimise both efficiency and quality in the provision of health care and, generally, to improve patients' quality of care.[7] eHealth seeks to dismantle the barriers of traditional health care support and to facilitate access to health services for all people, regardless of their geographical location.[8] It describes online applications and communication technologies, which traverse a range of activities and services within the health care sector.[9] The WHO defines eHealth as:

> 'the cost-effective and secure use of information and communications technologies in support of health and health-related fields, including health care services, health surveillance, health literature, and health education, knowledge and research'.[10]

eHealth exists at the intersection of 'medical information, public health and business'[11] and is a means of improving the quality of service delivery, especially in primary health care.[12] It comprises four interrelating categories: (a) clinical information systems, (b) telemedicine and homecare, (c) integrated regional/national health information, and (d) secondary usage non-clinical systems.[13]

---

[5] BM Kalema and MR Kgasi 'Leveraging E-health for Future-oriented Healthcare Systems in Developing Countries' (2014) 65 (8) *The Electronic Journal of Information Systems in Developing Countries* at 3.

[6] WMA 'Statement on Guiding Principles for the Use of Telehealth for the Provision of Health Care' (2009). See also A Le Roux 'Telemedicine: A South African legal perspective' (2008) 1 *TSAR* 99 at 100.

[7] Kalema and Kgasi (n 5) at 1.

[8] Ibid.

[9] S Callens and K Cierkens 'Legal aspects of eHealth' (2008) 141 *Stud Health Technology Information* 47–56.

[10] WHO (n 4) at 321.

[11] WHO 'WHA58.28 e-health' (2005).

[12] Ibid.

[13] eHealth Taskforce Report 'Accelerating the Development of the eHealth Market in Europe' (2007) *European Union eHealth Taskforce Report* at 10.

In an attempt to provide a definitive description of eHealth, Hans *et al.* undertook a systematic review of published, suggested, or proposed definitions of eHealth.[14] They conducted a qualitative analysis of these definitions of eHealth with regard to content and emerging themes, as gleaned from documents, articles, references and websites.[15] They found that, of the 51 unique definitions retrieved, although a wide range of themes were found, 'no clear consensus' about the meaning of the term eHealth could be established. Nevertheless, two universal themes were consistent, that of, 'health' and 'technology'.[16] The conclusion drawn was that, although the use of the term eHealth is 'widespread', there is a 'tacit understanding' of the meaning of the term.[17] As is the case with most neologisms, it is often problematic to establish the precise meaning of the term, with the meaning frequently transient and varying according to the context within which it is used. eHealth thus characterises 'virtually everything related to computers and medicine'.[18] Eysenbach defines eHealth as:

> '… not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology'.[19]

eHealth thus involves the use of online, digital and related information systems and technology in all aspects of health care.[20] Common themes included in

---

[14] OH Hans, C Rizo, M Enkin and A Jadad 'What Is eHealth (3): A Systematic Review of Published Definitions' (2005) 7 (1) *Journal of Medical Internet Research* at e1.

[15] A total of 1209 abstracts were scanned and 430 citations reviewed from various bibliographic databases.

[16] Hans *et al.* (n 14) at e1.

[17] Ibid.

[18] G Eysenbach 'What is e-health?' (2001) 3(2) *Journal of Medical Internet Research* at e20.

[19] Ibid.

[20] JE Orlikoff and MK Totten 'Trustee workbook 3. E-health and the board: the brave new world of governance Part 1' (2000) 53 (7) *Trustee* at 4.

the definition are health, health care[21] or health care delivery,[22] and the use of communications technology, either explicitly or implicitly.[23]

mHealth (or mobile health) is a component of eHealth.[24] mHealth is a 'medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants and other wireless devices'.[25] It is the utilisation of mobile devices to improve 'health outcomes, health care services, and health research'.[26] mHealth comprises health care practices supported by mobile devices.[27] When linked to the Internet and other social network platforms, mobile telephone functionality extends beyond mere one-to-one voice communication and instant messaging.[28] Mobile technology has enabled instant wireless connectivity and enabled users to communicate in real time, and gain access to Internet-based software applications, in a way that was not previously possible.[29] Consequently, mHealth has emerged as a rapidly expanding technology platform for transforming electronic health care.[30] It uses wireless technologies, for instance, Bluetooth, GSM/GPRS/3G, WiFi, and WiMAX, to transmit health data and facilitate health care services. These applications are accessed through devices such as mobile telephones, voice recorders, patient monitoring devices, Smartphones, personal digital

---

[21] 'Health care' is defined in Medical-dictionary.com as '[t]he prevention, treatment, and management of illness and the presentation of mental and physical well being through the services offered by the medical and allied health professions'.

[22] Hans *et al.* (n 14) at e1.

[23] Ibid.

[24] CZ Qiang, M Yamamichi, V Hausman and R Miller 'Mobile applications for the health sector' (2012) at 21. See also WHO 'mHealth: New horizons for health through mobile technologies' in the second *Global Observatory for eHealth Series* vol 3 (2011) at 6.

[25] Ibid.

[26] K Congdon 'The rise of mHealth' (2013) *Health IT Outcomes*.

[27] WHO (n 24) at 6.

[28] E Edouard and L Edouard 'Application of information and communication technology for scaling up youth sexual and reproductive health' (2012) 16 (2) *African Journal of Reproductive Health* at 197.

[29] AO Adesina, KK Agbele, K Kehinde, R Februarie, AP Abidoye and HO Nyongesa 'Ensuring the security and privacy of information in mobile health-care communication systems' (2011) 107 (9–10) *South African Journal of Science* at 4.

[30] M Mars and C Jack 'Why is telemedicine a challenge to the regulators? (2010) 3 (2) *SAJBL* 55 at 56.

assistants, sensor gadgets, laptops or tablet computers.[31] Medical information is then uploaded and stored on various mHealth electronic storage devices.[32]

The term 'telemedicine' has been applied in various forms since the early 1960s and has continued to develop steadily in scope and application.[33] The WHO defines telemedicine as:

> '[t]he delivery of health services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health providers, all in the interests of advancing the health of individuals and their communities'.[34]

Telemedicine is the practice of health care delivery, consultation, diagnosis and treatment, education, and the transfer of medical data[35] that is carried out 'at a distance'.[36] Telemedicine interactions are frequently between a host and a remote site and telemedicine describes a 'technique' for health care delivery rather than any one specific technology.[37] Telemedicine is provided in real time, interactively between the participants, using data, voice or video, for instance, or by making use of ancillary technological diagnostic tools, such as electronic stethoscopes.[38]

Telemedicine is categorised into either 'store-and-forward' telemedicine or 'face-to-face' telemedicine. 'Store-and-forward', or asynchronous telemedicine, is used for non-emergency situations where the eHealth consultation is made within 24 – 48 hours. The patient's data and accompanying images or sound files (usually x-rays, CT scans or MRI) are transmitted by secure e-mail or website to a colleague health practitioner, who then reviews the data and provides a diagnosis, advice and/or a

---

[31] Adesina *et al.* (n 29) at 4.

[32] R Wootton, NG Patil, RE Scott and K Ho *Telehealth in the Developing World (*2009) at 43.

[33] L Rannefeld 'The doctor will e-mail you now: Physicians' use of telemedicine to treat patients over the Internet' (2004) 19 (1) *Journal of Law and Health* 75 at 77.

[34] WHO 'Telemedicine Opportunities and developments in Member States' in *Global Observatory for eHealth series* (2010) 2 at 9.

[35] L Cilliers and SV Flowerday 'Health information systems to improve health care: A telemedicine case study' (2013) 15 (1) *SA Journal of Information Management* 1–5 at 1.

[36] Ibid and Rannefeld (n 33) at 77.

[37] Le Roux (n 6) at 101.

[38] M Mars 'Telepsychiatry in Africa: A way forward?' (2012) 15 *African Journal of Psychiatry* at 215.

health management plan.[39] In face-to-face or synchronous telemedicine, eHealth consultations are interactive and occur in real time, using, for example, video-conferencing, a two-way telephone conversation or Skype applications.[40]

Lastly, cyber-medicine is closely related to telemedicine[41] and is described as 'the science of applying internet and global networking technologies to medicine and public health, of studying the impact and implications of the Internet, and of evaluating opportunities and the challenges for health care'.[42] Although there are areas of overlap, telemedicine[43] focuses primarily on a restricted exchange of clinical information between patient and doctor or between doctor and doctor, while cyber-medicine dispenses health information and advice between a doctor and patient via the Internet, or other online platform, with or without an established or ongoing doctor-patient relationship.[44] This usually involves an online platform, such as an Internet website, where a health care practitioner, or a group of practitioners, offers various medical services to users. Services would usually be restricted to the provision of primary health care,[45] advice, information, and second opinions. The health practitioner and user communicate online via e-mail, instant messaging or a real-time chat service. The practice of this form of eHealth, although increasingly popular, is also the most controversial, with questions around the quality of the care, misdiagnosis, misrepresentation, breaches of privacy and confidentiality, and the potential abuse of online pharmaceutical drug prescriptions being of the most concern.[46] Whereas telemedicine is generally applied to 'diagnostic and curative

---

[39] Ibid.

[40] P Malindi and MTE Kahn 'Letter to the Editor: Rural Telemedicine in Africa' (2005) 47 (8) *South African Family Practice* at 4.

[41] Rannefeld (n 33) at 77.

[42] G Eysenbach, E Ryoung Sa and TL Diepgen 'Shopping around the Internet today and tomorrow: towards the millennium of cybermedicine' (1999) 319 (7220) *BMJ* 1294 at 1294.

[43] Or 'health care at a distance'.

[44] Le Roux (n 6) at 100.

[45] Primary health care is defined as 'the provision of integrated, accessible, health care services by clinicians who are accountable for addressing a large majority of personal health care needs, developing a sustained partnership with patients, and practicing in the context of the family and the community' in EE Westberg and RA Miller 'The basis for using the Internet to support the information needs of primary care' (1999) 6 *JAMIA* at 6.

[46] C Erwell 'Telemedicine: Overcoming obstacles on the road to global health care' (2003) *International Trade Law Journal* 68 at 69.

medicine', cyber-medicine is applied to 'preventive medicine and public health'.[47] While telemedicine is driven by a so-called 'technological push', cyber-medicine is characterised by a 'consumer pull'.[48]

The terms 'telemedicine', 'tele-health', 'online health', 'eHealth', 'connected health', and 'cyber-medicine' are used inconsistently and interchangeably in the literature and should be interpreted within the context within which they are used. What is constant, however, in the definitions of 'telemedicine', 'eHealth' and 'cyber-medicine' is the use of electronic and communication technologies within health care practice that are then often linked to the technologies of the time. For ease of reference, I have used the more general term of 'eHealth', unless the terms 'telemedicine', 'mHealth' or 'cyber-medicine' are more appropriate.

III NATURE AND SCOPE OF EHEALTH

Increasingly, the future of health care services is being defined by online social network tools like weblogs, instant messaging, video chat, online consultations and advice forums.[49] eHealth offers a myriad of opportunities to benefit from, manage and provide access to medical data, which in turn can deliver higher quality patient care.[50]

The South African National eHealth Strategy [51] includes the following activities and services that fall within the scope of eHealth:

- electronic health and medication records;
- health management information;
- health information networks / consumer health informatics;
- health knowledge management;

---

[47] G Eysenbach 'Towards ethical guidelines for dealing with unsolicited patient emails and giving teleadvice in the absence of a pre-existing patient-physician relationship systematic review and expert survey' (2000) 2 (1) *J Med Internet Res* at e1.

[48] 'Technology push' refers to the existence and availability of technology without defining the user's demands and does not necessarily lead to a widespread use of telemedicine applications and/or services. Customer or 'demand pull', in contrast, is a response to users' demands and needs, irrespective of existing or developing technology.

[49] C Hawn 'Take two aspirin and tweet me in the morning: How Twitter, Facebook, and other Social Media are reshaping health care' (2009) 28 (2) *Health Affairs* at 361.

[50] Kalema and Kgasi (n 5) at 1.

[51] 'National eHealth Strategy South Africa 2012–2016' *Department of Health* (2012) at 7.

- mHealth;
- telemedicine and tele-care services;
- virtual health care, diagnosis and treatment (health professionals' co-operation via ICTs, online diagnosis and treatment of limited and specific medical conditions and provision of primary health care); and
- health research.

Additionally, eHealth includes:

- the prevention of disease (including access to the latest news, articles and trends in health care and medically related matters as well as the promotion of health and well-being);
- remote patient monitoring (includes home-centered care, supporting self-management of chronic diseases and personal management tools, such as online disease management, for example, online health and tracking applications);
- online discussion and support groups;
- continuing education of health professionals and patients; and
- ePrescribing.[52]

Furthermore, eHealth extends to virtual reality, robotics, multimedia, digital imaging and computer assisted surgery.[53]

One should, however, differentiate between those who use health resources on various online platforms and on technological platforms merely as 'users' who seek advice and support for general medical, wellness and health conditions, and those who seek specific diagnosis, treatment, care and second opinions, and who may thus be more accurately described as 'patients'. eHealth, however, is steadily transforming 'patients' into 'users' and, finally, into 'consumers'. With innovative eHealth

[52] B Futter 'The naked patient' (2012) 79 (9) *South African Pharmaceutical Journal* at 64.

[53] N Ferraud-Ciandet 'Privacy and data protection in eHealth: A comparative approach between South African and French legal systems' (2010) *IST-Africa* at 1–10.

services, it is believed that health care systems can advance from a purely public service delivery towards transforming the patient into a consumer.[54]

IV BENEFITS AND USES OF EHEALTH

The benefits and uses of eHealth are considered hereunder. The following sub-sections discussed are online health information seeking, emerging virtual health care patterns, and the socio-economic impact of eHealth.

(1) eHealth and online health information seeking

The online environment provides instant data sharing, which includes applications, such as Myspace, Facebook, Twitter, YouTube, Wikipedia, as well as online websites developed for the purpose of information sharing and interconnectivity.[55] Users are increasingly using search engines to obtain health related information. In 2004, Google reported that five percent of all searches were health related.[56] This percentage has grown considerably, with a 2012 survey indicating that obtaining health information is one of the most popular activities conducted online: 72 percent of Internet users surveyed had searched for a health-related topic online within the preceding year.[57]

The extent of online personal diagnoses was explored in a health survey. Pew researchers asked participants whether they had used the Internet to search for at least one of 16 major health topics online, ranging from mental health and immunisations to sexual health information. The research found that users most frequently accessed the Internet to find information about a specific disease or medical condition (55 percent) or a particular medical treatment or procedure (43 percent). Information was

[54] N Friederici, C Hullin & M Yamamichi 'Chapter 3: mHealth' in *Information and Communications for Development 2012: Maximizing Mobile* (2012) at 45.

[55] Social media is defined as 'forms of electronic communication (as web sites for social networking and micro-blogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)'. Available at http://www.merriam-webster.com/ (accessed 12 February 2017).

[56] G Eysenbach and C Köhler 'Health-related searches on the Internet' (2004) 291 (24) *J Am Med Assoc* at 2946.

[57] Research conducted by the Pew Research Center's Internet & American Life Project 'Health Fact Sheet'.

also sought about diet, nutrition and exercise or fitness (60 percent). Other popular health topics included prescription or over-the-counter drugs (34 percent); medical test results (15 percent); information on depression, anxiety or stress (21 percent) and information on a particular doctor or hospital (21 percent). Fifty-two percent of smartphone owners and 31 percent of cellular phone owners have searched for health information on their mobile phone,[58] while 19% of smartphone owners have downloaded an application to track or manage their health.[59]

The Internet's popularity as a health resource does not appear to be abating. A 2010 survey revealed that an estimated 175 million people in the United States have used the Internet to search for health related information and that the number continues to increase. Frequency of use has also increased noticeably, with 32% of people who look for health information online doing so 'often'. The poll found that the percentage of people who have gone online to search for health information had increased noticeably to 88%, with a staggering 81% having looked for health information online in the last month. Moreover, 'very few' people reported being dissatisfied with their ability to find what they were looking for online and over half reported discussing information they found on the Internet with their doctors.[60]

As patients have wider access to medical resources, this has led to 'higher quality standards and evidence-based medicine'.[61] Fifty-three percent of online users said that they had used the information found online and discussed it with a medical professional.[62] Patient to patient interchanges have also increased in popularity.[63]

With the increased efficiency and acceleration of information transfer between information technology networks, the barriers to prompt and reliable exchanges of information, including health information and medical imagery, have been greatly eased. People can access information faster and more easily than was previously

---

[58] Ibid.

[59] Ibid.

[60] 'Cyberchondriacs on the Rise?' (2012) *Harris Interactive*.

[61] Eysenbach, Ryoung Sa and Diepgen (n 42) at 1295.

[62] S Fox and M Duggan 'Information Triage' (2013) *Pew Research Center's Internet & American Life Project*.

[63] Eysenbach Ryoung Sa and Diepgen (n 42) at 1295.

possible.[64] The value of eHealth lies not in the communication technology *per se* but in the ability to share medical information and expertise with others.[65]

(2) eHealth and emerging virtual health care patterns

eHealth has the advantage of affording users immediacy and anonymity. With immediate access at any time of the day or night, the continuous updating and revision of information and the extensive range of content available, online resources can be differentiated from other traditional forms of obtaining information.

To illustrate how popular eHealth has become, an incredible 92% of users surveyed revealed that the health information they found during their last online search was 'useful', with 81% saying 'they learned something new'.[66] Of the 21 million users who said they were influenced by what they read, 70% said 'the web information influenced their decision about how to treat an illness or condition', 50% said 'the web information led them to ask a doctor new questions or get a second opinion from another doctor', and 28% said 'the web information affected their decision about whether or not to visit a doctor'.[67] The significance of such widespread popularity seems to indicate that people are becoming more empowered to actively gain access to alternative accessible forms of health care services.[68]

Of interest is that the anonymity offered by the Internet is viewed by users as advantageous, as it 'allows users to ask awkward, sensitive, or detailed questions without the risk of facing judgment, scrutiny, or stigma, and to do so at their convenience'.[69] Additionally, users or patients are free to engage in a more participative health care model, which, in turn, alleviates the difficulties of physical

---

[64] C Jack and M Mars 'Telemedicine a need for ethical and legal guidelines in South Africa' (2008) 50 (2) *South African Family Practice* 60a at 60c-d.

[65] GT Bosslet, AM Torke, SE Hickman, CL Terry and PR Helft 'The patient-doctor relationship and online social networks: Results of a national survey' (2011) 26 *J Gen Intern Med* 1168 at 1172.

[66] S Fox and L Rainie 'The online health care revolution' *Pew Internet & American Life Project: Online Report* (2000).

[67] Ibid.

[68] Ibid.

[69] SR Cotten and SS Gupta 'Characteristics of online and offline health information seekers and factors that discriminate between them' (2004) 59 *Social Science & Medicine* at 1795.

access to health care practitioners experienced by those in isolated or remote areas. People have opted to perform previously face-to-face transactions online.[70]

In addressing the challenge of increased health care sustainable delivery, the EU has increased its focus on a more patient-centric care methodology so that patients are better able to manage their own care, more particularly, by influencing patient behaviour to improve lifestyle choices, enable the treatment of chronic conditions remotely, and better equip health care providers in improved clinical decision making.[71]

Data findings from a WHO survey noted that 91% of EU member states indicate that individuals and communities are using social media to learn about health issues. It reported that in 81% of EU member states, health care organisations use social media to promote health messages as part of their health campaigns, while 51% report that organisations use social media to make emergency announcements.[72] Additionally, 14% of EU member states are reported to have a national policy or strategy in place, regulating the use of social media in health professions.[73] eHealth data, when appropriately analysed, assists in establishing patterns of broader importance to various communities and societies. These patterns or trends may predict and avoid the escalation of potential health crises.

(3) eHealth and the socio-economic impact

A 2013 report states that, in utilising eHealth, the EU could save 99 billion Euros in total annual health care expenditure in 2017. This translates to the treatment of an additional 24,5 million patients, while assisting 185 million users to benefit by leading healthier lifestyles. The PwC report estimates that 45 million chronic patients and 47 million elderly people may require monitoring of their health conditions in the EU by 2017.[74]

---

[70] Ibid.

[71] 'Socio-economic impact of mHealth: An assessment report for the European Union' June 2013 *PwC*.

[72] WHO 'From innovation to implementation: eHealth in the WHO European Region' (2016). See C Dario, A Dunbar, F Feliciani, M Garcia-barbero, S Giovannetti, G Graschew, P Mancini, MTJ Mohr, P Ortiz García, S Pedersen, JM Pérez-Sastre and A Rey 'Opportunities and Challenges of Ehealth and Telemedicine via Satellite' (2004) *Eur J Med Res Supplement* at 1.

[73] Ibid.

[74] *PwC* (n 71) at 15.

eHealth has a socio-economic impact by shifting the emphasis of health care to the prevention of disease and the enhancement of wellness.[75] The proliferation of medical and health care websites, online databases, health care advice services and publications available on the Internet is testimony to the need for ongoing alternative sources of medical advice, support and treatment. An array of health information and advice is freely available online, with support groups and medical organisations, for example, the Heart and Stroke Foundation South Africa[76] and Diabetes South Africa[77], providing information to online users on the causes, symptoms, treatments and preventative measures for various conditions.

Websites that allow patients to gain online access to their medical reports and patient records, billing information, appointment bookings and clinical laboratory reports have also increased in popularity.[78] Social media provides the capacity for online users to make contact easily and effortlessly with other users with similar conditions.[79] With the number of medical websites currently well in excess of 100 000, there is a global awareness, if not something of a fascination, with medically related online content.[80]

eHealth is a worldwide phenomenon and growing steadily.[81] The number of health-related applications in Apple's online App Store increased from 4000 in February 2010 to more than 15 000 by September 2011, just 18 months later.[82] A survey of asthma patients between the ages of 12 and 40 years old named text messaging, email and Facebook as being used at least weekly by the majority of respondents (82%, 77% and 65%, respectively). Interestingly, female and Black or Hispanic participants were found to be more likely to have an interest in the use of

---

[75] Ibid at 9.

[76] Heart Foundation SA.

[77] Diabetes SA.

[78] For example, 'my health at Vanderbilt.com'.

[79] Adesina *et al.* (n 29) at 1.

[80] *Harris Interactive* (n 60).

[81] P Keckley and M Hoffmann 'Social Networks in Health Care: Communication, collaboration and insights' (2010) *Deloitte Centre for Health Solutions*.

[82] Friederici *et al.* (n 54) at 51.

electronic media for asthma care.[83] This trend seems to mimic the increase in usage of mHealth in those sectors of the population who were previously considered separated by the 'digital divide'.[84]

V EHEALTH IN DEVELOPING COUNTRIES

The purpose of eHealth is to reduce the cost of health care, enhance the quality of health service delivery, improve primary care interventions and public health initiatives, and address and improve the shortage of health professionals through partnership, collaboration and training.[85] Clearly, when it is optimally integrated into a health care system, eHealth offers an extensive advantage.[86] eHealth systems can transform existing health care systems.[87] When asked how eHealth can improve health system's performance, Godal responded:

> 'By incrementally improving existing health-care systems, and by opting for radically new ways of delivering and monitoring care. Entering patient data on a phone or a tablet in a rural clinic, transferring this electronically and extracting required information from this avoids the slow and labour-intensive steps of paper-based systems. But more importantly, e-health technologies can totally change the way health care is delivered and monitored. Front-line workers can now have tools for making decisions available at their fingertips and telemedicine can provide them with expert help. Thus new roles can be defined and patients empowered with information and a voice in monitoring'.[88]

---

[83] AT Baptist, M Thompson, KS Grossman, L Mohammed, A Sy and GM Sanders 'Social Media, Text Messaging and Email preferences of Asthma patients between 12 and 40 years old' (2011) 48 (8) *J Asthma* 824–830.

[84] UNICEF 'African Mobile Observatory 2011: Driving Economic and Social Development through Mobile Services' (2011); the 'digital divide' refers to the 'gap' between 'individual's households, businesses and geographic areas at different socio-economic levels with regard to both their opportunities to access information and communication technologies (ICTs) and to their use of the Internet for a wide variety of activities'.

[85] S Avancha, A Baxi and D Kotz 'Privacy in mobile technology for personal healthcare' (2012) 45 (1) 3 *ACM Computing Surveys* at 3.1.

[86] Rannefeld (n 33) at 78.

[87] WHO (n 4) at 321–400.

[88] Ibid at 321.

The digital environment provides an efficient, convenient, cost effective and private method of obtaining medical information and health care advice and delivery.[89] Thus, eHealth offers substantial value for informed decision-making and greater participation by individuals in directing and managing their own health care. While eHealth in developed countries is largely driven by the incentive to cut health care costs, in developing countries it is fundamentally supported by the increased access to primary health care.[90]

The successful integration of ICT (information communication technology) into health care systems is seen primarily in developed countries.[91] However, the broad policy debate on the value of eHealth in developing countries is an issue deserving of attention.[92]

As telecommunications technologies mature, what is emerging is the shift from using mobile phones merely as simple tools of communication to the creation of eHealth service delivery platforms, which can transform lives through innovative applications and services.[93] eHealth offers a tremendous opportunity for developing countries and communities to obtain medical care, while saving scarce resources by improving the efficiency of health care systems and the delivery of health care.[94] As stated by Sharmin *et al.*, an enormous potential exists 'in using mHealth as one of the supportive systems within the health care sector to solve the inequalities in health care delivery between rural and urban hospitals'.[95]

Although studies on telemedicine and eHealth in Africa in particular have centred on the 'technological feasibility, specialist clinical interest, implementation costs and estimated cost savings', [96] there are clear and obvious socio-economic

---

[89] Avancha *et al.* (n 85) at 3.1.

[90] WHO (n 34) at 6 and 21

[91] Kalema and Kgasi (n 5) at 1.

[92] WA Kaplan 'Can the ubiquitous power of mobile phones be used to improve health outcomes in developing countries?' (2006) 2 *Globalization and Health*.

[93] JC Aker and IM Mbiti 'Mobile Phones and Economic Development in Africa' (2010) 24 (3) *Journal of Economic Perspectives* at 212.

[94] Qiang *et al.* (n 24) at 15.

[95] J Sharmin, M Hoque Chowdhury 'mHealth: A Sustainable Healthcare Model for Developing World' (2014) 2 (3) *American Journal of Modeling and Optimization* at 73–76.

[96] PA Jennett *et al.* 'The socio-economic impact of telehealth: A systematic review' (2003) *Journal of Telemedicine and Telecare* at 311–312 and Le Roux (n 6) at 102.

benefits to users, namely, better quality care, greater participation, cost effectiveness and increased accessibility.[97] While electronic health technologies cannot physically transfer medicine, medical practitioners, and/or equipment between locations, their inherent strength is their ability to convey and process large volumes of data (much of which is personal and sensitive health data) in a myriad of forms, for instance, coded data, text, images, audio, and video, and then to interface with other devices and networks that may be linked to or support them.[98]

As is reported in Sarasohn-Kahn, users in 'emerging economies', such as Brazil, India, Mexico, and Russia, have 'a greater reliance on online health information because of the higher costs associated with seeing a medical professional face to face'. [99] Additional challenges facing developing countries are the chronic shortage of health care facilities and medical practitioners, and general inaccessibility of health care services, especially in remote areas. Developing countries, both low- and middle-income, tend to experience general shortages in health information, access to health care, poor treatment quality and lack of affordability for even the most basic care.[100]

Certain African health sectors face a considerable human resources crisis. For instance, a Lancet report found that failures in direction and weak management have resulted in inadequate implementation of otherwise good health policies in the South African public health system.[101] The HIV/AIDS epidemic has only exacerbated already challenged public health care systems.[102] A key factor emphasised in the report was that 'innovative approaches to health service delivery are needed in developing countries that are affected by both communicable and non-communicable diseases'.[103]

---

[97] Ibid.

[98] Qiang *et al.* (n 24) at 15.

[99] J Sarasohn-Kahn 'Health citizens in emerging countries seek health information online even more than their peers in developed economies' (2011) *Health Populi*.

[100] Qiang *et al.* (n 24) at 15.

[101] S Kleinert and R Horton 'South Africa's health: Departing for a better future?' (2009) 374 (9692) *The Lancet* 759–760; H Coovadia, R Jewkes, P Barron, D Sanders and D McIntyre 'The health and health system of South Africa: Historical roots of current public health challenges' (2009) 374 (9692) *The Lancet* 817–834.

[102] Ibid.

[103] Ibid.

An illustration of the doctor to patient ratio within an African country is confirmed by the South African Department of Health. While Africa carries 24% of the global disease burden, it only has a low 3% of the world's health practitioners.[104] With countries like France, America and the United Kingdom having 34, 24 and 27 doctors per 10 000 population respectively, countries in the African region have a reported 2 doctors per 10 000 population.[105] This is by far the lowest doctor to population ratio worldwide.

Illness and death in developing countries are often due to health conditions that are largely preventable and for which medical solutions are known and often easily implemented.[106] Despite this, the health of those living in developing countries remains at risk, where a disproportionately high burden of infectious diseases, escalating health care costs, unacceptably high levels of mother and child mortality and a continuing HIV/AIDS pandemic exist.[107] This is exacerbated by the general lack of and poor quality of health care services and the chronic shortage of health care professionals.[108]

Despite the need for sustainable and efficient health care services and the increased awareness that the Internet and various online technological platforms provide a beneficial solution, eHealth has not been fully integrated and remains on the fringe of most mainstream African health care systems.[109] It is suggested that '[t]o achieve better health in a cost-effective and sustainable way, developing countries need to exploit ideas and technologies that leverage resources that are readily available and affordable'.[110]

---

[104] Department of Health (2008).

[105] WHO 'World Health Statistics' (2012).

[106] Causes of death among children under 5 years old in Africa primarily include diarrhoea, measles, malaria, pneumonia and HIV/AIDS.

[107] Le Roux (n 6) at 99, and Kalema and Kgasi (n 5) at 2.

[108] M Kekana, B Mkhize and P Noe 'The practice of telemedicine and challenges to the regulatory authorities' (2010) 3 (1) *South African Journal of Bioethics and Law* at 33 and Le Roux (n 6) at 99.

[109] Ibid.

[110] Qiang *et al.* (n 24).

VI THE ROLE OF EHEALTH IN PROVIDING AN ALTERNATIVE OR COMPLEMENTARY HEALTH CARE SOLUTION

mHealth is a direct result of the rapid rise of mobile phone penetration. Sharmin *et al.* conclude that, in terms of 'size, portability, low power consumption and ability to operate with limited infrastructure', mobile phones are 'better platforms to provide health services in the developing countries'.[111] eHealth (and particularly mHealth) provides increased access to larger segments of the population and improves the ability of the health care systems in such populations to provide better health care.[112]

Although mHealth is still in its infancy, there are indications that it is already transforming health care systems.[113] The benefits of mHealth are: (a) increased access to health care delivery and information to particularly remote or isolated populations; (b) increased efficiency and decrease in the cost of service delivery; (c) improvement in the ability to diagnose, treat and track diseases; (d) the more timely dissemination of public health information; and (e) extended access to medical and health care education to users and health care practitioners.[114]

With an estimated 6 billion people worldwide (which roughly translates to 75% of the world's population) having access to a mobile phone, mobile phones are the single most ubiquitous modern technology.[115] In certain developing countries, more people have access to mobile phones than to electricity or clean water.[116] Mobile phone applications are portals to an online world – a powerful tool in providing developing countries with more than just a voice but also empowering them to engage in more informed decision-making and exposing them to wider choice.[117] The

---

[111] Sharmin *et al.* (n 95) at 73–76.

[112] Ibid.

[113] PN Mechael, H Batavia, N Kaonga, S Searle, A Kwan, A Goldberger, L Fu and J Ossman 'Barriers and gaps affecting mHealth in low and middle income countries' (2010) Policy white paper *The Earth Institute Columbia University* at 6.

[114] Ibid.

[115] M Tomlinson, MJ Rotheram-Borus, L Swartz and AC Tsai 'Scaling Up mHealth: Where Is the Evidence?' (2013) 10 (2) *PLOS Med*.

[116] World Bank 'Information and communications for development: Maximizing mobile' (2012) at 3.

[117] Ibid.

significance of the mobile phone is no longer in the phone itself, but in the way in which it is used and the content and applications to which users gain access.[118]

In recent years, mobile communications have experienced faster growth rates in lower-income groups – more than twice as fast as those in the high-income countries, thus accounting for more than 20% of the world mobile market share.[119] The prevalence of mobile phones in much of sub-Saharan Africa surpasses that of fixed-line phones.[120] Africa is the fastest growing mobile market in the world, with in excess of 500 million mobile users in sub-Saharan Africa in the first quarter of 2013.[121] In 2015, 46% of the African population subscribed to mobile services, with Egypt, Nigeria and South Africa being the most subscribed. While sub-Saharan Africa has 8% of the worldwide 6.5 billion mobile connections, it has the highest growth rate globally, with connections expected to increase by a further 50% over the next five years.[122] It is estimated that, within the next three years, an additional 168 million people will subscribe to mobile services across Africa, reaching 725 million connections by 2020. [123]

With the rapid expansion of mobile technology, Africans living in urban and rural communities have been able to access digital information through mobile and computer internet connectivity, more than ever before.[124] Statistics South Africa found that among the population of approximately 50 million in South Africa, there is an account of 100.48% mobile penetration, that is, of people owning, renting and/or having access to a mobile cellular device.[125] Regionally, South Africa has one of the highest mobile coverages in Africa, with 81% of the population having access to

---

[118] Ibid at 4.

[119] 'Africa: The Impact of Mobile Phones' (2005) *Vodafone Policy Paper Series Number 2* at 3.

[120] There were 52 million mobile users in Africa in 2003 with only an estimated 25 million fixed lines. Ibid also Aker and Mbiti (n 93) at 207.

[121] Sub-Saharan Africa Mobile Observatory (2012) *GSMA/Deloitte* at 9.

[122] 'The Mobile Economy: Africa 2016' (2016) *GSMA* at 2; 'Mobile trends in Sub-Saharan Africa' *GSMA Intelligence* and ibid.

[123] Ibid.

[124] Aker and Mbiti (n 93) at 207–232.

[125] 100.48% suggests that some people may have more than one phone. Statistics South Africa, Key Results (2001).

mobile service coverage.[126] As of September 2011, the African continent had the second largest mobile market in the world, with over 620 million mobile connections.[127] The developing world is described as 'more mobile' than the developed world.[128]

This technology for eHealth and specifically mHealth holds enormous promise for the public and private health care sectors[129] alike in improving the access and delivery of health care services within remote or vulnerable populations, but also to an increasingly technologically driven consumer.[130] In addition to this, the entry level for mHealth services is often lower than that of other eHealth applications, making it that much more financially attractive to users.[131] The youth with their familiarity with mobile phones, their adaptability, their high usage of such devices, and their ability to use social networking platforms can particularly benefit from mHealth applications, especially, for instance, in health promotion, disease prevention and sexual and reproductive health.[132] The youth are skilled technological consumers and their ability to comment, blog or use the 'share button' in respect of eHealth initiatives improves outreach and impact.[133] The interactivity of mHealth applications and their participatory functionality is proving popular and highly desirable to the youth.[134] In light of this, Edouard suggests that it is desirable then that health care professionals become familiar with using social networking platforms such as Facebook and Twitter in enhancing their service delivery.[135]

---

[126] Sub-Saharan Africa Mobile Observatory (n 121) at 9.

[127] UNICEF 'African Mobile Observatory 2011: Driving Economic and Social Development through Mobile Services' (2011) at 5.

[128] World Bank (n 116).

[129] The use of mobile phones for public health awareness has been recently demonstrated for HIV/TB awareness in Uganda. Available at http://ttcmobile.com/using-mobile-technology-in-tb-control-in-uganda/ (accessed 20 February 2017).

[130] Adesina *et al.* (n 29) at 4.

[131] Friederici *et al.* (n 54) at 50.

[132] Edouard and Edouard (n 28) at 197.

[133] The dissemination of information on sexual and reproductive health issues has been demonstrated in various projects across Africa. See 'Mobile technology: Text messages for better reproductive health' (2012) *Family Health International*.

[134] Edouard and Edouard (n 28) at 197.

[135] Ibid.

Clearly, developing countries have much to gain from leveraging off expanding 3G networks and mobile broadband, and mHealth applications are perfectly placed to provide a solution to the shortage of preventative and primary health care.

VII EXAMPLES OF EHEALTH APPLICATIONS

EHealth services and applications can be of enormous value to developing countries. The following sub-sections will highlight the use of mobile messages, and the role eHealth played in the Ebola outbreak, as illustrations of the tremendous benefit eHealth can provide.

(1) The use of mobile messages

A study conducted in South African using mobile phone technologies to connect tuberculosis patients to their caregivers, using reminder text messages found that, after the system was implemented, adherence to treatment regimens improved.[136] South Africa is a fertile testing ground for treatment compliance technologies, with several disease control specialists looking at short message services (SMSs) as a cost effective and effectual method of communicating with and monitoring patients located in remote areas.[137] The WHO reported a 71% treatment success rate in South Africa using its directly observed treatment short course (DOTS), while most patients who were not treated under DOTS defaulted on their treatment.[138] This programme has dramatically improved tuberculosis control around the world and is of particular importance, as both TB and HIV/AIDS treatments require constant patient supervision and rigorous adherence to a daily treatment regimen.[139] eHealth is being

[136] E Barclay 'Text messages could hasten tuberculosis drug compliance' (2009) 373 *The Lancet* at 15–16. See JA Blaya, HSF Fraser and B Holt 'EHealth technologies show promise in developing countries' (2010) 29 (2) *Health Affairs* at 244–251. See also study by R Elangovan and S Arulchelvan 'A Study on the Role of Mobile Phone Communication in Tuberculosis DOTS Treatment' (2013) 38 (4) *Indian J Community Med* at 229–233.

[137] Ibid.

[138] Ibid and 'National Tuberculosis Management Guidelines' (2008) *Department of Health South Africa*.

[139] See success achieved in South India using mobile phone communication in TB treatment, Elangovan and Arulchelvan (n 136) at 229–233.

successfully applied in maternal and child health care in South Africa[140] in programmes to reduce diseases associated with poverty, such as HIV/AIDS, malaria and tuberculosis.

Similarly, in June 2012, the delivery of a basic health care service was launched by the Pan-African mHealth Initiative in conjunction with the GSMA. The purpose was, by using mHealth, to address certain challenges, such as reducing maternal and infant mortality rates, combating infectious diseases and creating awareness of HIV/AIDS remotely.[141]

The South African Department of Health announced the launch of an eHealth initiative named the MomConnect service.[142] This is a service whereby all pregnant women, of which there are approximately 1.5 million a year, are to be sent SMS messages, if registered with the service. These messages will be sent fortnightly during pregnancy, and will continue for a period of at least 1 year after the child has been born. The messages will be appropriate to their stage of pregnancy and will advise them of relevant issues applicable to the progression of their pregnancy. After birth, information on the care of their newborn is to be provided for a period of 1 year. Health messages on such topics as growth monitoring, oral rehydration, breastfeeding, immunisation, food supplementation and family planning are to be provided electronically.[143]

(2) The Ebola outbreak in Western Africa

The 2014 Ebola virus disease outbreak in Western Africa is regarded as the severest outbreak since the disease was initially identified in 1976.[144] By October 2014, nine

---

[140] See 'Maternal messaging & mHealth programmes: Empowering and enabling decision makers to include mHealth services into their budgets' (2014) *Deloitte*/*GSMA*.

[141] Sub-Saharan Africa Mobile Observatory (n 121) at 48.

[142] Aaron Motsoaledi: Address by the Minister of Health, during President Jacob Zuma's State of the Nation Address, Parliament, Cape Town on 20/06/2014.

[143] Ibid.

[144] On 23 March 2014, the WHO issued WHO 2014a on the outbreak of the Ebola virus disease. See D Gatherer 'The 2014 Ebola virus disease outbreak in West Africa' (2014) 95 *Journal of General Virology* at 1619.

countries, Sierra Leone, Liberia, Guinea, Nigeria, Mali, the USA, Senegal, Spain and the United Kingdom, had been affected.[145]

To illustrate the expeditious and valuable application of eHealth service delivery, IBM launched three eHealth initiatives to curb the spread of the outbreak of the Ebola virus in West Africa.[146] These included 'a citizen engagement platform in Sierra Leone, the roll-out of coordination technology in Nigeria to strengthen their preparedness for future outbreaks and a global open data repository'.[147] What was instrumental in these initiatives was the application of mobile technology, data analytics and cloud computing, which afforded governments and relief agencies the opportunity to make considerable advancements in containing the deadly disease. Using supercomputing power and analytics capabilities via cloud technology, systems were able to rapidly identify correlations and highlight emerging issues across the entire data set. As stated by Chief Scientist, IBM Research for Africa, Dr. Uyi Stewart[148]: '…we are uniquely positioned to use innovation to help tackle some of the continent's biggest challenges'.

Chowdhury stated that: '[m]obile technology is Africa's most powerful communications platform providing an important channel for reaching large numbers of the population'.[149] Not only did the ability to monitor and track population movement enable scientists to map and predict the spread of disease, but the effective flow of important health information between patients, health workers and the general public was invaluable.

This eHealth initiative provided health workers with a 'reliable and secure digital platform to work together virtually and in person, enabling them to securely share documents, identify experts, exchange video, chat and audio messages, provide updates, tap into information via mobile devices and hold virtual meetings'.[150]

Likewise, efforts have been made to assist identify, inventory and classify all open data sources related to the Ebola outbreak. The objective is to establish a cloud-

---

[145] WHO Ebola Situation Reports (2015).

[146] T Chowles 'IBM launches Ebola eHealth solutions' (2014) *eHealth News.*

[147] Ibid.

[148] Ibid.

[149] Ibid.

[150] Ibid.

based Ebola Open Data Repository. This will provide governments, aid agencies and researchers with open access to data related to Ebola. African countries such as Sierra Leone, Liberia, Ghana, South Africa, Malawi and Tanzania have joined the Open Government Partnership[151] with the intention of obtaining published open data and consequently drive innovation and support better collaboration.[152]

This is indeed a most promising and compelling argument in favour of the real and rapid responses that can be offered by eHealth initiatives. While highlighting the tremendous impact that eHealth can have on health care systems, especially in humanitarian crises, cognisance should be taken of the concomitant dangers in the random, free and uncontrolled exchange of personal, medical data, especially when diseases are highly contagious and there is a realistic opportunity for potential stigmatisation, and abandonment or ostracism by a largely fearful community.[153]

Concerned about informational privacy and security, a 2010 report, conducting research on privacy and security in developing countries and humanitarian operations, concluded that policy change is insufficient in environments with 'minimalist legal frameworks, or where the rules are easily suspended in the case of emergency humanitarian and relief efforts'.[154]

VIII A BARRIER TO EHEALTH ADOPTION – PRIVACY PROTECTION

Despite the numerous advantages offered by eHealth systems, various challenges are present. A necessary consequence of eHealth is the creation of medical records, digital images and copious data, the subject of which is personal and highly sensitive.[155] Primary concerns of eHealth implementation are the privacy and security

---

[151] Ibid.

[152] Ibid.

[153] See O Maduka and O Odia 'Ethical challenges of containing Ebola: the Nigerian experience' (2015) *Journal of Medical Ethics* at 41 for the ethical challenges arising out of the Nigerian Ebola outbreak.

[154] Policy Engagement Network for the International Development Research Centre 'Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations' (2010) *LSE* at 4 and 6.

[155] A Geissbuhler, C Safran, I Buchan, R Bellazzi, S Labkoff, K Eilenberg, A Leese, C Richardson, J Mantas, P Murray and G De Moor 'Trustworthy reuse of health data: A transnational perspective' (2013) 82 (1) *International Journal of Medical Informatics* at 1–9.

issues arising from electronic data storage and management. With the adoption of eHealth, new forms of data collection, storage, and the extensive sharing and transference of sensitive medical data, the implicit threat of misuse of such data becomes immediately apparent.[156] Privacy and data protection are identified as vital to eHealth applications.[157]

Data handling and good, secure record keeping should form the backbone of any eHealth practice for it to succeed in securing user confidence and gaining global momentum. This is particularly so, in light of advancements in medical testing, genetic profiling and medical imaging, together with the dramatic increase in the volume and detail of digitally available health information.

Perhaps one of the greatest advantages offered by information technology in health care is that eHealth can create a platform and infrastructure for the sharing and exchanging of electronic health records. Personal medical information about a patient is recorded in a patient's medical record and may be kept in either paper or electronic form. Although these records may include extensive personal information regarding a patient, they usually include medical notes, historical reports, magnetic resonance images, clinical laboratory results, medical practitioners' letters, referrals, medication prescriptions and treatment regimes. They may then be centrally recorded and located and be accessible to various medical health care practitioners.[158] Interestingly, India's Health Management and Research Institute, through the integration of an eHealth application, has created over 10 million unique electronic health records, which is reported to be one of the largest public eHealth record databases worldwide.[159]

Electronic Patients Records (EPR) convert paper-based documents into a digital or electronic format.[160] EPRs are advantageous in that they allow real-time access to medical records and can be easily accessed and updated.[161] The corollary to

---

[156] J Hohmann and S Benzschawel 'Data protection in eHealth platforms' in *Legal and Forensic Medicine* (2013) at 1633–1658.

[157] Friederici (n 54) at 56.

[158] Hohmann and Benzschawel (n 156) at 1634.

[159] Qiang *et al.* (n 24). See also Friederici *et al.* (n 54) at 56.

[160] See Adesina *et al.* (n 29) at 4 and Westberg and Miller (n 45) at 6.

[161] Ibid at 3.

this, however, is that these benefits need to be balanced against the vulnerability of data to security breaches.

The EU eHealth Taskforce Report[162] concludes that, although there is a significant lag (at last ten years according to the report) in the implementation of IT solutions in health care, information technology can 'improve' and 'radically revolutionise' the health care system within the EU. Great emphasis however is placed on the manner in which the following fundamental issues are to be addressed, namely, the treatment of data, privacy issues, the movement of data across jurisdictional borders, research and the physician-patient relationship.[163]

Moreover, the European Commission's 2014 green paper on mHealth cites '[d]ata protection, including security of health data' as an 'issue at stake' in mHealth advancement.[164] The paper raises concerns about the appropriate processing of data collected through mHealth software applications or solutions by *inter alia* individuals, application developers or health professionals, as by their very nature, eHealth solutions and devices are capable of collecting and processing large volumes of data.

It is fair to say that these issues are not unique to the EU but resonate across all regions (including Africa) wishing to promote the development and implementation of eHealth solutions.

IX CONCLUSION

In line with the major advances in ICT over the past few years, as well as changing consumer behaviour, new avenues for innovative approaches to medical and health care access and treatment have developed. As online platforms continue to grow in accessibility and popularity, a clearer understanding is required of the extent to which online health care is influencing people's lives, along with the scope of such care and the implications this will have on people.

This chapter sought to define the concept, nature and scope of eHealth. Aspects of eHealth that were considered include online health information seeking,

---

[162] eHealth Taskforce Report 'Redesigning health in Europe for 2020' (2012) *European Union eHealth Taskforce Report* at 5.

[163] Ibid.

[164] European Commission 'Green Paper on mHealth' (2014) at 8.

emerging virtual health care patterns and the socio-economic impact of eHealth. The eHealth position in developing countries was considered. The health care crisis and the merits of alternative, or supplementary, methods of addressing health care delivery were explored. As examples of the potential solution that eHealth offers, viz. the Ebola outbreak in West Africa and the use of mobile text messages in the South African context of tuberculosis treatment were discussed. Finally, the challenge of protecting user privacy and data in eHealth developments were examined. The following chapter shall consider privacy and data protection in more detail.

CHAPTER 3: PRIVACY AND DATA PROTECTION

Progress is impossible without change, and those who cannot change their minds cannot change anything.[1]

George Bernard Shaw

[1] Available at http://www.quotes.net/quote/37025 (accessed 2 January 2017).

I INTRODUCTION

This chapter presents the notion of privacy and data protection. As privacy includes the privacy of information disclosed in an eHealth relationship, it is necessary to consider the concept of privacy and its influence on that relationship. This chapter thus seeks to explore and clarify the concepts of privacy and data protection more fully and to predict the implications thereof in eHealth development. Before the law around privacy and data protection can be affirmed and applied, it is essential to ascertain the interest, or subject, which is worthy of legal protection and which is being threatened. This chapter seeks to clarify the definitions of privacy and data protection and to explore the relationship between these concepts. The aim is thus to move beyond reducing privacy to a single value, by attempting to emphasise the multi-dimensional understanding of privacy, and that which it seeks to safeguard.

II THE EMERGENCE OF A NEW DIGITAL ORDER AND ITS THREAT TO INDIVIDUAL PRIVACY

RO Mason states that 'information forms the intellectual capital from which human beings craft their lives'.[2] Information is essential for the functioning of contemporary society. This information, or data,[3] may be used for a variety of economic, political and social purposes and may be collected, handled, stored and distributed by frequently unknown and unidentifiable persons or organisations.[4]

The unfortunate effect is that, with the increased prevalence in dealing with personal data, albeit on many levels that are beneficial and convenient, society has largely been turned into what is a 'privacy-unfriendly environment'. The uneasy

[2] See RO Mason 'Four Ethical Issues of the Information Age' (1986) 10 (1) *MIS Quarterly* at 5.

[3] Although I use the terms 'information' and 'data' interchangeably and as the context dictates throughout this thesis, the term 'data' can be described as collected, unprocessed facts, which of and by themselves are without meaning, whereas 'information' is generally considered to have meaning or use to the recipient, in other words, it is data that has acquired some degree of 'added value'.

[4] J Neethling 'Features of the Protection of Personal Information Bill, 2009 and the law of Delict' (2012) 75 *THRHR* at 242 puts its: '[i]t stands to reason that the complexities of modern society have produced ever more reasons why the state or persons have an interest in and an ever growing need for information about other persons. To obtain these data and satisfy the need, a new industry has developed, the practices of which, especially due to the use of computers, pose an immense threat to the personality of persons, primarily to their privacy and identity.'

juxtaposition of rapidly advancing information communication technology and conservative and underdeveloped informational privacy law has exacerbated sensitivities around potential privacy violations.[5] Van der Merwe speaks of privacy law as now being 'under considerable strain' to adapt to the rapidly changing digital environment.[6]

Technology is enhancing the collection, exchange, storage, use and dissemination of high volumes of, previously unwieldy, data both rapidly and easily, thereby leveraging potential incentives and financial benefits to companies, organisations and governments. Threats to the personal privacy of individuals and their personal data have become alarming.[7] The free market and technology have further exacerbated the threat to a person's privacy, and they have in effect become an 'invisible enemy'.[8] With data mining, user profiling, electronic monitoring and surveillance, and the global transference of data being increasingly pervasive, often without the user's knowledge or consent, the proclivity to use data for self-gain becomes axiomatic.[9] Accordingly, the tensions and challenges around information privacy require attention; they are touted 'as one of the most serious ethical debates of

---

[5] See C Prins 'When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?' (2006) 3 (4) *SCRIPTed* at 272. Also see D van der Merwe 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) 17 (1) *PER* at 300 and PA Pavlou 'State of the information privacy literature: Where are we now and where should we go?' (2011) 35 (4) *MIS Quarterly* at 977; SG Davies 'Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity' (1997) in *Technology and Privacy: The New Landscape* PE Agre & M Rotenberg (eds) at 143.

[6] Ibid at 297.

[7] See J Burchell 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* at 1 where '[t]hreats to individual privacy are greater now than ever envisaged' and 'pose enormous threats to individual …confidentiality'; and also, FS Chilapowski 'The Constitutional Protection of Informational Privacy' (1991) 71 *Boston University Law Review* at 133 and HN Olinger, JJ Britz and MS Olivier 'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007) *International Information and Library Review* at 31; see SD Esposti 'When big data meets dataveillance: The hidden side of analytics' (2014) 12 (2) *Surveillance and Society* at 209.

[8] See B Perinan 'The origin of privacy as a legal value: A reflection on Roman and English Law' (2012) 52 *American Journal of Legal History* at 186.

[9] L Edwards 'Privacy and Data Protection Online: The Laws Don't Work?' in L Edwards & C Waelde (eds) *Law and the Internet* 3 ed (2009) at 448.

the information age'.[10] The concern over violations to privacy is now a veritable threat, more so than at any previous time in history.[11]

Although the idea of data collection is not new,[12] the introduction of computers in the 1950s and the concomitant development of new information communications technologies, principally networks linking computers to the Internet, enabled information to be collected, stored, processed and disseminated more quickly and efficiently.[13] The enormity and scale of data usage and the consequential opportunity for its misuse are a danger, both perceived and real.[14]

As individuals' control over their data is lost and therefore not regularly checked or corrected, information may easily become 'misinformation', or the subject of incompleteness or distortion.[15] Moreover, personal data, although factually or contextually accurate, may be of such a sensitive and/or personal nature that it is not acceptable for use, as it may cause potential harm and embarrassment if disclosed without the individual's knowledge and consent.[16]

The management of personal data, especially in large volumes, has created newfound risks for the privacy of individual information and, by the end of the 1980s, the protection of personal data in e-transactions, including e-commerce and by

---

[10] See MD Birnhack 'The EU Data Protection Directive: An engine of a global regime' (2008) 24 *Computer Law and Security Report* at 508. Birnhack considers privacy under 'attack' by, firstly, the 'theoretical challenge posed by different understandings of privacy', secondly, by the 'technological challenge posed by the digital environment' and thirdly, by a 'legal challenge'. See Mason (n 2) at 5. Privacy along with 'accuracy', 'property' and 'access' are considered by Mason as the four most pressing ethical issues around information technology development.

[11] Davies (n 5) at 143 and D Banisar and SG Davies 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (2012) 18 (1) *John Marshall Journal of Computer & Information Law* at 4.

[12] For instance, acquiring and recording of information by conducting a census, issuing and monitoring passports, recording data in paper files or books, to name but a few, see Edwards (n 9) at 448.

[13] See A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 *South African Law Journal* at 401 and A Roos 'Privacy in the Facebook era: A South African legal perspective' (2012) 129 *South African Law Journal* at 377.

[14] Banisar and Davies (n 11) at 4.

[15] Where increased growth and sharing of data over the Internet have resulted in misinformation on the Internet being described as 'rife', see WHO 'Safety and security on the Internet: Challenges and advances in Member States' in *Global Global Observatory for eHealth Series* vol 4 *(*2011) at 10.

[16] Chilapowski (n 7) at 133. See also S Snail and S Papadopoulos 'Privacy and data protection' in S Papadopoulos & S Snail (eds) *Cyberlaw@SA* 3 ed (2012) at 275, 6 describing some of the dangers to privacy brought about by the Internet.

extension eHealth transactions, was identified as a distinct and important issue of public policy.[17]

Cyberspace has begun invading our private space.[18] Because of this, the subsequent emergence and development of data protection mechanisms has gained momentum, with several countries recognising and implementing measures to protect the privacy and, more narrowly, the personal data of their people.[19] In technologically advanced societies, privacy is, with varying degrees of success, high on political and technological agendas.[20]

The problem is exacerbated by the very nature of the Internet itself. Data can be accessed ubiquitously and conveyed seamlessly across borders and jurisdictions, creating difficulty in data management and control.[21] Hence, the transference of data between different jurisdictions with varying or no data protection laws further complicates matters.

Edward describes the impact of trans-global data flows on data protection rights as 'an opaque and politically thorny issue'.[22] Nevertheless, these issues in times of legal uncertainty and disintegration create a valuable catalyst for legal transformation and the opportunity to establish global legal cohesion. The unease experienced by those engaging in electronic transactions, caused principally by a

---

[17] CJ Bennett *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (1992) at 30; Pavlou (n 5) at 977 and Banisar and Davies (n 11) at 4.

[18] See R Clarke 'Internet privacy concerns confirm the case for intervention' (1999) 42 (2) *Communication of the ACM* at 60.

[19] In 1970, the German state of Hesse enacted the first data protection legislation. This was followed by Sweden enacting data protection legislation, namely, the Swedish Data Act in 1973. This has been replaced by the Personal Data Act (Sw. *personuppgiftslagen*, SFS 1998:204) when Sweden became a member of the European Union and when the EU Data Protection Directive 95/46/EC (hereinafter referred to as the 'EU Directive') was implemented in 1998. More recently, it was followed by the EU Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of person data and on the free movement of such data (General Data Protection Regulation) of 2012 (hereinafter referred to as the 'EU Regulation'. Numerous countries have adopted data protection regulations and enforcement laws, albeit to differing and various degrees. See FH Cate 'The EU Data Protection Directive, Information Privacy, and the Public Interest' (1994–95) 80 *Iowa Law Review* at 431.

[20] Policy Engagement Network for the International Development Research Centre 'Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations' (2010) *LSE* at 6.

[21] Edwards (n 9) at 449.

[22] Ibid.

largely unregulated, even lacking, approach to personal information protection, has advanced the growing advocacy of increased uniform and harmonised privacy regulations.[23] Although this form of privacy regulation resonates favourably with certain theorists' opinions, it cannot and should not be seen to be the only or the definitive source of privacy protection.[24]

III A HISTORICAL ACCOUNT OF PRIVACY

Privacy is a nebulous, ambiguous and controversial term.[25] The distinction between what a person exposes to public view and what is concealed, or exposed only to chosen intimates, is essential to permit human interaction without social disintegration.[26] The formation of a functioning adult in society necessitates a learned capacity to limit expression to what is acceptable within a public forum, while developing an inner and distinctly private life that is more uninhibited within a personal or private realm.[27]

The concept of privacy has well documented historical roots in religious and philosophical discourse.[28] Although deeply rooted in history and valued in various cultures, privacy and data protection as an established issue of public policy is a comparatively modern development.[29] Notably, Aristotle differentiated between the

---

[23] Burchell (n 7) at 2.

[24] Ibid.

[25] See H Gross 'The Concept of Privacy' (1967) 42 *NYULR* at 35, who describes the concept of privacy as 'inflicted with pernicious ambiguities'. Moreover, Julie Inness describes the legal and philosophical discourse of privacy as a state of 'chaos', in JC Inness *Privacy, Intimacy and Isolation* (1992). See the dispute in terminology, as illustrated in G Collste 'Global ICT-ethics: The case of privacy' (2008) 6 (1) *Journal of Information, Communication & Ethics in Society* at 79 and AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2 (3) *International Data Privacy Law* at 164.

[26] T Nagel *Concealment and Exposure and other essays* (2002) at 28.

[27] Ibid.

[28] The Qur'an, the Bible and Jewish law contain references to individual privacy, while classical Greece and ancient China support references to the concept with substantive protection of privacy. See B Moore 'Privacy Studies in social and Cultural History' (1984) *M.E. Sharpe Inc* at 3–80. Also Banisar and Davies (n 11) at 6 on the right to solitude.

[29] See Perinan (n 8) at 183 and 189 where the right to privacy, although in a different guise and without specific legal definition or content, was nevertheless recognised as a legal construction in ancient Rome. Protection of one's *privacitas* or *personalitas* in the form of the *actio iniuriarum* was available to protect individual personality and specifically 'non-physical' aspects of the personality, such as

public sphere of political activity ('the *polis*') and the private sphere of family and domestic life ('the *oikos*'), where the idea of privacy as a function of individual freedom was an attempt to distinguish home life from that of society.[30] Historical use of the term provides little clarity as to the meaning, value and scope of the concept of privacy.[31] Privacy law can be observed in 14th century England, when the English Justices of the Peace Act provided for the arrest of peeping toms and eavesdroppers.[32] John Stuart Mill in his treatise *On Liberty* asks:

> '[w]hat, then, is the rightful limit to the sovereignty of the individual over himself? Where does the authority of society begin? How much of human life should be assigned to individuality, and how much to society? ... To individuality should belong the part of life in which it is chiefly the individual that is interested; to society, the part which chiefly interests society.'[33]

The distinction between the private and public spheres arose again in 1689 in John Locke's *Second Treatise on Government*[34] where he argued that in the 'state of nature all the world's bounty is held in common, and is in that sense public', but 'one possesses oneself and one's own body, and one can also acquire property by mixing one's labor with it, and in these cases it is one's private property'. British Lord Camden CJ, in *Entick v Carrington* remarked:

> '[o]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does, he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law …we can safely say there is no law in this country to justify the

---

dignitas and *fama* (honour). See too Aristotle's distinction between public and private spheres in J DeCew 'Privacy' in EN Zalta (ed) *The Stanford Encyclopedia of Philosophy* (2013).

[30] See BM Carson 'Legally speaking: Warren, Brandeis and the creation of the legal concept of privacy' (2008) 20 (2) *Against the Grain* at 55 and ibid.

[31] Ibid.

[32] Banisar and Davies (n 11) at 8.

[33] JS Mill *On Liberty* (1869).

[34] J Locke Two Treatise on Government (1689).

> defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have.'[35]

In 1776, the Swedish Parliament enacted the first law on freedom of information and data protection legislation, the Access to Public Records Act, which allowed the people access to public records and documents in order to examine their accuracy, and ensured that all government-held information be used for legitimate purposes.[36] Shortly thereafter, in 1789, France's National Constituent Assembly adopted the Declaration of the Rights of Man and the Citizen,[37] which defined a collection of individual rights and rights for all men and declared that private property was inviolable and sacred. France prohibited the publication of private facts and set harsh fines for violators in 1858.[38]

In 1890, American authors Warren and Brandeis, in their essay entitled 'The Right to Privacy', cautioned that 'modern enterprise and invention have, through invasions upon his privacy, subjected an individual to mental pain and distress, far greater than could be inflicted by mere bodily injury'.[39] Citing 'political, social, and economic changes' and 'the right to be let alone' as key issues, they argued that a general right to privacy afforded a way to protect the privacy of the individual, and they sought to explain the nature and extent of such protection. They believed that, although privacy was well established in US common law, the development of new technological inventions necessitated explicit and separate privacy recognition and protection.[40] In doing so, they established the foundation for informational privacy, or the 'right to have control over information about oneself'.[41]

---

[35] The Court held that the common law does not recognise the interests of state as a justification for allowing what would otherwise be an unlawful search.

[36] RJ Rodrigues, P Wilson and SJ Schanz 'The Regulation of Privacy and Data Protection in the Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-identifiable Health Databases' (2001) at 89.

[37] The declaration inspired the 1948 United Nations Universal Declaration of Human Rights.

[38] Banisar and Davies (n 11) at 8.

[39] See SD Warren and LD Brandeis 'The right to privacy' (1890) 4 (5) *Harvard Law Review* at 193 and Carson (n 30) at 55.

[40] Roos (n 13) at 375 and 376, 'the right to be let alone' was an early recognition of the right to privacy.

[41] DeCew (n 29); early US cases introducing the right to privacy include *Manola v Stevens; Mackenzie v Soden Mineral Springs Co; Marks v Jaffa; Schuyler v Curtis;* and *Roberson v Rochester Folding Cox Co*.

As a consequence of Warren and Brandeis, and regardless of it initially not receiving widespread recognition as a fundamental right, US courts and the public began endorsing the newly developed right to privacy in the law of tort.[42] In the 1928 US case of *Olmstead v United States,* Brandeis AJ, in his dissenting judgment described privacy as 'the most comprehensive of rights and the right most valued by civilized men'. [43]

Over time the right to privacy, in one form or another, was declared to exist by the majority of US Courts. In 1960, William Prosser, in an attempt to clarify the position, carefully systematised what the US courts had protected over the 70 years following the publication of the Warren and Brandeis paper. He distinguished among four distinct infringements, namely:

> '1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
> 2. Public disclosure of embarrassing private facts about the plaintiff.
> 3. Publicity which places the plaintiff in a false light in the public eye.
> 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness'',[44]

Thus began a more formal recognition and expansion of the right to privacy in the US to include the control of information about individuals. This journey has been and still is being expanded to include unwarranted searches, eavesdropping, surveillance and misuse of one's communications.[45] A conversation about privacy has been the topic of continuing discourse. This conversation must now be broadened in light of the impact of the entire global communications infrastructure.[46]

IV PRIVACY AS A MORAL VALUE OR A FUNDAMENTAL HUMAN RIGHT?

The newly formed political ideas and social principles and structures arising out of the French Revolution and the development of the urban bourgeoisie with private

[42] Ibid.

[43] At 475.

[44] WL Prosser 'Privacy' (1960) 48 (3) *California Law Review* at 389.

[45] Nagel (n 26) at 28.

[46] J Kang 'Informational Privacy in Cyberspace Transactions' (1998) 50 *Stanford Law Review* at 1197.

property and personal individuality paved the way for a modern day construction of privacy rights. The advent of privacy as a legal value emerged more vigorously in Europe after World War II, and the rise of Nazism and Stalinism.[47] As a reaction to the atrocities of the war, freedom, like privacy, became recognised as fundamental to every human being.[48] The 'Big Bother' concern of state surveillance prevalent in Germany during the war years and subsequently in the Soviet bloc was a fear of western countries as the world was in the process of being rebuilt in the 1940s and 1950s.[49]

Despite, or perhaps because of, various critical philosophical debates around, and responses to, its definition and content, many theorists are of the view that privacy is a meaningful and valuable concept, worthy of protection.[50] In effect, the right to privacy has become increasingly more widely accepted as one of the more significant rights of the modern information age.[51]

---

[47] See B Perinan (n 8) at 184 and Edwards (n 9) at 447.

[48] See M Tugendhat & I Christie *The Law of Privacy and the Media* (2002) at 9.

[49] Edwards (n 9) at 447.

[50] See Moore (n 28) for an anthropological perspective on the development of privacy. Ibid at 443 questions whether privacy is an objective concept 'important in the same way to all people' or whether it has 'inherently subjective value', which should be balanced against other values.

[51] Privacy is not only protected by constitutional guarantee in South Africa, but also in other countries, namely, the Netherlands in the 1989 Constitution of the Kingdom of the Netherlands, the Republic of the Philippines in article III of the Constitution of the Republic of the Philippines, of 1987 and the Russian Federation (article 23, Constitution of the Russian Federation, 1993) also offer constitutionally recognised privacy protection. Although the right to privacy is not explicitly mentioned in the Constitution of the United States of America, courts in the US have held that the right to personal privacy is a fundamental liberty deserving of protection. Privacy is implied in the 1st, 3rd, 4th, 5th, 9th Amendments, and specifically in the 'due process' clause contained in the 14th Amendment to the US Constitution. The landmark decision in *Roe v Wade* implied a constitutional right to privacy, which rested on the judicial concept of 'substantive due process', as contained in the 14th Amendment. See Chilapowski (n 7) at 135 who argues that a new level of scrutiny for substantive due process analysis should be recognised in the US. Likewise, in 1961 the House of Lords in the United Kingdom approved the first Right of Privacy Bill. Since then, there has been a long evolution in UK Law from this 1961 enactment and the beginning of privacy, as a specific legal value. Since then, the UK has enacted general human rights legislation in the form of the Human Rights Act of 1998, which incorporates the European Convention of Human Rights into UK law. It has been observed that the influence and guarantee of the right to privacy contained in Article 8 of the European Convention has influenced the UK judiciary to broaden the scope of the cause of action for breach of confidence – now referred to as 'misuse of private information'. Edwards (n 9) at 444 states that the two most important legal regimes governing data protection in the UK are the Data Protection Act of 1998 (informed by the EU Directive) and the law of confidence (a creature of common law). Both legal regimes have been greatly shaped by the guarantee of the right to a private life contained in Article 8 of the European

'Privacy', 'dignity', 'identity', and 'reputation' are aspects of an individual's personality.[52] Burchell submits that all people have a right to privacy and that this, together with one's inherent right to dignity, contributes to that which makes us human.[53] Thus, he states that: '[w]e are fully human not only through engagement with other human beings, but also because others show respect for our private domain'. Dignity and privacy underscore one's individuality and dictate the 'limits of humanity and of human interaction'.[54]

Edmundson asserts that privacy and the right to privacy are 'closely intertwined' and that stating that something is 'private' serves to affirm that the matter or activity in question is 'protected by the right to privacy'.[55] He contends that privacy is a moral right and worthy of protection as a 'positive right or constitutional right'.[56] Clarke also views privacy as a 'moral or legal right'.[57]

However, the nature and scope of the moral right expressed as the 'right to privacy' requires clarification, as any subjective notion of privacy is legally shaped and given definition by legislation and judicial decisions into a general and objective model of privacy. This model is not always stable but is dependent on the social values in force in society, at any given time. This suggests that the standard of privacy reflected in social values can be legally modified by changes in substantive law. [58] Moreover, how effectively these legal rules, be they mere social values or fundamental rights, operate and are enforced within the information age and within the realm of the Internet, should be questioned.[59]

Convention of Human Rights. See further B Markesinis, C O'Cinneide, J Fedtke and M Hunter-Henin 'Concerns and Ideas about the Developing English Law of Privacy (and How Knowledge of Foreign Law Might be of Help)' (2004) 52 (1) *American Journal of Comparative Law* 133 at 157.

[52] Burchell (n 7) at 2.

[53] Ibid.

[54] Ibid.

[55] WA Edmundson 'Privacy' in Golding & Edmundson (eds) *The Blackwell Guide to the Philosophy of Law and Legal Theory* (2005) at 271.

[56] Ibid.

[57] Clarke (n 18) at 60.

[58] See B Perinan (n 8) at 187.

[59] See Edwards (n 9) at 444 and Ibid at 190.

Unfortunately, there is a failure to provide an authoritative definition of informational privacy protection, thus safeguarding the right to privacy by a process of ethical constraints, a legal system, and operational and procedural necessities. The lack of a comprehensive construct of privacy together with the inconsistencies in terminology, a flawed rationale, and discrepancies in principles leads to the unpacking of a legal notion of privacy that is both incoherent and incomplete.[60]

V CONCEPTUAL FOUNDATIONS

The concept of privacy lacks a single, precise, analytically workable or generally accepted meaning or exhaustive definition.[61] Most theorists agree that it is both a meaningful and a valuable concept.[62] There is also agreement that the essence and scope of privacy spans an array of situations encompassing *inter alia* the exclusiveness of the physical space around a person, freedom of thought, control over one's body and information about oneself, and the right to make private decisions without interference. Generally described in Gross, privacy is the limitation of the acquaintance with a person, or with the affairs of his life, which are personal to him.[63]

Despite various definitions being posited in philosophical, political and legal discourse, privacy, though valued as a sphere within which individuals' freedom from interference by others is to be protected, can function negatively, that is, as the cloak under which individuals may hide. Consequently, the multidimensionality and complexity of privacy renders its value open to debate with little consensus amongst theorists.[64] This difficulty in articulating what privacy is has had the regrettable consequence of making privacy law 'ineffective and blind to the larger purposes for which it must serve'.[65]

Certainly, one might expect that privacy exists when, and to the extent, that protection and preservation of an individual's privacy interest is sought and when

[60] NP Terry 'What's wrong with health privacy' (2009) 5 (1) *Journal of Health & Biomedical Law* at 2.

[61] See DeCew (n 29) and Banisar and Davies (n 11) at 6.

[62] See ibid for a more detailed discussion and critique of privacy.

[63] See Gross (n 25) at 36.

[64] See MS Olivier 'Database Privacy Balancing Confidentiality, integrity and availability' (2002) 4 (2) *SIGKDD Explorations Newsletter* 20 at 21.

[65] DJ Solove 'Conceptualizing privacy' (2002) 90 (4) *California Law Review* at 1090.

there is legal recognition of that interest. Yet, privacy seems not always to exist because of such legal recognition. It exists much like the concepts of secrecy, security, or tranquillity, 'by virtue of habits of life appropriate to its existence'.[66] Perhaps because of this, privacy is considered a much broader concept than that galvanised merely by law. Thus, the law does not determine privacy merely as a concept *per se*, but informs the circumstances or situations under which privacy is to be safeguarded and therefore afforded legal protection.

Unfortunately, this persistent lack of clarity and the failure to provide a compelling definition of the term create unease. This is because privacy is widely applauded as an integral tenet of freedom and democracy in modern society and worthy of protection.[67] The lack of a precise definition of privacy does not render it any less important, however, and the need for legal certainty and for an understanding of the range of legal protection offered is clear.[68]

VI CLASSIFICATIONS OF PRIVACY

Despite being the subject of widespread debate amongst theorists, the concept of privacy consists of a commonality of certain fundamental or core elements.[69] These are 'secrecy', that is, 'the extent to which we are known to others' or 'our concealment of information'; 'solitude' or 'the extent to which others have physical access to us'; and lastly, 'anonymity' or 'the extent to which we are the subject of others' attention'.[70] The writings of Warren and Brandeis add two further elements, that of 'personhood', that is, 'the protection of one's personality, individuality, and dignity' and 'intimacy' or 'control over, or limited access to, one's intimate

---

[66] See Gross (n 25) at 36.

[67] See C Ncube 'A Comparative Analysis of Zimbabwean and South African Data Protection Systems', 2004 (2) *The Journal of Information, Law and Technology (JILT)*. See Banisar and Davies (n 11) at 6.

[68] Gross (n 25) at 34, '[o]ur our ability to articulate and apply *principles* of legal protection diminishes, for we become uncertain about precisely what it is that compels us toward protective measures and wherein it differs from what has already been recognized or refused recognition under established legal theory.'

[69] Solove regards privacy not as containing a 'single common characteristic' but rather believes that it 'draw(s) from a common pool of similar elements'. See Solove (n 65) at 1091.

[70] See LA Bygrave 'The place of privacy in data protection law' (2001) 24 (1) *UNSW Law Journal* at 280.

relationships or aspects of life'.[71] There is considerable overlap between the constructions and although the conceptions may fall within different categories, they are by no means independent of each other.

In essence, the privacy boundary seeks, firstly, to avert intrusions into a person's personal or private sphere and, secondly, to circumvent unwarranted publication of what one holds dear or what is worthy of concealment. The scope and meaning of privacy is better clarified according to the interest it seeks to protect.[72] Thus privacy is classified within three different dimensions: as physical (spatial or locational) privacy, decisional privacy and informational privacy.[73] It is from informational privacy that the concept of data protection emerges.[74]

(1) Physical (spatial) privacy

Edmundson describes physical privacy as a person's enjoyment of spaces 'from which others may be excluded' and within which a person's activities are not monitored with their knowledge or consent.[75] Spatial privacy conveys the extent to which a person's territorial solitude may be shielded from unwanted invasion.[76] An example of physical privacy is one's right to be left alone in one's own home. There is a space between what is open to the public and that which people wish to keep to themselves.[77] Although this veil may be partially lifted at times, the management of one's inner life and one's exposure or concealment thereof should be largely, albeit not without qualification, a matter of personal choice.[78]

---

[71] Warren and Brandeis (n 39) at 193. This document, considered to be the foundation of privacy law in the US, gives unique insight into the thinking at the time and was instrumental in informing future thinking on the topic. On the recognition that the meaning of values is ever-changeable, it is stated that '[p]olitical, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the new demands of society'.

[72] DeCew (n 29).

[73] Edmundson (n 55) at 271 and 272. See also Kang (n 46) at 1202.

[74] Edwards (n 9) at 445, 'loosely, the right to control what is known about you'.

[75] Edmundson (n 55) at 272.

[76] Kang (n 46) at 1202.

[77] Banisar and Davies (n 11) at 6.

[78] Where there is criminal activity, for example.

While Edwards describes physical or bodily privacy as 'the right not to be touched or in some way acted on against your will',[79] Perinan describes the content of spatial privacy as that which has 'control over the extent, timing, and circumstances of sharing oneself (physically, behaviourally, or intellectually) with others'.[80]

(2) Decisional privacy

At issue in decisional privacy is the right to 'do something', as opposed to the right to do it in seclusion.[81] This sense of privacy concerns choice and a person's ability to make significant and self-defining decisions regarding his or her life without interference.[82] An example of this is the landmark US case of *Roe v Wade*[83], where the United States Supreme Court ruled that a woman's right to privacy extended to a woman's decision to have an abortion.

(3) Informational privacy

This notion of privacy concerns the control of a person over the processing of their personal information. The processing may include the acquisition, disclosure and use of such information.[84] Informational privacy is considered by Collste a 'subspecies' of the right to autonomy, and includes the right of an individual to control their own affairs and the circulation and dissemination of their information.[85] There is uncertainty as to what the nature and extent of such 'control' is and to what type of 'information' it relates. The type of information protected is defined differently in various countries but typically includes 'personal data', such as 'name, address, date of birth, contact details, financial, medical and social work details, identifiable photos, relationship status', amongst others.[86]

---

[79] Edwards (n 9) at 446.

[80] 'It could be said that beyond privacy there is nothing left or, that privacy represents the most intimate and inner sphere of any individual.' See Perinan (n 8) at 187.

[81] Edmundson (n 55) at 272.

[82] Kang (n 46) at 1202.

[83] 410 U.S. 113 (1973).

[84] Banisar and Davies (n 11) at 6.

[85] Collste (n 25) at 80.

[86] Edwards (n 9) at 445.

Although the three privacy 'types' are differentiated, they are functionally interconnected and their constructions often coincide.[87] Precise definitions and narrow categorisations are not readily possible. This being said, the lack of a strict definition of privacy is equally advantageous, in that there is greater scope for flexibility and for carving out a meaning and interpretation that best suits the situation to which it applies.[88] This ability to be adapted into a dynamic informational environment, for instance, makes it a particularly interesting area of ongoing research.

VII THE RIGHT TO PRIVACY IN THE DIGITAL AGE: DATA PROTECTION

Privacy is much more complex and difficult to define in an online environment.[89] The ramifications and implications of privacy in a digital context are numerous and widespread. Questions of its influence, regulation and protection are not easily resolved, and necessitate a consolidated, multidisciplinary approach between the law and technology.

While the preferred terminology used in Europe is 'data protection'[90], in the US the language tends towards the protection of 'privacy', 'data privacy' or 'information privacy'.[91] Regardless of differences in nomenclature, the focus of protection remains the same, that of 'regulating the processing of data' of persons 'to safeguard, at least partly, the privacy and related interests of those persons'.[92]

Nonetheless, data protection or data privacy, as it is increasingly being called, as an attempt to bridge the North American and European terminologies, has recently acquired a more precise and simplistic definition than that which embraces the complexities and vagueness encountered in defining the right to privacy.[93] Data

---

[87] Kang (n 46) at 1203.

[88] Bygrave (n 70) at 278.

[89] Edwards (n 9) at 443.

[90] This originated and derived from the German term 'Datenschutz'.

[91] Bygrave (n 70) at 165.

[92] Ibid at 166.

[93] Ibid at 168 and also Roos (n 13) at 402 and Pavlou (n 5) at 977 where, for an alternative view, Pavlou states that, as with the concept of privacy, the definition of data protection is the subject of 'much ambiguity and disagreement'. This is because information privacy is a 'complex concept that

protection refers to the concept of allowing individuals to determine when, how and to what extent their personal information is acquired, shared with and used by others.[94]

The central objective of data protection legislation is to safeguard personal privacy by regulating the processing of personal data.[95] This empowers individuals to participate in, and influence, the processing of information about themselves, and introduces the idea of self-determination or, at the very least, places them in a position of co-determination.[96]

While Bélanger and Crossler offer a rich discourse on the definition and nature of information privacy,[97] a concise definition of data protection is provided by Bygrave who defines data protection as 'a set of measures (legal and/or non-legal) aimed at safeguarding persons from detriment resulting from the processing (computerised and/or manual) of information on them, and embodying a group of principles on the processing of personal information'.[98]

It should be borne in mind that concepts, especially those under discussion, are prone to 'definitional instability'. Various definitions abound and are the subject of lengthy and vociferous debate. No sooner is some degree of consensus reached than new issues emerge, once again galvanising the need for further discourse.

---

can be studied from many perspectives, including law, economics, psychology, management, marketing, and Information Systems'.

[94] A Westin *Privacy and Freedom* New (1967) at 7 states '[t]he claim of individuals, groups or institutions to determine for themselves when, how and to what extent, information about them is communicated to others.' Also quoted by CJ Bennett Regulating *Privacy: Data Protection and Public Policy in Europe and the United States* (1992) at 14, Bygrave (n 70) at 279 and Perinan (n 8) at 185.

[95] See A Roos 'Core principles of data protection law' (2006) 39 *CILSA* at 104.

[96] See Bygrave (n 70) at 279, where 'data protection laws rarely give persons an absolute right to dispense with data about themselves as they see fit. Thus, the laws are better viewed as manifestations of an interest in informational co-determination as opposed to self-determination'. See Banisar and Davies (n 11) at 8, where '[p]rivacy can be defined as a fundamental, though not absolute, human right'.

[97] F Bélanger and RE Crossler 'Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems' (2011) 35 (4) *MIS Quarterly* at 1017–1041.

[98] LA Bygrave *Data protection law: Approaching its rationale, logic and limit* (2002) at 2 and Bygrave (n 70) at 279.

VIII DATA PROTECTION AND PRIVACY RIGHTS

The relationship and interaction between the right to privacy and data protection requires clarification. The question to be asked is whether the law should differentiate between these the rights to privacy and data protection.

(1) The relationship between data protection and privacy rights

The relationship between the right to privacy and the right to data protection is not as straightforward as one might expect.[99] While certain theorists view the concepts of privacy and data protection as synonymous and interchangeable, others maintain a contrary view.[100]

While closely related, the terms are not identical. Data protection is typically reserved for 'a set of norms that serve a broader range of interests than simply privacy protection'.[101] While there may be convergence between the concepts, data protection relates specifically to the 'informational' rather than the 'spatial or physical dimensions' of privacy. Although the scope and subject matter of data protection and privacy rights are disparate, albeit often intersecting, adequate justification merits them being treated differently.[102] What the rights do share is that they seek to serve frequently similar objectives.[103] The suggestion is that the rights to data protection and privacy are summarised as 'significantly overlapping yet distinct'.[104]

Although the CJEU (Court of Justice of the European Union) in the *Bavarian Lager* case considered that data protection was a subset of the concept of privacy, the

---

[99] In the US, the term 'information privacy' is used rather than 'data protection'. This is to avoid the possibility that the latter term be linked to intellectual property rights.

[100] See C Cuijpers 'A Private Law Approach to Privacy: Mandatory Law Obliged?' (2007) 4 (4) SCRIPTed 304 at 312. The question of whether data protection and privacy are the same is considered by Cuijpers who is of the opinion that 'data protection and privacy are not the same'. See also Makulilo (n 25) at 164 and O 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* at 569–597 in this regard.

[101] LA Bygrave 'Privacy and Data Protection in an International Perspective' (2010) *Stockholm Institute for Scandinavian Law* at 168.

[102] Lynskey (n 100) at 569–597.

[103] Ibid.

[104] Ibid.

subsequent *Volker* case treated data protection rights as a 'hybrid species' where, in the opinion of Advocate General Sharpston, a clear distinction between the rights to privacy and data protection could be established.[105]

Data protection law is not solely concerned with privacy. Both concepts of privacy and data protection, although they intersect on common ground, such as information control, non-interference and limited accessibility, are at the same time each broader and more comprehensive than the other.[106] Lynsley suggests that the right to privacy cannot be applied to the extensive range of data to which data protection policies apply more appropriately.[107] The risk of conflating these two rights lies in inadvertently subjecting the right to data protection to the restrictions imposed on the right to privacy, thereby impeding its development.[108] Whereas the concept of privacy extends beyond the narrow definition of data protection, data protection likewise includes a multitude of interests, such as data validity and integrity, and the reliance and completeness of data, which may not have a direct bearing on privacy-related values.[109] The right to data protection is thus wider in scope than the right to privacy.[110]

The focus of data protection laws is the processing and managing of data that conforms to an acceptable, legitimate standard. Significantly, data protection legislation aims at safeguarding the privacy and related interests of individuals, while simultaneously securing and balancing the legitimate interests of those processing personal data. Thus, the privacy interests of the individual and the counter-interests of those processing and managing the data are considered and secured. This promotes the belief that conflict between these respective sets of interests can be significantly

---

[105] See Bavarian Lager v Commission and Volker und Markus Schecke and Hartmut Eifert.

[106] See C Kuner 'Data Protection law and International jurisdiction on the Internet (part 1)' (2010) 18 *International Journal of Law and Information Technology* at 176 and C Kuner 'An International Legal Framework for Data Protection: Issues and Prospects' (2009) 25 Computer Law & Security Review 307 at 308, where privacy and data protection is described as 'twins but not identical'.

[107] Lynskey (n 100) at 569.

[108] Ibid.

[109] Cuijpers (n 100) at 313, '[e]ven though in Europe the choice has been made to lift the rules concerning data protection to the constitutional level, the fact remains that the processing of personal data in a lot of cases will not enter into the private sphere of an individual. Therefore, it often will not touch upon the individual's right to privacy'.

[110] Lynskey (n 100).

reduced through appropriate data protection legislative means.[111] Although principles of data protection legislation are similar across regions and legal systems, there is often considerable and substantial difference in the details of the laws.[112]

A further difficulty in the nature of the relationship between data protection and privacy is that data has the potential to acquire a commercial value, thereby becoming a tradable commodity.[113] As an illustration of this, on 23 July 2014, the Brazilian Consumer Protection and Defence Department fined the telecommunications company 'Oi' an amount of €1.2 million for violating user privacy by not notifying its Internet users that their browsing activities had been tracked and on-sold to a third-party.[114] The browsing data had been collected and stored in a database of user profiles, for the stated purpose of improving the users' browsing experience. According to the Justice Ministry, Oi's failure to inform Internet users constituted violations of their rights to information, the principles of good faith and transparency, and the right to privacy and intimacy.[115]

The potential of data to provide certain economic advantage is described as 'propertised'.[116] By vesting a property right in personal data, personal data becomes an economically viable asset and therefore the object of commodification. Personal information is a currency in the digital age.[117] Gunasekara states that '[p]ersonal information has become a valuable commodity, one which provides the raw material for and underpins the success of corporations such as Google and Facebook'.

---

[111] Bygrave (n 98) at 282

[112] Kuner (n 106) at 177.

[113] See the press release: European Commission Memo 'Progress on EU data protection reform now irreversible following European Parliament vote' Strasbourg (2014), where it is estimated 'that the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020'.

[114] C O'Donoghue and K Brimsted 'Brazilian Data Protection Authority fines Internet Provider $1.59m'.

[115] Although the case was based on Brazil's Consumer Law of 1990, a new Internet law (Marco Civil da Internet) has been introduced, in terms of which it is suggested that this case serves as a warning that strong action will be taken, should the new Brazilian Internet law be contravened.

[116] Prins (n 5) at 272.

[117] See G Gunasekara 'Paddling in unison or just paddling? International trends in reforming information privacy law' (2014) 22 (2) *International Journal of Law and Information Technology* at 141.

Individuals can be controlled and their identities stolen or 'mined' to extract value.[118] Consequently, the debate around the term 'big data' has gained momentum in recent years.[119] This is galvanised in the view that digital data represents the latest key asset that organisations can acquire for achieving a competitive financial advantage.[120]

Finally, the ECHR (European Court of Human Rights) attempted to demarcate the realm of privacy from that of data protection.[121] Karanja in his analyses of ECHR case law summarised the case law position with regard to data processing as follows: '[i]t is no longer doubtful that data protection is a human right although the Convention does not state this. '… the Court has boldly manifested data protection principles in its decisions by adopting the language of data protection law'. He goes on to say that what is still lacking 'is a positive statement in the general human rights legislation that human rights protect personal data'. He believes that a statement to that effect would give data protection 'the universal status enjoyed by human rights principles'. Karinga suggests that the EU has addressed this by providing data protection in its Charter of Fundamental Rights and the EU Constitution.[122] Since 2009 data protection has been protected as a fundamental right, next to the right of privacy, in the EU Charter of Fundamental Rights.

(2) Should the law differentiate between the right to privacy and the right to data protection?

The relationship and interaction between the rights to data protection and privacy, based on a comparison between the scope of the two rights and the protection they afford, requires clarification.[123] Two questions arise: What is the difference between the right to privacy and the right to data protection? Is there a convincing rationale to include the right to data protection as an independent right? While these two rights do

---

[118] Ibid.

[119] Big Data is discussed in Chapter 6.

[120] See Esposti (n 7) at 209.

[121] Makulilo (n 25) at 165.

[122] SK Karanja 'Schengen Information System and Border Control Co-Operation: A Transparency and Proportionality Evaluation' PhD Thesis *Faculty of Law University of Oslo* (2006) at 123.

[123] A more detailed discussion regarding the rights to privacy and data protection is contained above.

intersect, largely because of a commonality in their objectives, simply conflating the two rights appears problematic.

Despite this assertion, analysis of CJEU jurisprudence reveals that that court 'consistently conflates the two rights'. The indication is that the CJEU views the right to data protection as little more than 'a facet of the right to privacy''[124] Lynskey observes that on systematic analysis of the two rights, while extensive overlap exists, the rights to data protection and privacy are in fact distinct.[125] Lynskey argues that the right to data protection provides individuals with more extensive protection rights over numerous data types than those offered by the more general right to privacy.[126] The proposition is that, as significant differences are noticeable in the two rights, a detached right to data processing protection merits justification.

Moreover, closer examination reveals that an independent right to data protection enhances control of an individual over their data by, firstly, promoting their individual personality rights, which are placed under threat by the nature of personal data processing and, secondly, by attempting to reduce and address the imbalances in power, which exist between individuals and data processors.[127] The conclusion is that, while 'the content of the right to data protection overlaps significantly with that of the right to privacy, data protection nevertheless merits recognition as an independent right'.[128]

IX MODELS FOR THE REGULATION OF DATA PROTECTION

The models of data and privacy protection are identified in the literature as the comprehensive, sectoral, self-regulatory and technological models, which are all discussed below.[129] In certain countries, more than one model is used concurrently.[130]

---

[124] Lynskey (n 100) at 569–597.

[125] Ibid.

[126] Ibid.

[127] Ibid.

[128] Ibid.

[129] Ncube (n 67) at 1.

[130] Banisar and Davies (n 11) at 13 and 14.

(1) Comprehensive Laws Model

The comprehensive laws model comprises a general law, which regulates and controls the collection, use and dissemination of personal information in both the public and private sectors.[131] A regulatory body is mandated to ensure compliance and oversee the application of this general law. An official within the regulatory body, who is sometimes referred to as a Commissioner, Ombudsman or Registrar, monitors compliance with the data protection laws and directs enquiries into alleged breaches and violations.[132]

The reasons for the advancement of comprehensive data protection laws are threefold: Firstly, they are intended to remedy past injustices. Countries in Central Europe, South America and South Africa, for example, have adopted laws to remedy past privacy violations that occurred under previously repressive regimes. [133] Secondly, comprehensive data protection measures encourage electronic commerce.

Countries, especially in Asia, have thus developed data protection laws in an effort to promote the use of electronic commerce and facilitate electronic transactions. In an attempt to appease users who are uncomfortable with their personal information being used and freely disseminated, data protection laws are being initiated to safeguard their privacy. Lastly, the comprehensive laws set out to ensure that regulations are consistent with Pan-European laws on data protection.[134] Countries in Central and Eastern Europe are thus adopting data protection legislation based on the Council of Europe Convention and the EU Data Protection Regulation. Countries in other regions, such as Canada,[135] for example, have adopted new legislation to ensure that trade will not be adversely affected by non-compliance with the stringent requirements set out in the EU Regulation.[136]

---

[131] R Moshell 'And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend towards Comprehensive Data Protection' (2004–2005) 37 *Texas Tech Law Review* 357 at 366.

[132] D Banisar and S Davies 'Privacy and Human Rights**:** An International Survey of Privacy Laws and Practice' *Global Internet Liberty Campaign* and Banisar and Davies (n 11) at 11.

[133] Ibid.

[134] Ibid.

[135] Personal Information Protection and Electronic Documents Act, as amended.

[136] Banisar and Davies (n 132).

This approach found support and was adopted by the European Union to ensure compliance with its data protection regime, and appears to be the preferred model for most countries adopting data protecting laws.[137] The EU Data Protection Regulation is an example of strict compliance with this model.[138] The approach relies on industry to develop the rules for information and privacy protection, which are then enforced by a private agency.[139] The essential factor underling this model is enforceability so the comprehensive approach works particularly well where there is strict adherence to a general law and governmental oversight.[140] However, the powers of the commissions vary greatly between countries and inadequate resources to enforce the laws are noticed.[141]

A variation of the comprehensive model is the co-regulatory model, which involves cooperation between industry and government, with industry playing an active role in the development and enforcement of the regulation of data protection.[142]

(2) Sectoral Laws Model

This legal model provides governance of a particular sector.[143] The sectoral approach involves no general data protection law but targets specific industries that are perceived to be a threat to data privacy.[144] Despite it being effective when used in conjunction with and complementary to comprehensive data protection laws, on its own it lacks effective enforcement and is weakened by legislative delay, as legislation is tailored to govern only targeted industries.[145] Although a variant of this model has

---

[137] The comprehensive regulatory model has been adopted in Europe, Australia, Hong Kong, New Zealand, Central and Eastern Europe and Canada, amongst others, see Ibid and Banisar and Davies (n 11) at 11 and 13.

[138] Moshell (n 131) at 357 at fn 71.

[139] South African Law Reform Commission 'Privacy and Data Protection' Discussion Paper 109 Project 124 The Commission Pretoria (2005) at 10.

[140] Moshell (n 131) at 366.

[141] Banisar and Davies (n 132).

[142] Australia and Canada are examples of co-regulatory hybrids. See Banisar and Davies (n 11) at 13 and 14.

[143] Ibid.

[144] Moshell (n 131) at 367.

[145] Ibid and Banisar and Davies (n 11) at 14.

been adopted in the United States,[146] it has been the subject of criticism. This model requires legislation to be enacted with each new technology. For this reason, protections are frequently inadequate and out of sync with technological advances and practices. The absence of legal protections for genetic information in the US is an illustration of its limitations.[147]

The sectoral model is a viable approach to data protection regulation when used as a means to aid comprehensive legislation rather than to replace it. Moreover, sectoral laws are of benefit where they provide the necessary detailed protection required to safeguard certain categories of information, such as for instance, within the telecommunications, health care or financial sectors.

(3) Self-Regulation Model

This model provides governance through the establishment, by industry bodies, of various forms of self-regulation and self-policing. Industry self-regulation necessitates that each industry establish their own codes of practice.[148] By industry developing its own standards of regulation, however, a conflict of interests may arise.[149] Moreover, voluntary compliance and self-policing are required, which is not likely when there is, for instance, a conflict of interest or when financial benefit could be gained from non-compliance. Consequently, these codes are often inadequate and not efficiently enforced. This approach is promoted by the US, Singaporean, Japanese and Australian governments.[150]

(4) Technology Model

This model employs private technology based systems to provide protection.[151] Rather than being a model of governance, this approach is more a tool empowering government and individuals to control the use and distribution of their personal data.

---

[146] The US employs a hybrid of the sectoral and self-regulatory models, ibid at 357 at fn 76.

[147] Banisar and Davies (n 132).

[148] Banisar and Davies (n 11) at 14.

[149] Moshell (n 131) at 367.

[150] Banisar and Davies (n 132).

[151] Banisar and Davies (n 11) at 14.

Internet users, for instance, can employ a range of technical programs and systems, which can ensure varying degrees of privacy and data security.[152] The use of various programs and technological systems provide communication protection, for example, encryption, anonymous remailers, proxy servers and digital cash.[153] At issue, however, are the reliability and trustworthiness of these systems.

The European Commission evaluated various technologies in an online environment and stated that technological tools and technical platforms should not act as sufficient replacements to protect privacy. These technological tools must be applied within the context of a legal framework of enforceable data protection rules, providing a minimum and non-negotiable level of privacy protection.[154] In the absence of such a framework, the onus to protect the user shifts primarily onto the user himself. This undermines the internationally established principle (as endorsed by the OECD Guidelines of 1980, the Council of Europe Convention No. 108 of 1981, the UN Guidelines of 1990 and the EU Directives of 95/46/EC and 97/66/EC) that the 'data controller' is responsible for complying with data protection principles.[155]

On a practical note, most Internet users are unlikely to alter pre-configured privacy settings on their online technological platforms and the 'default' position set by the software developers regarding the user's preferences will in all likelihood reflect the overall level of online privacy protection. These default setting may or may not reflect the user's interest in enjoying a high level of privacy protection. Granted, these setting may be subject to user modification, however it is hoped that Internet software developers will implement technological tools that enhance rather than reduce levels of privacy protection.[156]

---

[152] Banisar and Davies (n 132).

[153] Banisar and Davies (n 11) at 14.

[154] European Commission Opinion 1/98 'Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)' (June 1998) at 1.

[155] Ibid.

[156] Ibid.

X CORE CONCEPTS OF DATA PROTECTION

The concept of privacy has evolved at an international level, necessitating the adoption of regulatory principles at a global level. Much of the western world, with Europe at the helm, has progressively instigated broad data protection legislation. Fair data practices regulating the exchange of data across international boundaries were codified in 1980 in the Organisation for Economic Co-operation and Development's (OECD) Guidelines. Consequently, the European Union recognised the need to tightening data protection provisions. The privacy benchmark at an international level can be found in Article 12 of the 1948 Universal Declaration of Human Rights. This article specifically protects territorial and communications privacy. Numerous other international human rights treaties also recognise privacy.[157]

Data protection laws protecting, in particular, the principles of data minimisation, or using data only for a set, lawful purpose and not allowing further processing, and the need for express, informed consent before data is gathered or processed, as found in the 1995 Directive (updated in the EU Regulation) provided much needed protection. Unfortunately, in reality they appear 'to fail to live up to their promise, whether through weakness of implementation or through poorly resourced enforcement'.[158]

It has been over forty years since the first comprehensive national data privacy legislation was enacted, establishing a basic set of core data protection principles.[159] Core concepts of data processing are primarily predicated on the following international documents. These serve as influential or persuasive models of national and international initiatives on data protection. They are the Council of Europe's 1981 Convention for the Protection of Individuals with Regard to the

---

[157] Article 17 of the International Covenant on Civil and Political Rights 1966, Article 14 of the United Nations Convention on Migrant Workers, and Article 16 of the UN Convention of the Protection of the Child. Regional conventions that recognise the right to privacy includes Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

[158] See PA Bernal 'Web 2.5: The Symbiotic Web' (2010) 24 (1) *International Review of Law Computers & Technology* at 36.

[159] Sweden's Data Act of 1973,

Automatic Processing of Personal Data; the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data; the EU Directive; the EU Regulation and the UN Guidelines Concerning Computerised Personal Data Files.

Expressions of data protection vary and considerable overlap exists, nevertheless minimum standards of personal information can be seen as common to the abovementioned declarations. These key concepts are described by Bygrave and include: that data processing should be fair and lawful; that data should be used only for the specified purpose for which it was originally collected; that data collection should be adequate, relevant and not excessive to the purpose of its collection; that data should be kept accurate and up-to-date; that data should be accessible to the subject to allow subject participation and control; that data should be kept securely and destroyed after its purpose has been completed; and lastly, that certain types of data, which may be described as sensitive, should be subject to more stringent controls than other personal data.[160] Crucially, the application of these concepts is of particular significance in health care, and data collected for medical purposes; for instance, an individual's HIV status may theoretically be used when assessing their risk for life or health insurance or employment. However, the use of data for an ulterior purpose, or what Edwards terms 'scope creep', is in practice 'almost impossible to control'.[161]

The above constitute elements that are present in various forms in data protection instruments and that serve to guide their more formal manifestations and abstractions in specific data protection legislation. This being said, however, certain core concepts do have a normative force of their own, having been incorporated into data protection legislation as fully developed legal rules in their own right.[162] Nonetheless, the core principles embody and shape the thinking around data protection law development and regulation. This is seen most obviously and profoundly in the adoption of the principles contained in the COE Convention and

---

[160] South African Law Reform Commission 'Privacy and data protection report' Project 124 (2009) *Pretoria: South African Law Reform Commission* at 8 and Bygrave (n 98) at 57–69, for a detailed explanation of the core principles of data protection.

[161] Edwards (n 9) at 449.

[162] See LA Bygrave (n 98) at 57.

OECD Guidelines on many recent data protection legislation enactments. These guidelines have influenced and been used widely even by non-OECD member countries.[163] Greenleaf, in his most recently updated report on data protection legislation, consolidates the core concepts as:

1. Data quality – relevant, accurate, and up-to-date;
2. Collection – limited, lawful and fair, with consent or knowledge;
3. Purpose specification at time of collection;
4. Notice of purpose and rights at the time of collection;
5. Uses and disclosures limited to purposes specified;
6. Security through reasonable safeguards;
7. Openness – regarding personal data practices;
8. Access – individual right of access;
9. Correction – individual right of correction; and
10. Accountable – data controller with task of compliance.[164]

XI SENSITIVE AND PERSONAL DATA

Can certain data be 'personal' or 'sensitive' and therefore more worthy of protection against disclosure? Privacy encompasses an intrusion into one's private sphere and includes a wide range of personal interests, *inter alia*, personal autonomy, bodily integrity, family life, sanctity of the home. By bringing data protection into this definition, one may seek to understand privacy as 'secrecy, or a right against disclosure of concealed information, or a right to limit access to the self, or control of information pertaining to oneself'.[165] In this regard, only secret, personal information is protected, that is, only such information that forms part of one's private sphere.[166]

---

[163] The OECD Guidelines provide eight principles relating to the collection, purpose, use, quality, security and accountability of organisations in relation to personal information.

[164] G Greenleaf 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (2013) *Journal of Law, Information & Science* at 8 and LA Bygrave 'Data Protection pursuant to the right to privacy in human rights treaties' (1998) 6 (3) *International Journal of Law and Information Technology* at 250.

[165] Prins (n 5) at 270.

[166] Cuijpers (n 100) at 304.

This suggests that not all aspects of data protection are covered by the scope of privacy protection and that that part, which falls outside the private sphere, does not enjoy data protection and is thus not protected as a fundamental human right.

It is critical in defending privacy against violations to refine and explain the concept of 'sensitive information' and the reason why such information is believed to be so.[167] The intimacy-orientated notion of privacy in data protection discourse relates only to individuals' information that is 'intimate' or 'sensitive'. Accordingly, not every disclosure of an individuals' information will necessarily amount in a loss of privacy, only where there is a loss of information that is considered 'sensitive' or 'intimate' is privacy infringed.[168] Julie Inness describes privacy as 'the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions'.[169]

The distinction between personal information that is privacy-sensitive (or what Inness calls 'intimate information'[170]) and that which is not, is culturally dependent as what is considered 'sensitive' or 'intimate' varies between individuals, societies and cultures.[171] While societies are isolated from one other, they develop different moral standards. However, when there is exchange and interaction between individuals belonging to different societies, one can expect an interchange and transference of moral norms, standards and values. Interestingly though, according to Kukathas, with constant and increased interactions and exchanges between differing societies and cultures, one can anticipate a convergence of moral standards and a concurrent adaption of prevailing practices and attitudes. This in the direction towards more universally accepted and standardised values.[172] According to this trend, globalisation should then increase mutual understanding and sharing of moral norms and values, or at the very least, a standardisation of the meaning and value of certain terms such as

---

[167] H Nissenbaum 'Privacy as contextual integrity' (2004) 79 *Washington Law Review* at 128.

[168] See Bygrave (n 70) at 280

[169] Inness (n 25) at 61.

[170] Ibid.

[171] Collste (n 25) at 80.

[172] See C Kukathas 'Explaining moral variety' (1994) 11 (1) *Social Philosophy and policy* at 20 and ibid at 84.

privacy is anticipated. This global convergence on ethics is of particular significance in the world of ICT.

This view of privacy as being only intimacy-orientated is problematic, primarily because intimacy-oriented definitions of privacy 'are unable to anticipate and capture the process by which detailed personal profiles of individuals are created through combining disparate pieces of ostensibly innocuous information'. 'Innocuous' information is information that, on its own, is neither sensitive nor intimate. However, when seemingly innocuous information is aggregated or combined, such as in the creation of detailed personal profiles, an insidious side of data management and manipulation is introduced, with an opportunity for privacy infringement.[173]

Information technology has the ability not only to collate existing data but also to create new data types. An example of this is known as 'clickstream' monitoring, that is, a page-by-page tracking of people's access (or digital footprint), as they navigate through the Internet. Detailed databases of pooled data can in turn reveal one's interests and tastes with unnerving precision. This collection of personal information is referred to as 'intelligence', and such 'intelligence' has the unfortunate effect of shifting the balance of power in favour of the party controlling it. This control equates to power that translates to financial advantage, which promotes the controlling party's interests and has become endemic, with the countervailing power of the individual data subject being limited or non-existent.[174] Thus the concept of online privacy is at odds with the most appealing and advantageous aspects of e-commerce, that is, the ability to infer a set of characteristics on an individual or collective entity based on their online behaviour, also known as profiling, and then for advertisers and interested parties to target them directly.[175]

As stated by Google, their network offers unparalleled reach through text, image, YouTube, and millions of web, domain, video, gaming, and mobile partner sites. In 2013, Google averaged around 6 billion searches a day and reached over 90%

---

[173] Bygrave (n 70) at 280. See also the Brazilian judgment discussed above.

[174] See Clarke (n 18) at 61.

[175] See A Leonard 'Your Profile, Please' (26 June 1997); S Olsen 'Nearly undetectable tracking device raises concern' July 12, 2000 *CNET News* and LA Bygrave 'Minding the machine: Article 15 of the EC data protection directive and automated profiling' (2001) 17 *Computer Law & Security Report* at 17 and ibid.

of Internet users worldwide.[176] Online users who do not access websites owned by Google are also being tracked.[177] The ability of modern technology to identify and track purchasing tendencies by means of, for instance, cookies, web bugs and sniffers, has raised significant privacy issues for individuals.[178] Any use of information, however anonymous and innocuous it may be, nevertheless may be seen to be a form of intrusion into an individual's privacy. The prevalence and power of technology and the Internet creates concern for individual users and presents a clear and real danger to their privacy. Users are of the opinion that invasion of their privacy can cause harm to them (such as identity theft) and that there is a need to safeguard their interests.[179] It is suggested that any conception of privacy that reflects only an intimacy-orientated approach is of relatively little real assistance or appreciation of data protection issues. Although intimacy-orientated conceptions of privacy provisions may place 'extra restrictions on the processing of certain categories of especially sensitive, personal data', data protection laws should not be limited to only sensitive or intimate information of a particular individual.[180]

XII CONCLUSION

The notions of privacy and data protection were addressed in this chapter. The concepts of privacy and data protection were described, as were the implications thereof in eHealth development. The relationship between the rights of privacy and data protection were explored and distinguished. Models for the protection of data and the core concepts in data protection were established. This chapter sought to move beyond the reduction of privacy to a single value, by attempting to emphasise the

---

[176] A Kreitman 'Reach 90% of Internet Users Worldwide (And 10 more reasons to buy traffic from Google AdWords)' (2014) at 1.

[177] See also B van der Sloot & F J Zuiderveen Borgesius 'Google and Personal Data Protection' in A Lopez-Tarruella (ed) *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models* Information Technology and Law Series vol 22 VIII (2012) at 75–111.

[178] Clarke (n 18) at 60.

[179] IM Azmi 'E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill' (2002) 16 (3) *International Review of Law, Computers & Technology* at 317 and see E Clark and G Cho 'Privacy in an e-business world: A question of balance' (2001) 11 (1) *Journal of law, information and science* at 7.

[180] Bygrave (n 70) at 281.

multi-dimensional understanding of privacy, and that which it seeks to safeguard. Sensitive data as a subject of data protection was described.

The following chapter shall consider data protection and privacy measures within Africa and explain the role of privacy in traditional African law.

CHAPTER 4: PRIVACY AND DATA PROTECTION MEASURES WITHIN AFRICA

The continent is too large to describe. It is a veritable ocean, a separate planet, a varied, immensely rich cosmos. Only with the greatest simplification, for the sake of convenience, can we say "Africa". In reality, except as a geographical appellation, Africa does not exist.[1]

Ryszard Kapuściński

[1] Ryszard Kapuściński writes of Africa in his book *The Cobra's Heart:* extracted from the author's book *The Shadow of the Sun* (2007).

I INTRODUCTION

In the context of the emerging eHealth sector in Africa, and in light of the importance of privacy and the protection of health care data, this chapter seeks to determine the extent to which privacy and personal data are indeed being protected on the African continent, and within the African regions and sub-regions. I seek to understand the influence of certain regional and sub-regional data protection instruments, specifically those of the African Union and its most recently promulgated Convention on Cyber Security and Personal Data Protection ('the Malabo Convention').

Finally, I consider whether there is a place for interpreting privacy, and the protection thereof, in a traditional African sense. I question whether a westernised notion of privacy is congruent with the African worldview and how this may be influenced by the African concept of *ubuntu.* I review the approach of the South African courts in adopting an inclusive attitude to customary law. Moreover, I question whether the dictates of the West are necessarily the only, or the only correct, approach to adopt when establishing solutions that are contextually relevant to primarily non-western problems.

II THE AFRICAN POSITION: PRE-DIGITAL AGE

Africa[2] is the second-largest and second-most-populous continent in the world. It comprises six percent of the earth's total surface area and 20.4 percent of the earth's total land mass. To view so vast and diverse a region and such a heterogeneous population as one comparable entity is flawed. As Kapuściński writes of Africa: '[o]nly with the greatest simplification, for the sake of convenience, can we say "Africa"'.[3]

[2] Africa is a vast continent consisting of 54 sovereign states recognised by either the AU or the UN or both, 9 territories and 2 *de facto* independent states with limited recognition. I have restricted my exploratory analysis to the WHO African Region, which consists of 46 member countries, of which 21 are Francophone, 20 are Anglophone, and five are Portuguese-speaking.

[3] Kapuściński (n 1).

Few, if any, data protection policies had been developed within Africa up until the 1960s and 1970s.[4] Prior to this time, there had been limited technological and informational development on the African continent, hence large-scale privacy awareness and regulatory responses were irrelevant. In subsequent years, however, the widespread introduction of the digital era along with the popularity and impact of digital technologies gained momentum. New found privacy concerns arose, driven by the urgency to strengthen protection in this rapidly changing global digital environment. As the impact of digital advancement reached the Africa continent, so too did the acknowledgement that informational privacy measures, critical to the digital revolution, required consideration.

III PRIVACY AND DATA PROTECTION WITHIN AFRICA

Although once lagging behind in the development of data protection laws, Africa has of late transformed its data privacy regimes.[5] The African region is 'catching up with the evolving international standards and norms on internet governance'.[6] Many African countries have included the right to privacy in their constitutions, or human rights instruments, with most countries regarding their constitutions as superior sources of law.[7] The South African Constitution, for instance, has a supremacy clause in Section 2.

Privacy underpins human dignity and is a central tenet of most democratic societies. Despite being well established in certain African constitutions, the right to privacy is not, however, always comprehensively or comparably defined between

---

[4] AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* at 81.

[5] C Rich 'Privacy Laws in Africa and the Middle East' (2014) 13 *Privacy and Security Law Report* at 1.

[6] A Gwagwa 'To what extent are Africa's regional and national cybersecurity regulatory frameworks keeping up with the emerging international norms on the protection of privacy and civil liberties in the cyberspace?'

[7] This may not be entirely correct in jurisdictions where Islamic religion and practice prevail, for instance, in Somali where *Sharia* law may be considered a primary source of law and superior law to that of constitution. See S Mancuso 'Legal transplants and the economic development: Civil Law vs Common Law?' (2009) *Springer* at 75. See MM Carauna and JA Cannataci 'European Union Privacy and Data Protection Principles: Compatibility with Culture and Legal Frameworks in Islamic States' (2007) 16 (2) *Information & Communications Technology Law* at 99–124.

African countries. Kenya and Malawi, for example, have included the right to privacy in their constitutions. Likewise, the Rwandan Constitution provides for the right to privacy in Article 22, as does the Tanzanian Constitution,[8] and the Constitution of the Republic of Ghana.

Privacy rights encompass not only physical or bodily privacy, but also information, communication or data privacy. An example of this is to be found in the Zambian Constitution, which includes the right not to have information relating to a person's family, health status or private affairs unlawfully revealed. General protection is afforded to persons, which is then extended to violations of their private communications and correspondence. The Constitution of Mozambique frames the right to privacy in a broader sense than elsewhere in the region with Article 71 providing specifically for the ''[u]se of computerised data'.

Nevertheless, most African constitutions call for the national legislature to align itself with, and uphold privacy rights, with the substance and scope of the right more carefully demarcated and detailed in generic or specific privacy protection legislation.

To this end, Burkina Faso, Tunisia, Morocco, and Mauritius (all Francophone countries) have adopted comprehensive data protection legislation.[9] According to Greenleaf and Georges, Africa is now leading the expansion of global data protection legislation.[10] Encouragingly, to date 21 African countries are noted as having privacy laws that regulate the collection and use of personal data.[11] These laws have either been recently enacted or amended, including Cape Verde,[12] Burkina Faso,[13] Gabon,[14]

---

[8] Article 16 (1) of the Constitution of the United Republic of Tanzania of 1977.

[9] LA Bygrave 'Privacy and Data Protection in an International Perspective' (2010) 56 *Scandinavian Studies in Law* 165–200 at 193. See ES Nwauche *An Overview of Data Protection and Privacy Legislation in Africa* (2013).

[10] G Greenleaf and M Georges 'The African Union's data privacy Convention: A major step toward global consistency?' (2014) 131 *Privacy Laws and Business International Report* at 18–21.

[11] See Rich (n 5) at B3. See G Greenleaf '120 national data privacy laws now include Indonesia and Turkey' (2017) Privacy Laws and Business International Report No. 145 10-26.

[12] The Law on Protection of Personal Data (Cape Verde Law) amended in 2013. See JL Traça and B Embry 'An overview of the legal regime for data protection in Cape Verde' (2011) 1 (4*) International Data Privacy Law* at 249.

[13] Law on Protection of Personal Information providing protection and Law No. 010–2004 on the Protection of Personal Data (Burkina Faso Law) of 2004.

[14] Law No. 001/2011 on the Protection of Personal Data (Gabon Law) of 2011.

Mauritius,[15] Tunisia,[16] Morocco,[17] Seychelles,[18] Cote D'Ivoire,[19] South Africa, Lesotho, Mali[20] and Ghana.[21] The most recent of these is the protection of personal data law adopted by Madagascar on 9 January 2015.[22]

Significant regional disparity in the adoption of privacy laws is noticed between the enactment of data protection laws in countries in the economic communities of East and West Africa.[23] African countries, for instance, Kenya[24], Tanzania[25], Uganda[26] and Nigeria[27], are expecting data protection laws to be enacted in the near future. The Government of Uganda, for instance, on 15 November 2014, opened a public consultation process regarding the country's Data Protection and

---

[15] The Data Protection Act No. XV of 2004 and Data Protection Regulations of 2009.

[16] Organic Law No. 2004–63 on Personal Data Protection (Tunisian Law) of 2004 (3 PVLR 1030, 9/6/04).

[17] Law No. 09–08 on the Protection of Individuals in relation to the processing of personal data (Moroccan Law) of 2009 (8 PVLR 563, 4/13/09).

[18] The Data Protection Act No. 9 of 2003 (Seychelles Law).

[19] Law No. 2013–450 on Protection of Personal Data (Cote D'Ivoire Law) of 2013.

[20] Law No. 2013/015 on the Protection of Personal Data (Mali Law) of 2013.

[21] The Data Protection Act 843 of 2012 passed by Ghana's Parliament in March 2012 and article 18 (2) of the 1992 Constitution.

[22] Article 28 of the Madagascan legislation creates an independent Data Protection Authority.

[23] DataGuidance Africa Advisory 'Africa: Regional disparity in the adoption of privacy laws revealed' April 2015.

[24] The Data Protection Bill of 2013 (expected to be tabled at the end of May 2014). The Bill was still being debated as of February 2016 and is yet to be passed. Also Article 31 (c) and (d) of the Constitution of Kenya of 2010 and The Cyber Security and Protection Bill of 2016.

[25] See ABP Magalla and GE Kabuje 'The Law of Privacy in Tanzania: A discussion on the challenges affecting privacy in digital environment' (2015) at 1. Article 16 of the Constitution of the Republic of Tanzania and the Tanzanian Data Protection and Privacy Bill of 2013.

[26] Article 27 of the Constitution of the Republic of Uganda, 1995 and the Uganda Communications Act of 2000. The Data Protection and Privacy Bill of 2015 is an attempt to rectify this position. See D van der Merwe 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda (2014) 17 (1) *PER* at 310 for the domestic legislative position in Uganda.

[27] In Nigeria, a right to privacy is provided for in section 37 of the Constitution of the Federal Republic of Nigeria of 1999. The Personal Information and Data Protection Bill is an attempt to rectify this position. See in this regard AS Adeniyi 'The need for data protection law in Nigeria' (2012) *Communications and IT Law* at 1 and also A Kusamotu 'Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by article 25 of European union directive 95/46' (2007) 16 (2) *Information and Communications Technology Law* at 149 and 152.

Privacy Bill, 2015. If passed by the Ugandan Parliament, the Bill would become Uganda's first piece of legislation that focuses exclusively on privacy and data protection.

Yet, despite modest progress being made thus far, the expectation is that the pace of legislative enactment will continue to accelerate in Africa. This is largely due to the requirements stipulated in the EU Regulation, which provides that the international transfer of personal data to third countries, that is, to non-European Union member states (which would include African countries) can only occur where such country can guarantee an 'adequate' level of data protection.[28] Thus far the EU Commission has recognised only a few countries outside of the EU as providing 'adequate' protection.[29] Noticeably and disturbingly, there is a complete absence of any African countries.

The repercussions for African countries are clear, and it serves to accelerate the emergence of EU compliant data protection legislative measures in Africa.[30] Additionally, the enormous increase in the volume and usage of information communication technology in Africa, and the realisation of the significant threats to data safety, are acting as a catalyst for the advancement of a solid body of privacy legislation in Africa.[31]

IV AFRICAN REGIONAL AND SUB-REGIONAL PRIVACY AND DATA PROTECTION MEASURES

Various regional and sub-regional instruments exist in an attempt to safeguard data within the African continent.

---

[28] Articles 40 through 45 of the EU Regulation set out the principle for transfers, the adequacy decision, appropriate safeguards and international co-operation for the protection of personal data. See Makulilo (n 4) at 163.

[29] Andorra, Argentina, Canada, Faroe Islands, Guernsey, Iceland, Isle of Man, Israel, Jersey, Switzerland, Lichtenstein, New Zealand, Norway, Switzerland and Uruguay.

[30] See Kusamotu (n 27) at 149.

[31] See AB Makulilo '"One size fits all"': Does Europe impose its data protection regime on Africa?' (2013) 7 *Datenschutz und Datensicherheit-DuD* at 447.

(1) African regional measures

Certain African regional instruments considered are the African Charter, the Arab Charter, the Malabo Convention, and the African Declaration on Internet Rights and Freedoms. These measures seek to advance the right to privacy and data protection within the region.

(i) The African Charter on Human and People's Rights and the Arab Charter on Human Rights

The African Charter on Human and People's Rights of 1981[32] was inspired by African legal philosophy, while taking cognisance of African needs. A fundamental difference between the Charter and its European and US counterparts is that it places reliance on principles 'primarily African in nature'.[33] Despite its intention to promote human rights in Africa, however, the Charter fails to display any willingness to embrace a culture of privacy. The deliberate disregard and omission of any reference with regard to the importance of the right to privacy and data protection on the continent is notable and disturbing.[34]

For the sake of completeness, a discourse on regional initiatives in the protection of human rights in Africa should mention the Arab Charter on Human Rights.[35] This charter is an important instrument, as it affects in excess of 395 million people, though not all African.[36] It has been signed by a number of predominately northern African states, including Egypt, Tunisia and Algeria. The Arab Charter serves as a valuable regional instrument in encouraging progress by Arab states in the area of human rights, including the right to privacy.

---

[32] African [Banjul] Charter on Human and People's Rights adopted June 27 1981 OAU Doc. CAB/LEG/67/3 rev.5 21 I.L.M. 58 (1982) entered into force October 1986.

[33] R Gittleman 'The African Charter on Human and Peoples' Rights: A legal Analysis' (1982) 22 (4) *Virginia Journal of International Law* at 667, 674 and 675.

[34] LA Bygrave 'Data Protection pursuant to the right to privacy in human rights treaties' (1998) 6 (3) *International Journal of Law and Information Technology* at 251. See also D Banisar 'Linking ICTs, the right to privacy, freedom of expression and access to information' (2010) 16 (1) *East African Journal of peace and human rights* 124–154 at 132 for legal protections.

[35] League of Arab States *Arab Charter on Human Rights* (2004).

[36] M Rishmawi 'The Arab charter on Human Rights and the League of Arab States: An update' (2010) 10 (1) Human Rights Law Review at 169–178.

(ii) African Union Convention on Cyber Security and Personal Data Protection: 'The Malabo Convention'

Previously known as the Organization of African Unity,[37] the African Union is a union of 54 African countries.[38] The Malabo Convention, adopted in June 2014, is an attempt to address certain cyber law uncertainties.[39] It is the first treaty outside of Europe to regulate personal data protection comprehensively.

a. Intention of the Convention

The Malabo Convention seeks to harmonise African cyber legislations and to elevate the rhetoric of 'protection of personal privacy' to an international level. Moreover, it intends to establish an appropriate normative framework consistent with the African legal, cultural, economic and social environment, for cyber security and personal data protection within the context of e-commerce and e-transactions.[40] The Malabo Convention represents a shared coordinated African position and seeks to reflect current legal thinking on the processing of personal information and its impact on the human rights of privacy, dignity, integrity, personality and autonomy. In recognising the increasing interdependence of African states, it calls for concerted action to be taken to protect the rights of individuals in 'the establishment of an appropriate normative framework'.[41]

---

[37] See AB Makulilo (n 4) at 81.

[38] Created in terms of the Constitutive Act of the African Union.

[39] See the African Union Convention on Cyber Security and Personal Data Protection adopted during the 23rd Ordinary Session of the Summit of the African Union (2014) ('the Malabo Convention' or 'the Convention') and its predecessor, the Draft African Union Convention on the Establishment of a Legal Framework conducive to Cyber Security in Africa (2012), African Union Commission. The Malabo Convention replaces the provisions of the Abidjan Declaration adopted on 22 February 2012 and the Addis Ababa Declaration adopted on 22 June 2012 on the Harmonisation of Cyber Legislation in Africa.

[40] See for content on the draft convention of 2012, UJ Orji *Cybersecurity Law and Regulation* (2012) at 135.

[41] Preamble Malabo Convention at 1.

The preamble to the Malabo Convention identifies certain major obstacles to the development of electronic commerce in Africa related to security issues.[42] Whereas the Draft Convention[43] was criticised for not adequately addressing privacy protection, the adopted version enjoins member states to enact legal and institutional frameworks for data protection and cyber security based on the stipulated provisions within the convention, thereby aligning themselves with the predetermined minimum standard of protection required.

The overall intention of the Malabo Convention is to define the objectives for an African information society and to strengthen existing legislation in member states and within the Regional Economic Communities. Its adoption seeks to maximise African and international experiences and expertise in cyber legislation and to accelerate relevant reforms in African member states. This is to be accomplished by providing a normative framework consistent with an African legal, cultural, economic and social environment. Its purpose is to balance the use of information and communication technologies with the protection of the privacy of individuals, while guaranteeing the free flow of information across borders.

b. Scope of the Convention

The Malabo Convention encompasses three central issues: electronic transactions, personal data protection and cyber-crimes. Chapter II of the Malabo Convention is of particularly relevance herein, as it focuses on the protection of personal data. The scope of application of the Convention is set out in Article 9. Its scope extends to both the public and private sectors generally, and to automated and non-automated processing.[44] Processing relating to 'public security, defence, research, criminal prosecution or State security' is subject to certain exceptions, as circumscribed in specific provisions in existing legislation. Exemptions include processing exclusively for an individual's 'personal or household activities', unless such processing is 'for systematic communication to third parties or for dissemination'.[45] Article 14 (3)

[42] Preamble at 2.

[43] Ibid.

[44] Articles 9 (1)(a) and (b).

[45] Article 9 (2)(a).

provides that processing for journalistic or research purposes is exempt in certain circumstances.

c. Principles in the Convention

Section III outlines the basic principles governing the processing of personal data. Articles 13 to 23 set out the basic principles governing the processing of personal data.[46] Pursuant to the need for tighter regulation, the Malabo Convention outlines the substantive principles that ought to be adhered to in processing personal data. With regard to privacy, Chapter II of the Malabo Convention contains specific personal data protection principles.[47] Principles include consent and legitimacy, [48] lawfulness and fairness, [49] purpose, relevance and storage of processed personal data, [50] accuracy,[51] transparency[52] and confidentiality and security of personal data.[53]

d. Rights of data subjects and obligations of data controllers

The Malabo Convention sets out the data subjects' rights and the obligations of personal data controllers.[54] Data subjects' rights include the right to information, or notification,[55] the right of access,[56] the right to object[57] and the right of rectification and erasure.[58] The obligations of data controllers include confidentiality obligations,[59] security obligations,[60] storage obligations[61] and sustainability obligations.[62]

---

[46] Section III Articles 13 (Principles 1–6) to 23.

[47] The basic principles of data processing in the Convention are contained in Articles 13 (1) through (6) and Article 14.

[48] Article 13 Principle 1.

[49] Principle 2.

[50] Principle 3.

[51] Principle 4.

[52] Principle 5.

[53] Principle 6.

[54] Section IV Articles 16 to 29 and Section V Articles 20 to 23.

[55] Article 16.

[56] Article 17.

[57] Article 18.

[58] Article 19.

e. Sensitive data

Article 14 stipulates specific principles for the processing of sensitive data. 'Sensitive data' is defined in Article 1 as all personal data 'relating to religious, philosophical, political and trade-union opinions and activities, as well as to sex life or race, health, social measures, legal proceedings and penal or administrative sanctions'. Moreover, Article 14 (1) prohibits any data collection and processing 'revealing racial, ethnic, and regional origin, parental affiliations, political opinions, religious or philosophical beliefs, trade union membership, sex life and genetic information or, more generally, data on the state of health of the data subject'. Exceptions to this prohibition are contained in Article 14 (2). The categories of sensitive data appear to be limited to only those stipulated within the section.

f. Data transference

Article 14 (6)(a) stipulates that a data controller 'shall not transfer personal data' to countries outside the AU unless the recipient country can ensure 'an adequate level of protection'. In certain instances, prior 'authorisation' by the Data Protection Authority is necessary to transfer data in terms of Article 14 (6)(b). Unfortunately, the term 'adequate level' is not defined in the Convention, neither is it determined how findings of 'adequacy' are to be made.[63] The 'adequacy' requirement does not apply to AU member states, irrespective of whether or not they have ratified the Convention, but only to non-AU member countries. Thus, AU member states are free to adopt any data export provisions they choose in relation to each other.[64]

In terms of Article 9 (1)(c), the Malabo Convention only applies to the 'processing of data undertaken within the territory' of a member state of the AU.

---

[59] Article 20.

[60] Article 21.

[61] Article 22.

[62] Article 23.

[63] Greenleaf and Georges (n 10) at 18–21.

[64] Ibid.

Thus, extra-territorial application is not required, but neither is it forbidden.[65] Concerning the international movement of personal data, the Convention is therefore consistent in only requiring minimum standards of protection, while allowing protections that are more extensive.[66]

g. Enforcement and formalities

Chapter II Section II establishes an institutional framework for the protection of personal data by providing for a 'national protection authority'.[67] This authority is responsible for the protection of personal data in each member state of the AU and is tasked in Article 12 (1) with ensuring that the processing of personal data is consistent with the provisions of the Malabo Convention. Additionally, in Article 12 (2), the independent national protection authority is to ensure that information communication technologies do no constitute a threat to public freedoms and to the private lives of citizens.[68]

(iii) African Declaration on Internet Rights and Freedoms

The African Declaration on Internet Rights and Freedoms was launched in September 2014 in South Africa.[69] In its preamble, the Declaration affirms that the Internet is 'a vital tool for the realisation of the right of all people to participate freely in the governance of their country, and to enjoy equal access to public services' and that it is 'the responsibility of states to respect, protect and fulfil the human rights of all people' including '…individual rights to privacy'. Moreover, the Declaration emphasised 'that the Internet is particularly relevant to social, economic and human development in Africa' and that '…the Internet is an enabling space and resource for the realisation of all human rights'. To this end, the Declaration sets out various key

[65] Ibid.

[66] Ibid.

[67] Section II Articles 11 and 12.

[68] Article 12 (2)(a)–(o) sets out the protection authorities responsibilities.

[69] At the 18th annual Highway Africa Conference South Africa ('the Declaration'). Available at http://africaninternetrights.org/articles/ (accessed 27 November 2016).

principles to inform policy and legislative processes on Internet rights, freedoms and governance in Africa.

Article 6 sets out the principle of privacy and data protection. In realising the right to privacy, the Declaration calls for 'compliance with well-established data protection principles'. Although not specifically mentioned in the Declaration, this is most likely a reference to the provisions contained in the Malabo Convention.[70]

(2) African sub-regional measures

African sub-regional measures considered are those emanating from ECOWAS, EAC, SADC and ECCAS.

(i) ECOWAS

There was increased activity among francophone African data protection authorities, with the Association of Francophone Data Protection Authorities (AFAPDP), which unites 27 data protection authorities from the 24 countries that are members of the Organisation Internationale de la Francophonie (OIF)[71] tasked with promoting co-operation and harmonisation between French-speaking countries in the field of data protection and providing expertise for countries that do not have legislation concerning data protection.[72] Key support came from UNCTAD's e-Commerce and Law Reform Programme and from the AFAPDP for Franco-phone Africa.

In 2010, in an attempt to standardise and harmonise the emerging national data protection legislation in their respective countries, and to prevent the disruption of the flow of personal data, the Economic Community of West African States (ECOWAS), a group of fifteen West African member states, adopted a sub-regional framework for its member states.[73] The Act provides that the content of the data protection laws in

---

[70] Greenleaf and Georges (n 10) at 18–21.

[71] Albania, Andorra, Austria, Belgium, Bulgaria, Burkina Faso, Canada (federal, New Brunswick, (Quebec), Cape Verde, Cyprus, Croatia, France, Greece, Hungary, Lithuania, Luxembourg, Macedonia, Monaco, Poland, Romania, Senegal, Slovakia, Slovenia, Switzerland and Tunisia.

[72] ECOWAS Treaty 1975 as revised in 1991, Art.3. A supplementary Act ECOWAS. Supplementary Act A/SA.1/01/07 on the Harmonisation of Policies and the Regulatory Framework for the Information and Communication Technology (ICT) Sector 2007.

[73] The ECOWAS Supplementary Act on Personal Data Protection of 2010.

the individual states should be influenced very strongly by the EU Directive and that a data protection authority should be established.[74] However, the legal vacuum created by online transactions is not satisfactory dealt with by the Supplementary Act.[75]

Generally, West Africa has a developed legal framework of privacy protection at a sub-regional level with the strongest developments in Africa emanating from ECOWAS.[76] When compared to other sub-regions within Africa, ECOWAS is described as the most vibrant and dynamic sub-regionals in Africa.[77] Of the 15 member states of ECOWAS, as at 2013, five had enacted laws, namely, Benin, Burkina Faso, Cape Verde, Senegal and Ghana, with Nigeria, Niger, Ivory Coast and Mali having data protection legislations, which are fully in force and have established data protection regulators.[78] Only six ECOWAS countries have yet to make legislative progress in this regard.[79] Three other member states of ECOWAS have passed data protection legislation but are yet to establish a data protection regulator. Data protection laws have also been drafted, although not yet enacted, in two other ECOWAS member countries.[80]

(ii) EAC

The East African Community (EAC) comprises five countries: Kenya, Uganda, the United Republic of Tanzania, Rwanda and Burundi.[81] The EAC has the objective of widening the process of integration between its members, thereby creating conditions favourable for regional economic development. A focused privacy protection policy is found in the EAC Legal Framework for Cyber Laws 2008/2011. The cyber law

---

[74] Greenleaf (n 11) and again in G Greenleaf 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (2013) *Journal of Law, Information & Science* at 19.

[75] The principles of data processing are covered in Chapter V of the Supplementary Act.

[76] Makulilo (n 4) at 163 and Greenleaf (n 74) at 18.

[77] See A Banjo 'The ECOWAS Court and the Politics of Access to Justice in West Africa' (2007) 32 (1) *CODESRIA Africa Development* at 70 and Makulilo (n 4) at 82.

[78] DataGuidance Africa Advisory (n 23) at 1.

[79] In certain ECOWAS member states, Niger being one, treaties can have direct effect and be legally binding without requiring local enactment.

[80] DataGuidance Africa Advisory (n 23) at 1.

[81] Established in terms of the Treaty for the Establishment of the East African Community and later amended in December 2006 and August 2007.

reform was developed in two phases, namely, the EAC Legal Framework for Cyber Laws (Phase I and II).[82]

The aim of these frameworks is to develop standardised guidelines to assist in the enactment and implementation of national cyber legislation within the EAC region. The primary purpose for the framework is the harmonisation and standardisation of the establishment of policies and regulations in the sub-region.[83] The reformation of regulatory principles is based primarily on transparency, flexibility, regional harmonisation, proportionality and legal certainty, these being the core concepts underpinning regulatory frameworks in other similarly integrated regional communities and the European Union legislation.[84] Although the recommendations lack substantive data protection principles, they encourage their member states to reflect international best practices by adopting data protection legislation.[85]

In contrast to the ECOWAS, limited data protection has been enacted in the EAC.[86] A factor contributing to the rather slow process of harmonising law in the East African region is due, at least to some extent, to the two very different underlying legal regimes, which apply within the region itself. While Kenya, the United Republic of Tanzania and Uganda follow a common law system, both Burundi and Rwanda subscribe to a predominantly civil law system, which is resulting in divergent legal practices and procedures between these countries.[87]

Although East African Community member countries have to ensure that their domestic legislation complies with the Community's Cyber Laws Framework, they are, and have been, at various stages in the development of their national privacy and

---

[82] The framework for cyberlaw has been developed in two phases. See East African Community East African Legislative Assembly Report of the Committee on communications, trade and investments on the on-spot assessment of regional cooperation in ICT November 2013 at 10 and UNCTAD 'Harmonizing Cyberlaws and Regulations: The experience of the East African Community' (2012) *United Nations* at 7.

[83] See Makulilo (n 4) at 84 and van der Merwe (n 26) at 301.

[84] East African Community East African Legislative Assembly Report of the Committee on communications, trade and investments on the on-spot assessment of regional cooperation in ICT November 2013 at 9.

[85] Makulilo (n 4) at 42–50.

[86] DataGuidance Africa Advisory (n 23) at 1.

[87] UNCTAD (n 82) at 2.

cyber legislation and have been making progress, albeit slowly and steadily, at their own pace. Subsequently, harmonisation has become a more pressing policy issue, with support coming from UNCTAD's e-Commerce and the Law Reform Programme focused on the East Africa Community.

Despite a number of hurdles, progress has been made in the East African region.[88] Kenya drafted data protection legislation in 2009, which was subsequently revised in 2013.[89] This was followed by the Tanzanian Data Protection and Privacy Bill of 2013. In November 2014, Uganda engaged in public consultation regarding the Data Protection and Privacy Bill of 2014. The Bill was still being debated as of February 2016 and is yet to be passed. If enacted by the Ugandan Parliament, the Bill would become Uganda's first piece of legislation that focuses exclusively on privacy and data protection. Development in this regard has required a participatory and consultative approach to be a meaningful form of synergy and regulatory convergence in legal development between the countries and within the sub-regions.[90]

(iii) SADC

The Southern African Development Community (SADC), established in 1980, comprises various member states, namely, Angola, Botswana, the Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, South Africa, Swaziland, Seychelles, Tanzania, Zambia and Zimbabwe.[91] The objective of SADC is to promote the harmonisation and standardisation of legal instruments within the region and to improve cooperation between member states, including the development of electronic technology. With regard to privacy and data protection legislation, however, only five SADC member states, namely, Seychelles (2003), Mauritius (2004), Angola (2011), Lesotho (2012) and South Africa (2013), have adopted comprehensive data privacy legislation.[92]

---

[88] Greenleaf (n 74) at 19.

[89] The Data Protection Bill of 2013.

[90] C Stephanou 'Regulatory Convergence in the Wider Europe Region: Goals and Means' (2003) *Associazione Universitaria di Studi Europei ECSA Italy*.

[91] Declaration and Treaty of SADC as revised in 1992.

[92] Makulilo (n 4) at 86.

At a sub-regional level, SADC is still considering drafts of data protection model law, most notably the SADC Data Protection Model Law of 2012.[93] The intention of such model law is to ensure that the widespread use of ICT does not result in the concurrent weakening of personal data protection. It seeks to give effect to the principles of data protection by placing limitations on the processing of personal data. Moreover, its purpose is to combat violations of privacy arising from the unlawful and/or unfair collection, processing, transmission, storage and use of data activities.

As South Africa plays an influential role in regional economic development, the enactment of the Protection of Personal Information Act No. 4 of 2013 (POPI Act) is expected to affect and expedite the promulgation of other SADC member states' data protection legislation significantly.

(iv) ECCAS

The purpose of the Economic Community of Central African States (ECCAS) is to achieve collective autonomy, raise the standard of living of its peoples and maintain economic stability through harmonious regional cooperation. Its ultimate goal is to establish a Central African Common Market.[94] Central Africa has the least developed data privacy policy, when compared to other African sub-regions.[95] Sub-regional data protection measures are being undertaken by the ECCAS, with the support of partners, such as the International Telecommunication Union (ITU) and the Economic Commission of Africa (ECA).[96] The model law on the protection of personal information is undergoing internal national review and stakeholder consultations. Cameroon, for instance, holds huge potential capacity of growing into a major ICT

[93] J-M van Gyseghem 'Model Law on Data Protection Support for Harmonization of ICT Policies in Sub-Saharan Africa' *International Telecommunications Union* (ITU) 06/02/2012.

[94] It consists of Angola, Burundi, Cameroon, Central African Republic, Chad, the Democratic Republic of the Congo, Congo (Brazzaville), Equatorial Guinea, Gabon, Rwanda and Sao Tome and Principe.

[95] Makulilo (n 4) at 87.

[96] Ibid.

development hub within the Central African region.[97] ICT development is facilitated by extensive multilateral, regional and bilateral cooperation.[98]

Although the sub-region is supportive of developing a bold ICT approach to the deployment of policy, coherent strategies in advancing the processing and protection of information and the harmonisation of privacy policies within the region are sorely limited, lacking direction or any hope of a quick solution.[99]

V PRIVACY IN TRADITIONAL AFRICAN LAW

Whether the notion of privacy is embraced within a traditional African context will now be considered. Are human rights to be found embedded within broader African values and what has been the approach of the South African courts to safeguard privacy protection as manifest within traditional African law? Lastly, the concept of *ubuntu* as a social construct will be considered as a means of furthering privacy rights.

(1) Human Rights and African Values?

The relevance of African values with regard to privacy and its role in health care is not easily determined. Whether it is prudent to apply certain values to the vastness that is Africa, and to such heterogeneous populations, where a complex blend of cultural values and divergent traditions exist, is questionable.[100] At issue is whether there is a point at which the regional multiplicity of African value systems becomes contextually positioned to transcend regional diversity? It must also be considered whether privacy laws are a cultural construct, and to what extent this informs decision making with regard to health care privacy policies.[101] Gutwirth articulates the situation as follows: '[s]hed privacy of its institutional, social, cultural, religious,

---

[97] National Policy for the Development of Information and Communication Technologies (2007) *National Agency for Information and Communication Technologies* at 17.

[98] Ibid at 37.

[99] Ibid at 19.

[100] S Gutwirth *Privacy and the Information age* (2002) at 29.

[101] S Cockcroft, N Sandhu and A Norris 'How does national culture affect citizens' rights of access to personal health information and informed consent?' (2009) 15 (3) *Health Informatics Journal* at 230.

historical, and epistemological context, and it becomes a useless, naked notion, bare to the bone'.[102]

Although the effect of culture as a demographic indicator has been used in various information privacy studies,[103] few studies have explored the influence that cultural diversity has had on domestic privacy regulation.[104] Cockcroft *et al.* propose the existence of a cultural component to patients' rights of privacy and the impact such cultural dimensions have on the adoption of health information privacy regulation. They provide empirical evidence of the effect and role of national culture as informing, for instance, the inclusion and content of informed consent provisions, in the governance of privacy in health care.[105] Based on their findings, they conclude that: '… in a true democracy, information privacy and consent concerns (*driven in part by culture*) should match policy'.[106]

A significant driver of cultural bias may be religious beliefs, creating a 'new composite cultural sensitivity and ethical tradition'.[107] While Biggar argues that religion ought to be included in any discourse on medical ethics,[108] other authors respond in broadly utilitarian terms, and adopt a strictly secular approach to ethical considerations in medicine.[109] The importance of values and traditions, whether derivations of religious, social or cultural philosophies, is echoed by Andoh who writes:

> '[i]n order that African traditional ethical values are not seen as irrelevant for contemporary society and researchers, there is a serious need for bioethics in Africa to reclaim and return to the roots of African thinking so as to reconsolidate a true African authenticity. For bioethics to be authentically African, Africans must

[102] Gutwirth (n 100) at 29.

[103] S Bellman, EJ Johnson, SJ Kobrin and GL Lohse 'International differences in information privacy concerns: A global survey of consumers' (2004) 20 (5) *Information Society* 313–324 and JB Earp, AI Anton, L Aiman-Smith and WH Stufflebeam 'Examining internet privacy policies within the context of user privacy values' (2005) 52 (2) *IEEE Transactions on Engineering Management* 227–237.

[104] Cockcroft *et al.* (n 101) at 230.

[105] Ibid.

[106] My emphasis. Ibid at 241.

[107] J Kenny 'African culture and medical ethics' (2015) *Traditional African Clinic* at 56–57.

[108] N Biggar 'Why religion deserves a place in secular medicine' (2015) 41 *J Med Ethics* at 229–233.

[109] KR Smith 'Religion, secular medicine and utilitarianism: A response to Biggar' (2015) 41 *J Med Ethics.*

endeavour to root it, ground and fashion it according to their cultural norms as well as practical realities.' [110]

The benefit of reflecting indigenous thought is that it can 'deeply enrich our ethical discourse'.[111] Issues faced by medical ethics within an African context are numerous.[112] Despite this, what is troubling is that little synergy is being forged between those advocating African values versus global modernity. This lack of debate, rather than allowing the much-desired evolution of African values, has resulted in the abolishment and outright replacement of African values with imported secular ones. The needed conversation should inspire 'an African concept of modernity and a modern concept of "Africanness"'.[113]

The generalisation that African values are less supportive of privacy and individualism and more concerned with the interests of the collective good, communalism and interdependence is the view held by various writers.[114] The perception persists that privacy is less relevant in African societies than in the west. Such a difference between values is examined by Sihlongonyane. Whereas western values are observed as 'atomic, individualistic, modernised and compatible with capitalist objectivised ideals', African values are established on communalistic and traditional ideals.[115] Western values are associated with 'complexity, heterogeneity, differentiation, secularisation and technological advancement', while traditional African values are equated with 'underdevelopment, the primitive, simple, homogeneous, undifferentiated and supernatural influence'.[116] The western family has 'materialistic, scientific and secular values', while African values are described as being 'communal, socialistic, sacred and magical'.[117] Oosthuizen believes that 'Africa

[110] CT Andoh 'Bioethics and the challenges to its growth in Africa' (2011) 1 (2) *Open Journal of Philosophy* at 67–75.

[111] KG Behrens 'Towards an indigenous African bioethics' (2013) 6 (1) *S Afr J BL* at 33.

[112] Kenny (n 107) at 57, where, for instance, many African traditional societies, such as Nigeria, have no place for abortion, and those guilty would be punished by death.

[113] Ibid.

[114] This discourse is presented in Bygrave, Gutwirth, Olinger *et al*, Bakibinga and Dagbanja.

[115] MF Sihlongonyane 'The Invisible Hand of the Family in the Underdevelopment of Africa Societies: An African Perspective' Scholarly Papers Series: AFRICA - 1.

[116] Ibid.

[117] Ibid.

still cherishes the "humanity" of the African' unlike western cultures. Africa teeters on the perimeter of the modern world, 'with his roots still firmly embedded in all that is essentially human'.[118]

To establish whether an African-style belief in privacy existed in African culture as a 'genuine' concept of value, Bygrave argued that the absence of comprehensive data privacy in Africa was indicative of Africa's lack of a privacy culture.[119] In subsequent work, however, he modified his stance.[120] His revised thinking asserts that privacy in Africa does in fact exist, although essentially as an imported western construct of an individualistic, liberal paradigm. Although the concept is still underdeveloped, Bygrave senses that a change in the value of privacy is now likely in Africa. He suggests that this change is reflected in the emergence of recent data protection laws.[121] Moreover, he cautions that 'care must be taken not to paint countries and cultures into static categories'.[122] Baniser cautions against overstating the differences in cultural understanding of privacy between Africa and the west, as globalisation will inevitably compel privacy protection differences to be resolved and understandings to shift in the same direction as dictated by information technology.[123]

It must be determined whether a person in an African society stands on an equal footing as his or her western counterpart vis-à-vis their privacy entitlements. If such entitlements are the very essence of the belief in human rights and the construction of a shared humanity,[124] and not derived by virtue merely of a person's citizenship of any particular country, or from association with or membership of any nation, but rather as an intrinsic universal entitlement inherent in all human beings,

---

[118] GC Oosthuizen 'Africa's Social and Cultural Heritage in a New Era' (1987) 17 (2) *Africa Insight* 107–120 at 107.

[119] LA Bygrave 'Privacy protection in a global context: A comparative overview' (2004) 47 *Scandinavian Studies in Law* 319–348 at 328.

[120] LA Bygrave 'The place of privacy in data protection law' (2001) 24 (1) *UNSW Law Journal* at 176.

[121] Bygrave (n 119) at 319–348.

[122] Ibid.

[123] Banisar (n 34) at 125.

[124] A Sen 'Human rights and Asian values' (1997) *Carnegie Council on Ethics and International Affairs* at 10.

then no disparity in the position between Africa and the west should exist.[125] Yet, despite these ideals, it seems that privacy is not a universally cherished value.[126] The aspiration of equality begs the question whether non-western societies should be persuaded, even intimidated, into conforming to a set of standards aligned with, and better suited to, the western values of liberty and freedom.[127]

The concept of human rights suggests an entitlement ingrained in all human beings, simply by virtue of them being human beings. However, differing contextual cultural identities and discrepancies of privacy values within regions are noted. This is exacerbated by the fact that privacy by its very nature is a particularly slippery concept to define.[128] Adding to this is the fact that universal human rights as a fundamental entitlement are a relatively recent historical development, with the existence of traditional laws well predating these developments both in Africa and in the East.[129]

This dichotomy of belief structures effectively gives rise to a 'clash of civilizations' or a 'battle between cultures' that divides the western world from Asian countries, the salient points of which also apply to contemporary African society.[130] Sen highlights the differences between the Asian values of order and discipline (and their alternative views on political and civil rights) and their antithesis, the western approach that is based largely on individual rights, autonomy and freedom.[131] Although Sen's arguments are based on the position found in Asia and the ostensible divide between east and west, it is worth considering an extrapolation of this in an African context.[132]

How does one integrate privacy rights in non-western societies and, in so doing, does such coercion not amount to yet another variant of 'cultural

---

[125] Ibid.

[126] Gutwirth (n 100) at 29 and Sihlongonyane (n 121) at 1.

[127] Sen (n 124) at 9–31 and A Sen 'Universal truths' (1998) 20 (3) *Harvard International Review* at 40.

[128] Bygrave (n 120) at 278. On a contrary position, the lack of a precise definition of privacy and data protection is seen in Bygrave as an opportunity for, or 'room for flexibility', in its implementation.

[129] Sen (n 127) at 40.

[130] Ibid.

[131] Sen (n 124) at 10.

[132] Sen (n 127) at 40.

imperialism'?[133] Yankuzo argues that the globalisation of African culture is 'cultural imperialism manifesting through the domination of the indigenous culture both in the material and non-material modes by the foreign cultures'.[134] The acceptance by non-western countries of western-based privacy rights and the adoption thereof, when done merely as a necessary compliance measure to satisfy the west by virtue of its position as an economic stronghold and power, with scant regard to the ideological views of the communities within which such rights are to operate, is troubling. Notions 'alien' to African cultures ought to be sensitively and critically evaluated in a contemporary, African-focused manner before they are integrated into African society, thus avoiding cultural alienation and exploitation by an emerging imperialistic force.

Muzaffar cautions that 'new forms of colonial domination and control are institutionalised and legitimised in the name of globalisation'.[135] As globalisation celebrates the 'rootless and ruthless profiteering that eschews civic connectedness and national sacrifices', the so-called 'outdated' virtues of African family customary values risk being progressively eroded.[136] The western world, in exercising economic control, may steadily enforce its dominating values. Thus, traditional African society has undergone a transformation from communal humane values through the imposition of the ideologies of colonial and neo-colonial forces, and now subsequently to the adoption of Eurocentric values, which dominate the globalisation process and which are promoted by global organisations.[137]

What is gaining momentum is thus a new wave of modern cultural domination that is being mounted by the west. Western values informed the development paradigm and planning models in African societies, and African independence constitutions referred to the rights of privacy and individualism in an attempt to

---

[133] G Hosein 'Privacy and Developing Countries' (2011) Privacy Research Paper, Office of the Privacy Commissioner of Canada.

[134] KI Yankuzo 'Impact of globalization on the Traditional African Cultures' (2014) 4 *International Letters of Social and Humanistic Sciences* at 8.

[135] C Muzaffar 'Human Rights, the State and the Secular Challenge' (1995) 26 (3) *Japan-Asia Quarterly Review* at 47–53.

[136] Sihlongonyane (n 115) at 1.

[137] Ibid.

appease the departing colonialist regimes.[138] By conforming in this way, African society has slowly deprived itself of self-determinism, thus ensuring further cultural deprivation, under-development and marginalisation of African values.[139]

It is not surprising then that the so-called 'propulsion' and 'enforcement' by the west, compelling non-western countries to adopt privacy standards and laws historically foreign to them, may result in an outright rejection of western-based privacy rules.[140] Enforcing and imposing compliance, especially by the previous colonial regimes could result in various 'rebellious' rationales for non-performance of the implementation of privacy rules being assumed by non-Western countries.[141] Granted, transformations of truth and value, complicated by the jagged testimony of colonial dislocation, its transposition of time and person, its damage to culture and domain, exhaust any ambition of creating an all-inclusive and complete theory of colonial oppression consistent throughout Africa.[142] The heterogeneous identification of colonised subjects, based on the traditional sociological alignment of self, society, history and psyche, is rendered questionable by Fanon.[143] Fanon writes that the colonial condition most profoundly evoked is one of 'over-determined from without'.[144]

Arguments against the implementation of western privacy laws are not the preserve of only African countries. These arguments may be extended to other previously colonised countries in the rest of the world too. An example of this is presented in the strongly disputed opinion against the adoption of the 1995 EU Directive in India by Basu, based primarily on cultural differences.[145] In discussing the position found in India, Basu proposes that 'all judgments about adequate

---

[138] IG Shivji *The concept of human rights in Africa* (1989) and IG Shivji 'Constructing a New Rights Regime: Promises, Problems and Prospects' (1999) 8 (2) *Social Legal Studies* 253–276.

[139] Sihlongonyane (n 115) at 1.

[140] Sen (n 124) at 10.

[141] Makulilo (n 4) at 78.

[142] See F Fanon *Black Skins, White Masks* (1967) at *x*.

[143] Ibid at *xiii*.

[144] Ibid. In this regard, Fanon's work examines the sociological and psychological effects of colonialism on its subjects; see F Fanon *Wretched of the Earth* (1961).

[145] S Basu 'Policy-Making, Technology and Privacy in India' (2010) 6 *The Indian Journal of Law and Technology* 65–88 at 85.

protection must remain sensitive to important cultural differences'.[146] Basu further proposes that the notion of privacy is a component of the 'collective good', thereby at least recognising the possibility of adopting a more extensive concept of privacy.[147] The implication of this approach is significant.[148] In embracing human diversity, as Locke puts it, 'men may choose different things, and yet all choose right'.[149] In conclusion by Sen:

> '[t]he recognition of diversity within different cultures is extremely important in the contemporary world, since we are constantly bombarded by oversimple [sic] generalizations about "western civilizations", "Asian values", "African cultures", and so on. These unfounded readings of history and civilization are not only intellectually shallow, they also add to the divisiveness of the world in which we live'.[150]

(2) The approach of the South African courts to traditional African law

Numerous intellectual traditions and philosophies informing African law attest to the importance of freedom and tolerance within African society. This augments the belief in universal human rights. Such rights have been upheld, for instance, in the South African Constitution, which has instigated a transition in the relative value judgments underlying the courts' reasoning and decisions, and has argued in favour of adopting a more inclusive approach to traditional African law in developing constitutional jurisprudence.

For instance, evidence of a sensitive approach to contextualised judicial decision-making is found in South African case law. In *Bernstein v Bester*[151], the minority judgment of Kriegler, J advocated the need for a more nuanced use of comparative law.[152] Such thinking also found favour in *S v Mamabolo*, where the

---

[146] Ibid at 88.

[147] Ibid at 85 and 88.

[148] Ibid.

[149] J Locke *The works of John Locke. To which is added the life of the author and a collection of several of his pieces* publ. by Mr. Desmaizeaux (1812).

[150] Sen (n 124) at 40.

[151] At para 65 and 69.

[152] See DM Davis 'Constitutional borrowing: The influence of legal culture and local history in the reconstitution of comparative influence: The South African experience' (2003) 1 (2) *Oxford University Press and the New York University School of Law* 181 at 191.

Court cautioned against slavishly adopting North American jurisprudence.[153] The reasoning behind this is simply that the two legal systems were found to be inherently incompatible, as they not only originate from different common laws, but also apply to materially different constitutional regimes.[154]

In comparing the US Constitution to the South African Constitution, the Court held: '[o]ur Constitution is a wholly different kind of instrument. … it is infinitely more explicit, more detailed, more balanced, more carefully phrased and counterpoised, representing a multi-disciplinary effort...'. These discrepancies were raised by the court, despite the South African Constitution being modelled on, and influenced by, a myriad of international instruments and decisions,[155] and specific provision contained in Section 35(1) of the Constitution[156] compelling the courts, where applicable, to have regard to, and engage in, comparative enquiries with public international law sources in interpreting and developing South African constitutional jurisprudence.[157]

In creating a uniquely South African constitutional jurisprudence, the Constitutional Court has endeavoured not to use direct comparative law in ascertaining the meaning and scope of the rights contained in the Constitution. As stated by Davis, interpretation of the rights indicates 'a determination to have the use of comparative law mediated by *indigenous history*'.[158]

In light of the historical position with regard to human rights abuses perpetrated in South Africa, and within the context of a newly transformed South African legal regime, it appears that a uniquely African interpretation and an inclusive approach to the content and definition of the rights contained in Chapter 2 of the

---

[153] Para 40.

[154] Ibid 40 and 41.

[155] The Canadian Charter of Rights and Freedom, and German and American jurisprudence amongst others.

[156] Which states: '[i]n interpreting the provisions of this Chapter a court of law shall promote the values which underlie an open and democratic society based on freedom and equality and shall, where applicable, have regard to public international law applicable to the protection of the rights entrenched in this Chapter, and may have regard to comparable foreign case law'.

[157] Davis (n 152) at 192.

[158] Ibid and *S v Zuma*, where the court held that 'regard must be paid to the legal history, traditions and usages of the country concerned' and in *S v Makwanyane*, where the Constitution represents a 'decisive break' from the past.

Constitution is reasonable. Section 39 (2) of the Constitution provides that, when interpreting the Bill of Rights (or any legislation), courts have a specific instruction to develop common and customary law, taking into account the spirit, purport and object of the Bill of Rights. Responding to the challenge of transformation requires the exhausting task of engaging critically with the values promoted by the Constitution.

The adoption of principles of African traditional law, to the extent that they are congruent with the core normative framework contained in the Constitution, will more readily enable Africans to apply their own culture, moral traditions and ethical values when considering ethical dilemmas, thereby reclaiming their dignity and re-affirming their identity.[159]

Likewise, this idea of incorporating traditional legal principles into a transformed form of legal adjudication is not dismissed in *S v Makwanyane*, where Mokgoro J made extensive reference in her judgment to the concept of *ubuntu*[160], while Madala J acknowledged '... the need to bring in the traditional African jurisprudence to these matters, to the extent that such is applicable, and would not confine such research to South Africa only, *but to Africa in general*'.[161] Additionally, Sachs J at paragraph 373 held : '[i]n my view, s 35(1) requires this court not only to have regard to public international law and foreign case law, but also to all the dimensions of the evolution of South African law, which may help us in our task of promoting freedom and equality. This would require reference not only to what in legal discourse is referred to as "our common law" but also to traditional African jurisprudence'.

Moreover, in paragraph 39 of his judgment, Chaskalson JP stated: '[i]n dealing with comparative law, we must bear in mind that we are required to construe the South African Constitution, and not an international instrument or the Constitution

---

[159] Behrens (n 111) at 33.

[160] At para 306, 'in interpreting the Bill of Fundamental Rights and Freedoms, as already mentioned, an all-inclusive value system, or common values in South Africa, can form a basis upon which to develop a South African human rights jurisprudence. Although South Africans have a history of deep divisions characterised by strife and conflict, one shared value and ideal that runs like a golden thread across cultural lines, is the value of *ubuntu* – a notion now coming to be generally articulated in this country' and at para 312 '(o)ur new Constitution, unlike its dictatorial predecessor, is value-based. Among other things, it guarantees the protection of basic human rights, including the right to life and human dignity, two basic values supported by the spirit of *ubuntu* and protected in Sections 9 and 10 respectively'.

[161] At para 258.

of some foreign country, and that this has to be done *with due regard to our legal system, our history and circumstances, and the structure and language of our own Constitution'*.

In the words of the Constitutional Court in *Mayelane v Ngwenyama and another*[162], '[t]here is an untapped richness in customary law, which may show that the values of the Constitution are recognised, or capable of being recognised, in a manner different to a common-law understanding'.[163] However, the Court in *Bhe and others v Khayelitsha Magistrates and others* rejected evidence, as the Court held that certain practices did not represent widespread developments in living customary law. Of significance though is the observation inherent in the Court's findings.[164] The Court describes customary law as a 'parallel system' and stated '[q]uite clearly *the Constitution itself envisages a place for customary law in our legal system'*.[165]

Moreover, paragraph 41 states that '[c]ertain provisions of the Constitution put it beyond doubt that our basic law specifically requires that customary law should be accommodated, *not merely tolerated*, as part of South African law, provided the particular rules or provisions are not in conflict with the Constitution'.[166] The Court held that, '[i]t is for this reason that an approach that condemns rules or provisions of customary law merely on the basis that they are different to those of the common law or legislation, … would be incorrect'.[167]

The decision in *Bhe* raised an important issue of how universal human rights are to be translated and applied in a culturally diverse society.[168] Pertaining to the nature and underlying values of living customary law, the Court tended to adopt at pragmatic approach, as its norms in practice adapt to 'circumstantial changes, human frailty and the vagaries of people's behaviour'.

In *Pillay*, Justice Langa quotes the words of Martin Chanock:

---

[162] Para 50.

[163] Ibid.

[164] Paras 40 and 41.

[165] Ibid.

[166] Ibid at para 41.

[167] Ibid at para 42.

[168] E Grant 'Human rights, cultural diversity and customary law in South Africa' (2006) 50 *Journal of African* at 4.

> '[t]he idea of culture derived from anthropology, a discipline which studied the encapsulated exotic, is no longer appropriate. There are no longer (if there ever were) single cultures in any country, polity or legal system, but many. Cultures are complex conversations within any social formation. These conversations have many voices.'[169]

Determinations and decisions are thus influenced by and made within a veritable value laden historical, traditional and cultural context. This resonates particularly in a society with the diverse range of peoples and cultures, as is evident in South Africa.

(3) Ubuntu: An African worldview that influences social conduct

It is worth noting that, in both western and African traditions, societies and values have much diversity and variation within themselves. They are constantly in a state of growth and continued transition. It would be overly simplistic to claim that a single African worldview exists or to attempt to articulate what that is. As already stated at the beginning of this chapter, Africa is diverse and complex. A crude notion of what is 'African' is meaningless and unhelpful. It must be recognised that within various cultures there is both a contradictory dichotomy and a harmony of values that are constantly evolving in the contemporary world. Being bombarded by generalisations of what is considered 'western civilisation', 'African values' or 'Asian values' is essentially unconstructive.[170]

That being said, certain noticeable and distinctively African beliefs and ideologies are nonetheless prevalent and practiced by a predominant number of sub-Saharan Africans. One such prevailing African perspective is the significance of and reliance placed on the community.[171] This is confirmed by Biko: '[t]he oneness of community ... is at the heart of our culture.'[172]

---

[169] *MEC for Education: KwaZulu-Natal and Others v Pillay* at para 54. The reference is to M Chanock 'Human Rights and Cultural Branding: Who Speaks and How?' in A An-Naim *Cultural Transformation and Human Rights in Africa* (2002) at 41.

[170] Sen (n 124) at 9–31.

[171] Behrens (n 111) at 33.

[172] S Biko I Write What I Like (2004).

The view that traditional values play a role in the creation of South African law is echoed in Mokgoro, where she calls it a 'patriotic obligation' that is placed on all South Africans to not allow the Constitution and the principles of respect for human rights and dignity 'to slide into disrepute'.[173] She explains that the very concept of *ubuntu* underlies and, in fact, demands the respect for human rights upon which the Constitution has been so carefully constructed. Moreover, her observation is that it is against the background of the call for an 'African renaissance', that the inspiration for, and development of, the traditional African concept of *ubuntu,* and the social values it represents, should motivate the expansion of a 'new South African law and jurisprudence'. This assertion too is made by the court in *Port Elizabeth Municipality v Various Occupiers*[174], viz. that *ubuntu* is the 'underlying motif of the Bill of Rights'.

Although caution is expressed against a superficial interpretation of the concept,[175] *ubuntu* can be described as 'a philosophy of life, which in its most fundamental sense represents personhood, humanity, humaneness and morality; a metaphor that describes group solidarity where such group solidarity is central to the survival of communities with a scarcity of resources, where the fundamental belief is that *motho ke motho ba batho babangwe/umuntu ngumuntu ngabantu* (which translated means: a person can only be a person through others).'[176] *Ubuntu* 'can be grasped only on a "I know it when I see it" basis, its essence not admitting of any precise definition.'[177]

Archbishop Desmond Tutu expressed it as follows: '[a] person is a person because he recognises others as persons'.[178] The maxim is inclusive and may be

---

[173] Y Mokgoro '*Ubuntu* and the law in South Africa' (1998) 1 (1) *Potchefstroom Electronic Law Journal* at 1, and again at 6, where '[t]he values of *ubuntu* are therefore an integral part of that value system which had been established by the Interim Constitution'. Moreover, section 211 provides: '[t]he courts must apply customary law when that law is applicable, subject to the Constitution and any legislation that specifically deals with customary law'.

[174] (CCT 53/03) [2004] ZACC 7; 2005 (1) SA 217 (CC); 2004 (12) BCLR 1268 (CC).

[175] See M Kunene 'The Essence of being Human: An African Perspective' Inaugural lecture 16 August 1996 Durban at 10.

[176] Mokgoro (n 173) at 2.

[177] Ibid. See *Port Elizabeth Municipality v Various Occupiers* at para 308.

[178] The Desmond Tutu Peace Foundation. Available at http://www.tutufoundation-usa.org/exhibitions.html (accessed 28 January 2017).

interpreted in the following ways: '[o]ne becomes a moral person insofar as one honours communal relationships', and '[a] human being lives a genuinely human way of life to the extent that she prizes identity and solidarity with other human beings', and '[a]n individual realises her true self by respecting the value of friendship'.[179] Desmond Tutu explains:

> '[w]hen we want to give high praise to someone, we say *Yu u nobuntu*; Hey, so-and-so has *ubuntu*.' The claim that one can obtain *ubuntu* "through other persons" means, to be more explicit, by way of communal relationships with others.'[180]

Ubuntu is not merely a social ideology but is 'the very quality that guarantees not only a separation between men, women and the beast, but the very fluctuating gradations that determined the relative quality of that essence'. He calls it the 'potential of being human'.[181] The implication is that 'one is constantly challenged by others, practically, to achieve self-fulfilment through a set of collective social ideals', and the term is used in a more philosophical sense to describe 'the belief in a universal bond of sharing that connects all humanity'.[182]

Despite no reference being made specifically to privacy, Mokgoro states that '[g]roup solidarity, conformity, compassion, respect, *human dignity*, humanistic orientation and collective unity have, *among others*, been defined as key social values of *ubuntu*'. She asserts that, by virtue of its expansive nature, the concept of *ubuntu* and its social value will depend on the approach and purpose for which it is intended. Thus its value is a 'basis for a morality of co-operation, compassion, communalism and concern for the interests of the collective respect for the *dignity of personhood*, all the time emphasising the virtues of that dignity in social relationships and practices'.[183]

Metz submits that 'it is up to those living in contemporary Southern Africa to refashion the interpretation of *ubuntu* so that its characteristic elements are construed

---

[179] T Metz 'Ubuntu as a Moral Theory and Human Rights in South Africa' (2011) 11 *African Human Rights Law Journal* at 540.

[180] D Tutu *No future without forgiveness* (1999) at 31.

[181] Kunene (n 175) at 10.

[182] Ubuntu Human Rights International. Available at http://www.ubuntuhri.com (accessed 20 February 2017).

[183] Mokgoro (n 173) at 3.

in light of our best current understandings of what is morally right'. [184] This was reiterated by former South African President Thabo Mbeki:

> '[a]s we know, the African people in this country have, over many centuries evolved a value-system of *ubuntu*. Many of us have been brought up to uphold values based on this age-old African adage. Through socialisation many Africans have ensured that our families and communities are themselves grounded on the value-system of *ubuntu*'.[185]

Collective responsibility and confidentiality accord with the philosophy of *ubuntu* providing a cohesive social basis in African culture.[186] Dignity, by embracing the *ubuntu* quality of humanness, is guarded as a comprehensive right of personality in indigenous legal systems. Hence, there is a need to harness these qualities with care, ingenuity and creativity, so that the intricate traditional African social, historical and cultural facets are supported and represented by contemporary legal notions, and a legitimate, participative system of law can be advanced for all South Africans.[187]

Notwithstanding the intrinsic value of *ubuntu*, hurdles and objections to its implementation do exist. Difficulties include its vagueness, its failure to acknowledge the value of individual freedom, and the fact that its application is more appropriate for traditional, small-scale culture and pastoral societies and less suited to modern, industrial societies with a plurality of cultures.[188] These shortcomings should not, however, preclude *ubuntu* from grounding public morality nor of being used as a method of resolving contemporary moral dilemmas in South Africa.[189]

---

[184] Metz (n 179) at 532 and 536.

[185] Address of Thabo Mbeki at the Heritage Day Celebrations, North West Province (2005).

[186] A Le Roux-Kemp 'HIV/AIDS, to disclose or not to disclose: That is the question' (2013) 16 (1) *PER: Potchefstroomse Elektroniese Regsblad.*

[187] Mokgoro (n 173) at 4 and WW Rankin '*Ubuntu*: An African term meaning humaneness, inclusive community where all are respected' (2000) 15 (1) *Journal of Pediatric Nursing* at 50. See also HN Olinger, JJ Britz and MS Olivier 'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007).

[188] Metz (n 179) at 534.

[189] Ibid.

(4) The myth of harmonisation of privacy into African data privacy policies

Based on a review of the literature, the sentiment shared by many authors seems to suggest that privacy as a value is more clearly and broadly observable and enforceable in the western world.[190] Makulilo states: '[p]rivacy is a value that has its roots in the Western world'. He reiterates: '[i]n contrast privacy is a value that is less developed in the non-Western world'.[191] He then questions whether 'other cultures in the non-Western sphere can support claims for privacy'.[192] He concedes, however, that the argument that the significance of privacy is less established in the non-western world, where the culture of collectivism outweighs claims for privacy, is 'rarely supported by empirical evidence'.[193] Nonetheless, the widely held position is that African moral ideas revolve around communal relationships and that themes of communal connections are interpreted and conceived as objectively desirable interactions and are less concerned with autonomy or individuality.[194]

Unfortunately, the failure on the part of the African Charter of Human and People's Rights 1981 to include the right to privacy protection in the Charter does not help to endorse its value and it consequently may be construed as testimony to Africa's unwillingness to embrace an expansive, strengthened right of privacy on the continent.[195]

Nevertheless, of late there has been full endorsement and promotion of the existence and development of privacy laws in Africa. The fallacy that Africa is a static and unchanging society is being challenged. Privacy as an evolving concept within Africa is beginning to be embraced. To advocate a 'one size fits all' approach

---

[190] Gutwirth (n 100) at 24. See also HN Olinger, JJ Britz and MS Olivier 'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007) *International Information and Library Review* 31–43; J Burchell 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* at 2 and DN Dagbanja 'Privacy in Context: The right to privacy, and freedom and independence of the media under the constitution of Ghana' (2014) 22 (1) *African Journal of International and Comparative Law* at 40–62.

[191] Makulilo (n 4) at 81, Bygrave (n 10) at 165–200 and Gutwirth (n 100) at 24.

[192]Ibid at 81 and JA Cannataci 'Privacy, Technology Law and Religions across cultures' (2009) 1 *Journal of Information, Law and Technology* 1–22 at 1.

[193] Olinger *et al.* (n 187) at 37.

[194] Sihlongonyane (n 115).

[195] Gutwirth (n 100) at 24; Bygrave (n 10) at 180 and Olinger *et al.* (n 187) at 37.

towards general privacy protection throughout Africa, however, is dangerous. The reasoning behind this is that adoption of such an approach may negate, and potentially even damage, the nuanced cultural traditions and subtle sensitivities evident in the diverse societies and communities within Africa. Rather, a delicate, thoughtful and skilful response to context sensitive data protection is recommended.

VII CONCLUSION

Harmonisation of national data protection laws in Africa is an increasing phenomenon.[196] A nation's eHealth readiness extends beyond the technological imperative, and it should be predicated upon the inclusion of a sound legal and regulatory framework around privacy. Unfortunately, the reality is that, with the proliferation of data protection laws being imposed within Africa and little consensus apparent between nations, resulting in differing cross-border rules and procedures to abide by, a fragmented and somewhat cumbersome outcome seems inevitable.[197] Moreover, many African data protection regimes are still in their formative stages, and regulations have either not yet been put into practice, or are progressing at a slow pace, resulting in dubious and inexact enforcement efforts. Additionally, data protection and privacy literature across large sectors of Africa remains incomplete, with privacy issues currently either under-researched or not researched at all.[198]

Significantly, a most compelling and powerful incentive of the development of minimum standards of privacy law among developing nations is the desire to engage in, and be included in, and thereby benefiting from global e-commerce, e-transactions, and the exchange and transfer of data freely across jurisdictions.[199] Undoubtedly, this has been a principal motivation for the adoption of, and adherence to, data privacy legislation in Africa.[200]

---

[196] Ibid.

[197] Gwagwa also speaks of 'fragmentation' in Africa's attempts to control cyberspace. See Gwagwa (n 6).

[198] Makulilo (n 4) at 163.

[199] Ibid at 81.

[200] Ibid.

However, all is not lost. With the momentum of data protection and the sheer inertia provided by the more than 100 countries with legislation in place, there is little opportunity to turn back, with clear evidence of an upward trajectory. The following chapter shall consider privacy and data protection in South Africa.

CHAPTER 5: PRIVACY AND DATA PROTECTION MEASURES WITHIN SOUTH AFRICA

The question isn't 'What do we want to know about people?' It's 'What do people want to tell about themselves?'

Mark Zuckerberg

I INTRODUCTION

For illustrative purposes, the position of privacy and data protection within South Africa is considered in this chapter. South Africa is a useful example of how data protection regulation may be implemented on a domestic level. This chapter furthermore provides a case study mirroring the issues found within the African region as a whole. The position in South Africa is merely used to illustrate the domestic implementation of data protection regulation within a health care environment and is not an attempt to provide a complete solution.

In this regard, I consider various provisions of the South African Constitution, the common law position, relevant case law, and the legislation and medical regulatory guidelines relating to privacy and data protection measures, which have an influence on data-related issues emanating from the practice of eHealth in South Africa. Given the absence of an eHealth specific privacy or data protection statute within South Africa, I have had to take recourse to generic privacy and data protection provisions currently prevailing in South African law, together with more recently enacted data protection legislation, in an endeavour to extract their relevance to and implications for the field of information communications technology and eHealth in South Africa.

II THE SOUTH AFRICAN POSITION

Privacy may be protected by virtue of the common, or civil, law (usually the law of delict), by the protected right to privacy enshrined in the Bill of Rights or the Constitution, or by provision in general or specific privacy and/or data protection legislation.[1] These means of protection often run concurrently within a legal system, and rather than existing independently, their convergence and mutual interaction serve to strengthen any consequential privacy protection.[2]

[1] See J Burchell 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* at 2.

[2] Ibid at 2, 3 and 4.

(1) South African common law protection of privacy

Neethling *et al.* describe the South African private law approach to privacy as 'an individual condition of life characterised by exclusion from publicity. This condition includes all those personal facts, which the person himself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he evidences a will for privacy'. They suggest that '[p]rivacy can be infringed only by an acquaintance with personal facts by outsiders and contrary to the determination and will of the person whose right is infringed, and such acquaintance can take place in two ways only, namely through intrusion (or acquaintance with private facts) and disclosure (or revelation of private facts)'.[3] Neethling *et al.* describes an individual's right to privacy as including the control that individuals have over their personal information and the freedom to conduct their personal affairs without unwanted intrusions.[4]

By definition, privacy is viewed in Neethling *et al.* as a personality right, this being a distinct category of rights distinguishable from three other classes of rights, namely real rights, personal rights and immaterial property rights.[5] Personality rights are worthy of protection in terms of private law by virtue of them falling within the individual's 'inner sanctum'.[6] The ambit of constitutional privacy protection, as contained within the Bill of Rights may suggest that the concept of privacy, quite correctly, is extended beyond merely that of the 'inner sanctum'.[7]

Contrary to the position in many other common law countries,[8] the protection of the right to privacy is an integral part of the South African law of delict.[9] Despite

---

[3] See J Neethling, JM Potgieter & PJ Visser *Neethling's Law of Personality* (2005) at 31 fn 334 and also J Neethling 'The Concept of Privacy in South African Law' (2005) 122 (1) *The South African Law Journal* at 18 and *National Media Ltd ao v Jooste 1996 (3) SA 262 (A) 271–2*.

[4] Ibid where it was held '[a]bsent a will to keep a fact private, absent an interest (or a right) that can be protected. The boundary of a right or its infringement remains an objective question. As a general proposition, the general sense of justice does not require the protection of a fact that the interested party has no wish to keep private'.

[5] Ibid.

[6] Ibid.

[7] See IM Rautenbach 'The conduct and interests protected by the right to privacy in section 14 of the Constitution' (2001) *Journal of South African Law* at 115.

[8] While English common law has, for centuries, placed value on the related interests of dignity and privacy, ironically, it has been reluctant to protect or recognise the right to privacy as a separate cause

various legal remedies at one's disposal in instances of privacy violations, ultimately, the source of legal protection of privacy lies in the law of delict, that is, a modern application of the Roman *actio iniuriarum*.[10] This is particularly relevant in countries, like South Africa, where an immediate remedy is found in the Roman Dutch common law of delict.[11] This provides protection of dignity, under the *actio iniuriarum,* which not only protects individuals' dignity and reputation, but also their physical integrity.[12]

Thus, the protection of an individual's private information already forms part of the law of delict in South African law. It is, according to Chaskalson P, the obligation of the courts within South Africa 'to develop a constitutional jurisprudence' constructed on principle and then to adjudicate cases based on such established principles.[13] Moreover, 'where principles have not yet been established', Chaskalson P held that 'courts may draw on the burgeoning international jurisprudence on constitutional rights'.[14]

Despite the reliance on common law as a remedy, cognisance should be taken of the judgment in *Pharmaceutical Manufacturers Association.* The court held that it 'cannot accept this contention, which treats the common law as a body of law separate and distinct from the Constitution'[15], and that '[t]here is, however, only one system of law and within that system the Constitution is the supreme law with which all other law must comply.'[16] Moreover, the court in the case of *Fose v Minister of Safety and*

---

of action in tort. See C Okpaluba 'Constitutional protection of the right to privacy: Evaluating the contributions of Chief Justice Langa to the law of search and seizure' *Acta Juridica* (2015) at 407.

[9] D McQuoid-Mason 'Privacy' in Woolman *et al.* (eds) *Constitutional Law of South Africa* (2 ed) vol 3 at 38.

[10] Burchell (n 1) at 2 and 6. See A Roos 'Core principles of data protection law' (2006) 39 *CILSA* at 102; A Roos 'Personal data protection in New Zealand: Lessons for South Africa?' (2008) 4 *Potchefstroom Electronic Law Journal* at 65 and J Neethling 'Features of the Protection of Personal Information Bill, 2009 and the law of Delict' (2012) 75 *THRHR* at 245.

[11] Ibid at 3.

[12] Ibid at 3 and 5.

[13] *Mistry v Interim Medical and Dental Council of South Africa* at para 3.

[14] Ibid.

[15] *Pharmaceutical Manufacturers Association of South Africa ao: In re Ex parte President of the Republic of South Africa and Others (CCT31/99) [2000] ZACC 1; 2000 (2) SA 674; 2000 (3) BCLR 241 (25 February 2000)* at para 44.

[16] Ibid.

Security held that the remedy granted under the *actio iniuriarum* was appropriate in this instance 'for the preservation of personality rights'.[17]

Instances, where an action for invasion of privacy at common law has been recognised as worthy of protection by the South African courts and protected under the general principles of the *actio injuriarum*[18], are well documented.[19] The recognition of the separate personality right of privacy is manifested in the following two instances:[20] Firstly, it is relevant in instances of acquaintance or intrusion, that is, when a person becomes acquainted with another person or his personal affairs, which the person elects to be kept private.[21] These may include entry into private residence;[22] obtaining facts about one's health;[23] secretly watching a person;[24] reading private documents;[25] listening in on private conversations;[26] following a person;[27] taking an unauthorised blood test;[28] disclosing the HIV-positive status of a patient by a medical practitioner[29] and the improper interrogation of a person by the police.[30]

---

[17] At para 40.

[18] *O'Keeffe v Argus Printing and Publishing Co Ltd and Another* at 248; D McQuoid-Mason *The Law of Privacy in South Africa* (1978) at 86; D McQuoid-Mason 'Invasion of Privacy: Common Law v Constitutional Delict – Does it make a Difference?' (2000) *Acta Juridica* at 227.

[19] See Roos (n 10) at 30. In the recognition of a right to privacy in South African law, the court in the 1954 case of *O'Keeffe* (n 18) held that the *actio iniuriarum* could be used as protection against the unauthorised publication of a person's name and likeness in an advertisement. Also *the cases of Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk; National Media Ltd v Jooste; Financial Mail (Pty) Ltd vs Sage Holdings Ltd* and *Janit v Motor Industry Fund Administrators (Pty) Ltd.* Also *S v A and Jansen van Vuuren v Kruger.*

[20] J Neethling, JM Potgieter & PJ Visser *Law of Delict* (2010) at 347.

[21] Neething (n 3) at 222–226 and Neethling (n 10) at 243.

[22] *Pretoria Portland Cement Co Ltd v Competition Commission* at 71, where the court held with regard to the validity of a search and seizure operation conducted in terms of a warrant, 'I must emphasize that the facts which I have set out, even the undisputed facts, involve a gross violation to the appellants' rights to privacy under the Constitution.'

[23] *Tshabalala-Msimang v Makhanya*; *Jansen van Vuuren v Kruger* and *NM v Smith (Freedom of Expression Institute as amicus curiae)*.

[24] *MEC for Health, Mpumalanga v M-Net* at 718–719 and 721.

[25] *Reid-Daly v Hickman*.

[26] S v A.

[27] *Huey Extreme Club v MacDonald t/a Sport Helicopters* at 498–499.

[28] *C v Minister of Correctional Services); S v Orrie* at 589–590 and 591.

[29] *Hoffmann v South African Airways* and *Jansen van Vuuren v Kruger* at paras 11 to 14, and 38.

[30] *Gosschalk v Rossouw* at 492.

Secondly, instances of disclosure or intrusion, that is, where a person acquaints third parties with another person, or his personal affairs, which, although known, remain private.[31] These instances include the disclosure of personal facts acquired by a wrongful act of intrusion;[32] the disclosure of personal facts contrary to the existence of a confidential relationship[33] and the publication of private facts by the media.[34]

Data processing thus has the potential to infringe on an individual's personality in two ways: in instances where correct and accurate personal information is processed, a person's privacy may be infringed, and, secondly, where false or misleading information is processed, the individual's identity may be infringed.[35] Both instances may be protected in the law of delict by the *actio iniuriarum*.[36] Any patrimonial loss emanating from the wrongful, negligent infringement of the personality may also be claimed with the institution of the *actio legis Aquiliae*.[37] Moreover, an interdict is available at common law to avert an impending interference with one's right to privacy or identity, or to prevent the continuation of a wrongful infringement.[38]

As each person determines the destiny of their private information and consequently the scope of their interest in privacy, the aim of data protection is

---

[31] Neethling *et al.* (n 3) at 226–236.

[32] *Financial Mail (Pty) Ltd v Sage Holdings Ltd* at 463; *Motor Industry Fund Administrations (Pty) Ltd v Janit* at 303 and *MEC for Health, Mpumalanga v M-Net*.

[33] *Swanepoel v Minister en Sekuriteit.*

[34] *NM v Smith* and *MEC for Health, Mpumalanga v M-Net.*

[35] Roos (n 10) at 89.

[36] The *actio iniuriarum* protects a person's corpus, fama and dignitas, whereas the term 'dignitas' is a collective term embracing a number of personality rights, including dignity, privacy and identity, at Neethling *et al.* (n 3) at 229, and C Gowar and CJ Visser 'Distinguishing between Dignity, Identity and Privacy: Is it Really Necessary? *Kumalo V Cycle Lab (Pty) Ltd* (31871/2008) [2011] ZAGPJHC 56' (2012) 75 *Journal of Contemporary Roman-Dutch Law* at 154.

[37] See J Neethling and J Potgieter 'Defamation of a Corporation: Aquilian Action for Patrimonial (Special) Damages and *Actio Iniuriarum* for Non-Patrimonial (General) Damages: *Media 24 Ltd v. SA Taxi Securitisation and Amici Curiae* 2011 5 SA 329 (SCA)' (2012) 75 *Journal of Contemporary Roman-Dutch Law* at 304–312 where at 312 the author's state in their concluding remarks that: '[t]here seems to be general agreement that the *amende honorable* or similar remedies are available or can at least be developed in our law to substitute the *actio iniuriarum*' and also Gowar and Visser '(n 36) at 154–162, for a discussion on the correct *actio* to be used.

[38] Roos (n 10) at 90.

essentially to enable persons to exercise effective control over the processing of their personal information, for instance, personal data processed by a bank, an insurance company, employer or health care professionals. [39]

Identity, in contrast, is described by Neethling as that uniqueness, which identifies a person as a particular individual (or corporation), and consequently distinguishes them from others. [40] Identity may be revealed by a person's life history, name, voice, handwriting or physical image and is the characteristics by which an individual may be recognised. Infringement of identity is typically through misrepresentation, where a characteristic or representation of a person does not accurately reflect the person's true image. Neethling postulates the distinction: 'truthfulness is an element of infringement of privacy', while 'falsity is an element of infringement of identity'. Therefore, privacy is 'threatened by the processing of true personal information', whereas identity is 'endangered by the processing of false or misleading data'.[41]

It must also be considered whether specific legislative data protection measures are necessary and should be enacted to counter any threats to the rights to privacy and identity, or whether it is sufficient protection for the courts to utilise, develop and adapt traditional principles of common law directed at the protection of personality rights with regard to the protection of private data.[42]

Despite remedies being available in delict, Roos is of the opinion that data protection must be strengthened and extended: '[s]ince the common law in South Africa does not provide adequate protection for personal data, specific data protection legislation is also required'. [43] This position was reiterated by Neethling in his doctrinal work on the right to privacy, in which he concludes that the introduction of data protection legislation in South Africa was 'urgently necessary'.[44] Yet again in Van der Merwe *et al.*, this view is repeated where it is written that, given that, at that

---

[39] Neethling (n 10) at 244.

[40] Ibid.

[41] Ibid.

[42] This was addressed by the Law Reform Commission in assessing whether legislative adoption was necessary to protect personal data in South Africa. See Ibid and SALRC Report 14–42.

[43] Roos (n 10) at 102.

[44] In Neethling (n 10) at 241. See J Neethling *Die reg op privaatheid* (LLD thesis UNISA 1976) at 406.

time of the authors' writing, no general data protection existed in South Africa, they recommend that '[a]n omnibus data protection Act is required'.[45]

The grounds in favour of separate remedial data protection legislative measures are numerous and compelling.[46] Perhaps in light of the doctrine of the separation of powers, it is regarded by Neethling as 'improbable' that the application of traditional principles in case law by the courts will occur 'often or extensively enough' in the immediate future to warrant the reliance on the courts to develop sufficient, extensive jurisprudence to protect personal data adequately and immediately.[47] This is, in reality, a slow jurisprudential process, despite the court's willing compliance with their obligation to develop the common law in accordance with the values and principles underpinning the South African Constitution.

Moreover, effective data protection requires that persons themselves should be able to exercise a measure of control over their personal data. This unique requirement of exercising specific control, by giving or withholding consent in a predetermined manner, not only differentiates it from, but places it beyond the ambit of traditional common law privacy protection principles. Accordingly, such requirements and measures can be more easily and concisely accommodated for through specifically tailored data protection and privacy legislation.

Lastly, to comply with the stringent data protection requirements stipulated by the latest data protection regulation coming out of the Europe Union, which, for instance, controls the free cross-border flow of personal information, appropriate and compliant data protection legislation is essential. Unfortunately, the law of delict does not provide such comprehensive and rapidly enforceable protection.

While common law and the law of delict provide opportunities that may be helpful in addressing matters of privacy violations, they may not provide satisfactory recourse in confronting all the issues. Supplementary legislative measures may indeed be useful.

---

[45] D van der Merwe, A Roos, T Pistorius & S Eiselen 'Chapter 9 - Data protection' in *Information and Communications Technology Law* (2008) at 367.

[46] See S Snail and S Papadopoulos 'Chapter 13 - Privacy and data protection' in S Papadopoulos & S Snail (eds) *Cyberlaw@SA* III ed (2012) at 295 where it is stated that '… it is clear that data protection legislation is necessary.'.

[47] Neethling (n 10) at 245.

(2) South African constitutional right to privacy and human dignity

Uncertainty about the exact nature, content and scope of privacy as a concept and how it relates to, and concurs with, other rights, was also confirmed in *Bernstein v Bester*[48], where Ackermann J described the concept of privacy as 'an amorphous and elusive one, which has been the subject of much scholarly debate'. Despite its elusive quality, Banisar noted that privacy is 'one of the most important human rights issues of the modern age'.[49]

The right to privacy is indispensable in achieving the constitutional commitment of safeguarding human dignity.[50] Both of these rights, the right to privacy and the right to have one's dignity respected and protected, are provided for in Sections 14 and 10 of the Constitution. By including privacy and dignity protection in the Constitution, the very essence and inherent objective embodying human rights protection is achieved, that of shielding those most vulnerable in society.[51] Section 14 of the Constitution provides:

> '[e]veryone has the right to privacy, which includes the right not to have (a) one's person or home searched, (b) one's property searched, (c) one's possessions seized, or (d) the privacy of one's communications infringed'.

Section 14 thus has two parts: the first guarantees the general right to privacy, or substantive privacy rights, and the second, informational privacy rights, are contained in paragraphs (a) through (d), and provide protection against specific violations, namely, searches and seizures and infringements of the privacy of communications. Although certain infringements are specifically named in Section 14 (a) to (d), the list of privacy violations is not exhaustive. Section 10 of the Constitution provides:

---

[48] *Bernstein v Bester (CCT23/95) [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (27 March 1996)* at para 65 and 67.

[49] D Banisar and SG Davies 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (2012) 18 (1) *John Marshall Journal of Computer & Information Law* at 3.

[50] Ibid.

[51] Ibid.

'[e]veryone has inherent dignity and the right to have their dignity respected and protected'.

Although not recognised *eo nomine* in the Constitution as specified rights, identity and reputation may well be considered part of the right to human dignity. This was confirmed by O'Regan J who articulated in the *Khumalo* case that '[n]o sharp lines then can be drawn between reputation, *dignitas* and privacy in giving effect to the value of human dignity in our Constitution'.[52]

(3) South African case law

The Constitution provides a solid motivation for the South African courts to develop the law of delict and vindicate human rights. From modest beginnings, the South African courts have begun to shape the concept of privacy.[53] In *Mistry v Interim Medical and Dental Council of South Africa*[54], the Constitutional Court provided a general framework regulating data privacy protection.[55] Although the facts of the case did not turn on the issue of informational privacy and therefore were not dealt with extensively by the court, the court contended that the 'texture and perimeters' of informational privacy are 'complex and controversial'. The case touched on the difficulties inherent in breach of informational privacy actions, which, unlike invasion of private communications, is not addressed expressly in Section 13 of the Interim Constitution (subsequently replaced by Section 14 of the Constitution).[56] In the judgment of Sachs J, the court, quoting the privacy provisions in the Act, afforded protection based on the broad provisions of the right to privacy in the section.[57]

---

[52] *Khumalo and Others v Holomisa* at para 27.

[53] The courts have to date delivered judgments on the right to privacy with regard to the possession of indecent or obscene photographs, the scope of privacy in society and searches and seizures. See the following cases in this regard: *Case and Another v Minister of Safety and Security* 1996 (3) SA 617 (CC); *Curtis and Another v Minister of Safety and Security* 1996 (3) SA 617 (CC); *Bernstein v Bester; National Media Ltd and Another v Jooste* and *Mistry v Interim Medical and Dental Council of South Africa*.

[54] *Mistry v Interim Medical and Dental Council of South Africa*.

[55] Burchell (n 1) at 7.

[56] Ibid at 14.

[57] At paras 47 and 48.

The determination in *Mistry* turned on whether the information was obtained in an intrusive manner; whether the nature of the information concerned intimate aspects of the individual's personal life; whether the specified purpose of the information was not adhered to and the information was used for an ulterior purpose; and, lastly, whether the information was disseminated to the press or general public from whom the subject 'could reasonably expect such information would be withheld'.[58]

The 1996 Appellate Division of the Supreme Court of South Africa in *National Media Ltd and Another v Jooste* recognised that privacy is a condition that 'embraces all those personal facts, which the person concerned has determined himself to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private'.[59]

Interestingly, Harms JA quoted the words of Warren and Brandeis in the introduction to his judgment.[60] Exactly where the boundary between the right to privacy and the infringement thereof should be drawn remains a question to be determined. The court held that 'a person is entitled to decide when and under what circumstances private facts may be made public' and such disclosure or consent to such disclosure may 'be limited conditionally or unconditionally and irrespective of motive'.

In *Tshabalala-Msimang v Makhanya* an application was brought before the South African High Court, calling upon it to consider the inherent conflict between the competing constitutional rights of privacy and that of freedom of expression entrenched in Section 16, also positioned as the public's right to know.[61] The application was based on the provisions contained within the Constitution and the National Health Act pertaining particularly to one's right to privacy and to the confidentiality of, access to, and protection of medical records. The court confirmed that, in terms of 'the National Health Act, the medical records of a person are private

---

[58] *Mistry v Interim Medical and Dental Council of South Africa* at para 47. See additionally, D McQuoid-Mason (n 18) at 227.

[59] At para 13 quoting Neethling's definition of 'privacy' in his doctoral thesis, *Die Reg op Privaatheid* (UNISA 1976) at 287.

[60] Ibid.

[61] *Tshabalala-Msimang v Makhanya*.

and confidential'.[62] The court followed: 'where a person acquires knowledge of private facts through a wrongful act of intrusion, any disclosure of such facts by such person or by any person, in principle, constitutes an infringement of the right to privacy'.[63] The court reiterated the importance of keeping the information concerning a user, including information relating to his/her health status, treatment or stay in a health establishment, as confidential.[64] The reason for this is clear. Confidential medical information invariably contains 'sensitive and personal information about the user', concerning the 'individual's health, reflects sensitive decisions and the choices that relate to issues pertaining to bodily and psychological integrity as well as personal autonomy'.[65] The court emphasised the 'potential harmful effects' that may result from such disclosure.[66]

In *Jansen van Vuuren v Kruger* the court reiterated the importance of a medical practitioner's duty of maintaining confidentiality regarding information acquired in a medical practitioner's professional capacity. The plaintiff argued that the disclosure by the medical practitioner of his HIV status – despite an explicit request by the patient to keep the information confidential – to other health practitioners was an invasion of his privacy and an injury to his rights of personality. The court confirmed that the Hippocratic Oath, which requires a medical practitioner 'to keep silence' about information acquired in his professional capacity relating to a patient, 'counting such things to be as sacred secrets', is still applicable. The court held that the duty of a medical practitioner to respect the confidence of his or her patients is not merely an ethical duty but also a legal duty that is well recognised by South African common law. The court held that the duty of a medical practitioner to maintain patient confidentiality not only serves to protect the privacy of patients, but it is also vital in securing public health.

The reaffirmation of the importance of the patient's right to privacy and the non-disclosure of medical information by medical practitioners was restated in the case of *NM v Smith.* The applicants in this case contended that, because of the

---

[62] Ibid at para 26.

[63] Ibid.

[64] Ibid at para 27.

[65] Ibid.

[66] Ibid.

disclosure of their names and HIV status to the public, their rights of personality, more particularly their right to privacy, dignity and psychological integrity, had been violated.[67] The constitutional court was called upon to address the effect of the South African Constitution on the common law right of privacy and to pronounce on the scope and content of this right.[68] On hearing the case, the constitutional court justices were unanimous in agreement regarding the private nature of information concerning a person's medical condition, in general, and the fact that they were HIV positive, in particular. However, the dissenting justices did offer a different approach from that of the majority with respect to both the interpretation of the facts of the case and to the legal interpretation of the right to privacy.[69]

Madala J held that:

> '[p]rivate and confidential medical information contains highly sensitive and personal information about individuals. The personal and intimate nature of an individual's health information, unlike other forms of documentation, reflects delicate decisions and choices relating to issues pertaining to bodily and psychological integrity and personal autonomy'.[70]

Consequently, the lack of respect for medical information and its unauthorised disclosure might result in 'fear, jeopardising an individual's right to make certain fundamental choices that he/she has a right to make'.[71] The protection of medical information was furthermore extended, rather than being limited only to the health care personnel.[72] The court in *NM v Smith* continued:

> '[a]s a result, it is imperative and necessary that all private and confidential medical information should receive protection against unauthorised disclosure. The involved parties should weigh the need for access against the privacy interest in every instance

---

[67] *NM v Smith* at para 35.

[68] T Gidron 'Publication of private information: An examination of the right to privacy from a comparative perspective (part 2)' (2010) 2 *Tydskryf vir die Suid-Afrikaanse Reg* at 271–287.

[69] Ibid.

[70] *NM v Smith* at para 40.

[71] At para 41.

[72] A Le Roux-Kemp 'HIV/AIDS, to disclose or not to disclose: That is the question' (2013) 16 (1) *PER: Potchefstroomse Elektroniese Regsblad*.

> and not only when there is an implication of another fundamental right, in this case the right to freedom of expression'.[73]

Regardless of the fact that the applicants had given their consent to participate in the clinical trial and in the consequential enquiry, the court held that they unquestionably had not given express informed consent for highly personal and confidential material to be published in a book, which was to be widely circulated throughout South Africa.[74] Earlier consent given by the applicants was for a specific limited purpose, and it precludes the information from being published for an alternative purpose. The consent was 'limited to medical records and if any other publication was envisaged the requisite consent had to be obtained for that particular publication'.[75] Thus, an individual's direct interest in controlling information about himself and keeping it confidential remains intact. It was made clear by the court that it is fundamentally flawed to assume that others have the right to access private medical information once it has left the hands of authorised medical personnel involved in their medical treatment.[76] The courts verified one of the cornerstones of health care and a fundamental characteristic of the practice of medicine, viz. that of confidentiality.[77]

Section 14, in creating a new constitutional right to privacy, may influence the development of the common law action for privacy infringement. Inversely, courts, in providing content and recognition to the substantive right to privacy, will be guided by common law precedents.

It is argued by McQuoid-Mason that the distinctions between a 'private law delict' under common law and 'public law delict' arising from a breach of a fundamental right are 'more apparent than real'. The investigation, he suggests, should rather consider whether or not the common law of delict vis-à-vis personality rights 'should be incrementally developed to accommodate the relevant constitutional

---

[73] *NM v Smith* at para 43.

[74] Ibid at para 80.

[75] Ibid.

[76] Ibid at para 44.

[77] Le Roux-Kemp (n 72).

imperatives', thereby evolving into a new, and different, form of constitutional delict, and, if so, what such version of invasion of privacy should look like.[78]

Currently, the courts seem likely to continue advancing the common law by 'infusing it with the spirit of the Constitution'.[79] Consequently, a 'hybrid action based on a mixture of the common law and constitutional imperatives' may emerge in time.[80] Clearly, though, broad protection is afforded to the right to privacy by the South African legal system, which is the favourable rhetoric of the courts. Undeniably, privacy protection in South Africa, particularly within a health care context, is both well established and understood in the jurisprudence.

(4) Limitation of the right to privacy

The South African constitutional right to privacy, like its common law counterpart, is not an absolute right but may be limited.[81] The limitation clause is set out in Section 36 of the Constitution. Accordingly, the Constitution provides that the rights in the Bill of Rights may be limited only in terms of the law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society, based on human dignity, equality and freedom, taking into account all relevant factors, including (i) the nature of the right; (ii) the importance of the purpose of the limitation; (iii) the nature and extent of the limitation; (iv) the relation between the limitation and its purpose; and (v) less restrictive means to achieve the purpose.[82]

Data protection legislation should therefore strike a balance between the fundamental right to privacy of the data subject, as contained in Section 14 of the Constitution, on the one hand, and the legitimate need of other persons, on the other hand, to obtain information about the data subject.

---

[78] McQuoid-Mason (n 18) at 227 at 246 and South African Law Reform Commission 'Privacy and Data Protection' Discussion Paper 109 Project 124 The Commission Pretoria (October 2005) at 18.

[79] McQuoid-Mason (n 18) at 260.

[80] Ibid at 260 and 261.

[81] See in *Bernstein v Bester*: '… In the context of privacy this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community.'

[82] Section 36(1) of the Constitution.

The balance is between the right to privacy, and the right of access to information and the freedom of speech and expression. These are provided for in Chapter 2 of the Bill of Rights at Sections 16 and 32.

Competing interests may be, for instance, the administering of national social programmes, the need to maintain law and order, issues of national security and protecting the rights, interests and of others, including the economic interests of banking, insurance, direct marketing, *health care*, *pharmaceuticals* [my emphasis] and travel services. Clearly, the task of balancing these opposing interests is a delicate one.[83] Ackermann J in the Constitutional Court case of *Bernstein v Bester* cautioned against employing common law principles when interpreting fundamental rights and their limitations.[84]

At common law, the determination of whether an invasion of privacy has occurred forms a single enquiry. The court held that '[a]s in the case of other *iniuriae,* the presence of a ground of justification excludes the wrongfulness of an invasion of privacy'.[85] To find delictual liability under the common law for a violation of privacy, the conduct in question must be said to be wrongful, that is, when using the criterion of reasonableness or the norm of *boni mores*.[86] Thus, in terms of common law, data industry practices may constitute a wrongful invasion of privacy, where such violation is by way of an unlawful intrusion upon the personal privacy of another, or an unlawful disclosure of private facts about a person. The unlawfulness of an infringement of privacy is adjudged 'in the light of contemporary *boni mores* and the general sense of justice of the community as perceived by the Court'.[87]

---

[83] See the summary of preliminary recommendations set out in the South African Law Reform Commission report 'Privacy and Data Protection' Discussion paper 109 Project 124 October 2005.

[84] *Bernstein v Bester* at para 71, which held that '[c]aution must be exercised when attempting to project common law principles onto the interpretation of fundamental rights and their limitation; it is important to keep in mind that at common law the determination of whether an invasion of privacy has taken place constitutes a single enquiry, including an assessment of its unlawfulness. As in the case of other *iniuriae* the presence of a ground of justification excludes the wrongfulness of an invasion of privacy. In constitutional adjudication under the Constitution, by contrast, a two-stage approach must be employed in deciding constitutionality of a statute'.

[85] Defences may include *inter alia* consent, absolute privilege, statutory authority, private defence and necessity.

[86] *Bernstein v Bester* at para 68 and *Financial Mail (Pty) Ltd v Sage Holdings Ltd* at 462F.

[87] *Financial Mail (Pty) Ltd v Sage Holdings Ltd* at 462G.

The court, however, explained that the position in constitutional adjudication differs, in that it requires a two-stage approach.[88] In the case of a constitutional invasion of privacy, it requires the assertion, firstly, of whether the invasive law or conduct infringes on the right to privacy, as contained in the Constitution. To do so, the person has to show that he or she has 'a subjective expectation of privacy', which is 'objectively reasonable'.[89] Unless it is a violation of a person's 'inner sanctum', a person's expectation of privacy should be balanced against 'the conflicting rights of the community'.[90]

And if so, secondly, it must be asked whether such an infringement is justifiable in terms of the requirements contained in the limitation clause in Section 36 of the Constitution. For this reason, the Constitutional Court has cautioned against simply applying common law principles to the interpretation of fundamental rights and their limitations.[91]

(5) South African legislation influencing privacy and data protection in health care[92]

The Constitution requires that all laws in South Africa be congruent with the provisions contained in the Constitution. Section 8 and the related s 39(2) of the Constitution mandate the legislature to ensure that all constitutional rights are provided substance and content, and that any prevailing conflicting laws be brought

---

[88] *Bernstein v Bester* at para 71.

[89] McQuoid-Mason (n 18) at 247 and see *Bernstein v Bester* at para 75.

[90] Ackermann J describes a person's 'inner sanctum' as their 'family life, sexual preference and home environment' in *Bernstein v Bester* at para 69.

[91] See *Bernstein v Bester* at para 71 and South African Law Reform Commission '(n 84) at 18. Also McQuoid-Mason (n 18) at 246.

[92] It is beyond the scope of this thesis to discuss the intricacies of all South African data protection legislation, for instance, the National Credit Act No. 32 of 2005 and the POPI Act. I have restricted myself to only those enactments, which have a direct influence on data protection within the health care system primarily for two reasons: firstly, the POPI Act seeks to consolidate many of the disparate provisions found in the various acts and, secondly, data protection governance within the health care environment is also and more importantly to be found embedded in various health care legislation and medical regulatory guidelines.

into line, not only with the express provisions of Chapter 2, the Bill of Rights, but also with the 'spirit, purport and objects' of the Bill of Rights.[93]

In South Africa, statutory measures have been introduced to achieve health-related demands, and to bring about health reform, thereby ensuring that human rights are not mere promises but legitimate and enforceable rights.[94] This pertains not only to the constitutional right to life but also to the right to privacy. Singh *et al.* assert that South Africa is one of the best known examples of how 'human rights matter to health' and that South Africa is a country 'in which an explicit codified right to health has prompted health reforms'. Despite the country's 'failure to ratify the covenant on economic, social, and cultural rights' [specifically article 12 of the International Covenant on Economic, Social, and Cultural rights of December 1966], South Africa has shown 'how respect for, and promotion of human rights can lead to improved health outcomes'.[95]

(i) The National Health Act No. 61 of 2003 and the National Health Amendment Act No. 12 of 2013[96]

The National Health Act has as its primary purpose to 'provide a framework for a structured uniform health system within the Republic, taking into account the obligations imposed by the Constitution and other laws… with regard to health services…'.

In the preamble to the National Health Act, the Act recognises 'the socio-economic injustices, imbalances and inequities of health services of the past and the need to improve the quality of life of all citizens', and acknowledges Section 27 (2) of the Constitution, which provides that the State must take 'reasonable legislative and

[93] Section 39(2) states: '[w]hen interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights' and sections 8(3)(a) and (b) which provides: '[w]hen applying a provision of the Bill of Rights to a natural or juristic person in terms of subsection (2), a court – (a) in order to give effect to a right in the Bill, must apply, or if necessary develop, the common law to the extent that legislation does not give effect to that right; and (b) may develop rules of the common law to limit the right, provided that the limitation is in accordance with section 36(1)'.

[94] JA Singh, M Govender and EJ Mills 'Do human rights matter to health?' (2007) 370 *Lancet* at 521.

[95] Ibid.

[96] A Gray and Y Vawda 'Health Policy and Legislation' in *South African Health Review 2013/2014* (2014) *Health Systems Trust*.

other measures within its available resources to achieve the progressive realisation of the right of the people of South Africa to have access to health care services'.

Regarding the position of eHealth and privacy protection in South Africa, Chapter 2 of the National Health Act has particular relevance. Confidentiality-related provisions are set out in Section 14, and Sections 15 through 17[97] provide for access to health records and their protection. These sections effectively strengthen the ethical principles of confidentiality into a statutory requirement.[98] Section 14 of the National Health Act defines confidentiality as follows:

'(1) All information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment, is **confidential**.

(2) Subject to section 15, no person **may disclose any information** contemplated in subsection

(1) unless –

(a) the user consents to that disclosure in writing;

(b) a court order or any law requires that disclosure; or

(c) non-disclosure of the information represents a serious threat to public health'.

'Protection of health records' is contained in Section 17, which provides for privacy related issues.[99] Particular references in Sections 6, 7 and 8 are made regarding informed consent.

---

[97] Section 15 provides: a health care professional '... may disclose such personal information to any other person, health care provider or health establishment as is necessary for any legitimate purpose within the ordinary course and scope of his or her duties where such access or disclosure is in the interests of the user…'.

[98] H Oosthuizen and T Verschoor 'Ethical principles becoming statutory requirements' (2008) 50 (5) *SA Family Practice* 36 at 38 and A Gray, Y Vawda and C Jack 'Health policy and legislation: legislation and financing' (2012/2013) *South African Health Review* at 10 and 11.

[99] C Jack and M Mars 'Telemedicine: A need for ethical and legal guidelines in South Africa' (2008) 50 (2) *South African Family Practice* at 60c.

(ii) The Health Professions Council of South Africa's guidelines

The Health Professions Council of South Africa[100] is a statutory body, created pursuant to powers granted in terms of the Health Professions Act. The Council, which is mandated by the South African government to provide regulations, guides health care professions in South Africa in aspects pertaining to the ethical behaviour and conduct of health professionals and in 'fostering compliance with health care standards'.[101] The HPCSA has developed a series of ethical rules and guidelines, which have been set out in booklets regulating, for instance, the good ethical practice relating to, for instance, confidentiality and the protection of information.[102] The regulatory mandate of the HPCSA affects health care practitioners in both state and privately owned health care institutions and its primary purpose is to protect patients against abuse or maltreatment by health care practitioners, while affording guidance to medical professions on what constitutes good medical practice and appropriate and acceptable conduct.[103] With regard to the regulation of eHealth and telemedicine, the HPCSA has recently published draft guidelines governing the ethical practice of telemedicine in South Africa.[104]

The existing guidelines contained in Booklet 11 in respect of confidentiality seek to inform medical professionals dealing with patients' personal information and to provide direction concerning the storage, confidentiality and protection of such patient information.[105] These guidelines state that a practitioner may divulge information regarding a patient only if this is done: 'in terms of a statutory provision, at the instruction of a court, in the public interest, with the *express consent* of the patient, with the *written consent* of a parent or guardian of a minor under the age of 12

[100] Referred to as the 'HPCSA'.

[101] As described on the HPCSA's website. Available at http://www.hpcsa.co.za/ (accessed 20 February 2017).

[102] HPCSA *Confidentiality: Protecting and providing information* (2nd ed) Booklet 11 (2007).

[103] HPCSA *General Ethical Guidelines for good practice in Telemedicine* Booklet 17.

[104] Ibid.

[105] Although still regarded as primary sources of guidance, the promulgation of recent legislation has amended and extended this considerably. See Oosthuizen and Verschoor (n 98) at 37–40.

years, or in the case of a deceased patient with the *written consent* of the next of kin or the executor of the deceased's estate'.[106]

Likewise, the draft 'General Ethical Guidelines for good practice in Telemedicine Booklet 17' states at 4.5.3 that '[h]ealthcare practitioners should not give medical advice or provide treatment using telemedicine *without obtaining proper informed consent* from the patient for both the treatment to be given and the use of telemedicine technology'.[107] The draft guidelines continue at 4.6.2 '[i]nformed consent for the use of telemedicine technologies must be obtained *in writing*.' Additionally, a lengthy and onerous list of documentation is required in the provision of informed consent'.[108]

The guidelines provide that a patient should be informed as to who will have access to their information where telemedicine is practiced. Additionally, a copy of the consent form should be kept with the patient's records and a duplicate given to the patient.[109]

Certainly, one should exercise caution in distinguishing between eHealth medical professionals *per se* and other health care professionals, as defined by the Health Professions Act. Perhaps it is prudent rather to talk of health care practitioners who provide the same services, treatment and care, but who merely use eHealth platforms to do so and who must nevertheless adhere to the same laws and regulations as those providing traditional health practices. Surely, eHealth medical practitioners have the same core ethical values, responsibilities and duties as their non-eHealth counterparts in respect of the same health care services, as required by virtue of their being qualified and registered in terms of their respective professions.[110]

It is worth noting that the principles established by the HPCSA do not bind every member of the health care sector, but only those registered in terms of the Health Professions Act. Unfortunately, this results in an entire sector of the health care industry being without guidelines: this includes allied health practitioners,

---

[106] HPCSA (n 102) at 2–3.

[107] HPCSA (n 103) at 8.

[108] Ibid at 9 and 4.6.5 at 10.

[109] Ibid at 10.

[110] See M Kekana, P Noe and B Mkhize 'The practice of telemedicine and challenges to the regulatory authorities' (2010) 3 *S Afr J Bioethics Law* at 34.

African traditional practitioners and health establishments, ranging from clinics and hospitals to service providers assisting with the storage of stem cells and sperm banks.

The guidelines do not bind other eHealth industry players either, such as software developers and those controlling and transferring personal health data outside of the medical profession, where the potential for data mismanagement is rife. Likewise, in light of the jurisdictional limitations inherent in the application of the guidelines, together with the borderless unrestricted flow of eHealth data and advisory resources, draft guideline 4.1.3 stipulates that, where telemedicine crosses country borders, medical practitioners assisting or treating South African patients should be registered not only with the regulating bodies in their country of origin but also with the HPCSA.[111]

A further challenge posed by the implementation of eHealth is the involvement of non-health care participants, for instance, information technology specialists. There is no requirement for these IT specialists, operators and data managers to register with any regulatory authority. Moreover, they fall outside of any provisions determined by the HPCSA and are thus not governed by them. Although certain protection may be afforded by compliance in terms of the POPI Act, a clear risk to the privacy and safety of patient information cannot be excluded.

With regard to the security of patient information, the following is provided:

> '(a) Patient information should only be transmitted from one site to the other and stored, with the full knowledge and approval of the patient, in line with the informed consent guidelines'.[112]

The informed written consent required by the guidelines, along with the extensive written documentation required surrounding such consent, and the onerous stipulation that written records be held at both the sending and receiving location where eHealth activities are practiced, are not only impractical but excessively burdensome on a health care system, which is already understaffed and in crisis.

Additionally, the position regarding how, if at all, informed consent may be obtained electronically by, for instance, the use of cellular telephones, remains unresolved. Whether consent obtained in this way can be construed as 'written'

---

[111] HPCSA (n 103) at 6.

[112] Ibid at 14.

consent, consistent with the provisions of the ECT Act, is also unclear. eHealth activities can be conducted partially or wholly electronically in an online environment. The ECT Act (as does the UNCITRAL Model Law on E-Commerce[113]) adopts the principles of non-discrimination, technological neutrality and functional equivalence.[114] The principle of non-discrimination stipulates that any document should not be denied legal effect, validity or enforceability by virtue solely because it is in an electronic format.[115] The principle of technological neutrality enforces the provision that various technologies used are all of neutral value, while functional equivalence establishes criteria under which electronic documents may be considered equivalent to paper-based documents.[116] Despite the formality for consent to be 'written', the extent to which the ECT Act may provide relief to eHealth practitioners, where data messages are recognised as the functional equivalence of written messages, and electronically provided consent has the equivalent legal value as that written on paper, is uncertain. The imposition of written informed consent by policy makers in those countries with low literacy levels and significant language variances is suggestive of an impediment to telemedicine and eHealth usage rather than an enabling one. It was found in research conducted by Jack and Mars that '[w]ritten informed consent is not routinely obtained from patients during clinical examination or when using ICT for the transfer of patient information' despite a statutory requirement for this to be undertaken.[117] This suggests that, where a requirement in law is impractical or unrealistically achievable, it may simply not be implemented or

---

[113] UNCITRAL Model Law on Electronic Commerce: Resolution adopted by the General Assembly [on the report of the Sixth Committee (A/51/628)] 51/162 Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law, see particularly Chapter III article 5, which holds '[i]nformation shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.'.

[114] See ECT Act Chapter III Part I s 11(1) to (3), s 12, s 14(1) and (2), s 15(1) to (4), s 16 (1) and (2), and s 17(1) and (2).

[115] Section 11 of the ECT Act provides '(1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message'.

[116] Section 12 of the ECT Act provides '[a] requirement in law that a document or information must be in writing is met if the document or information is - (a) in the form of a data message; and (b) accessible in a manner usable for subsequent reference.'

[117] As set out in the National Health Act. For more, see CL Jack and M Mars 'Informed consent for telemedicine in South Africa: A survey of consent practices among health care professionals in Durban, KwaZulu-Natal' (2013) 6 (2) *South African Journal of Bioethics and Law* at 55–59.

enforced. Nevertheless, the narrative is clear: eHealth issues and the governance thereof require thoughtful and insightful direction and remain an ongoing challenge to policy regulators in South Africa.[118]

(iii) The Electronic Communications and Transactions Act 25 of 2002 (ECT Act)

Sections 50 and 51 of the ECT Act apply to personal information that has been obtained through electronic transactions. The ECT Act sets out the accepted data protection principles, describing how personal data, as defined in the ECT Act, may be collected and utilised.[119] The definition contained in the ECT Act for 'personal information' includes specifically 'physical or mental health, well-being and disability'. Section 51 compels 'data controllers' to have the 'express written permission of the data subject for the collection, processing or disclosure of any personal information on that data subject'.[120] Moreover, sub-section 4 provides that '[t]he data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.'

Additionally, a data controller may not disclose any personal information to a third party unless required by law or expressly permitted by the data subject to do so, should 'delete or destroy all personal information which has become obsolete', and may use personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, only so 'long as the profiles or statistical data cannot be linked to any specific data subject by a third party'.[121]

Integral to the success of eHealth delivery systems is the sharing and exchange of sensitive or personal data, which infers the transmission of data between parties and locations. Data security methods, such as cryptography, digital watermarking and

---

[118] Kekana *et al.* (n 110) at 33.

[119] See Snail and Papadopoulos (n 46) at 292–293 for the ways in which personal data may be collected including viruses, 'trojan horses', hacking, and 'spoofing'.

[120] A 'data controller' means 'any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject'.

[121] Sections 51(6) and 80.

steganography have been proposed as possible measures to safeguard data.[122] The onus of non-disclosure of information to third parties rests on the data controller.

However, the ECT Act is silent on the extent of security, if any, required – but merely unreservedly prohibits disclosure to a third party without consent. One can only deduce what constitutes the expected adequate or plausible level of security under the circumstances, as this is not explicitly stipulated in the ECT Act, but presumably, it is whatever is reasonably necessary to avert disclosure to third parties. Given that the POPI Act provides protection for the processing of personal information in an electronic format, it will probably supersede the comparable provisions in the ECT Act.[123]

(iv) The Protection of Personal Information ACT 4 of 2013 (POPI)

The introduction of the POPI Act in South Africa will necessitate amendments to existing South African legislation. Most notably, it will affect certain provisions in the Promotion of Access to Information Act 2 of 2000, the ECT Act and the National Credit Amendment Act 19 of 2014.[124]

a. The background to the POPI Act

In 2013, the much-anticipated POPI Act was assented to by the President of the Republic of South Africa and promulgated in Government Gazette No. 37067. Its commencement date is to be determined on a date in accordance with s 115(1) of the Act by proclamation in the Gazette. Section 114 allows parties who process personal information, a period of one year from the date of commencement of the provisions of the POPI Act to conform therewith.

Privacy and data protection issues were initially approved for inclusion in an enquiry conducted by the South African Law Reform Commission as early as 2000.The SALRC's report noted the significant impact that global trends have on

---

[122] AO Adesina, KK Agbele, K Kehinde, R Februarie, AP Abidoye and HO Nyongesa 'Ensuring the security and privacy of information in mobile health-care communication systems' (2011) 107 (9–10) *South African Journal of Science* at 1.

[123] Van der Merwe *et al.* (n 45) at 368.

[124] SALRC (n 83) at 9 fn 49.

international trade and the unrestricted exchange of data across borders, and records that information privacy cannot 'simply be regarded as a domestic policy problem'. It recognised that personal information can be effortlessly transferred outside the borders of the country of origin, resulting in the necessity of strengthened international harmonisation efforts, and a concomitant endeavour to regulate and standardise transborder data flows between nations.[125] Moreover, the report recommended that South Africa's information privacy and data protection framework should align itself more closely with transnational data protection instruments, thus ensuring that the 'adequate' protection demanded by certain international regulations is complied with, and that future participation in global information markets is encouraged.

b. The purpose of the POPI Act

The POPI Act has as its primary purpose the promotion and protection of personal information processed by private and public bodies, thereby giving effect and substance to the right of privacy contained in Section 14 of the Constitution. In so doing, it endeavours to achieve a delicate balance of this right to privacy against other rights contained in the Constitution, particularly the right of access to information.[126]

The legislation seeks to find a sustainable and equitable balance between the interests of opposing rights, that of an open, transparent and accountable society, on the one hand, and the right to be left alone, on the other.[127] The right to privacy, as embodied in the POPI Act, is delicately balanced against the interests contained in its legislative 'competitor', the Promotion of Access to Information Act.

The POPI Act has committed to the objective of regulating 'the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information' and to protect 'important interests,

[125] Ibid at v.

[126] Neethling (n 10) at 245.

[127] SALRC (n 83) at 4 and C Piller 'Privacy in peril' (1993) 10 (7) *Macworld* at 124–130.

including the free flow of information within the Republic and across international borders'.[128]

The POPI Act provides for the safeguarding of personal information, as defined. Exceptions include the processing of personal information by the Cabinet and the courts, as well as for purposes of purely personal or household activities, national security or defence, criminal investigation and prosecution, and journalism. Such exemptions and exceptions are granted to data processors where the risk of privacy violation is relatively low, or where private or the public interests exceed those of the right to privacy.[129]

The POPI Act, in seeking to regulate the way in which personal information is processed, includes the processing of so-called 'special information', and provides recourse by means of remedies to those whose rights have been infringed.[130] A degree of flexibility is envisaged, in that data processing industries are permitted to develop their own codes of conduct, in accordance with the data protection principles set out in the Act, which will be overseen by a regulatory authority.[131]

Section 107(a) of the POPI Act grants individuals protection measures with regard to their rights, and remedies and penalties for non-infringement or violation are severe.[132] Section 39 provides for the establishment of an Information Regulator, thus ensuring the enforcement and fulfilment of the rights protected in terms of Act.

c. Conditions for the processing of personal information

Section 4 of the POPI Act provides for the lawful processing, as defined, of personal information. The POPI Act seeks to protect the eight core data-protection principles in respect of the processing of personal information embodied within the Act. Accordingly, Section 4 (1) sets out the conditions for the lawful processing of personal information by a responsible party under the following headings:

---

[128] Chapter 1 Section 2 (a) ii and 2 (b) of the POPI Act. See a commentary on the bill before it was enacted in Snail and S Papadopoulos (n 46) at 299.

[129] A Roos 'Core principles of data protection law' (2006) 39 *CILSA* 102 at 127.

[130] Chapter 3, Part A and Part B of the POPI Act, and chapters 10 and 11.

[131] Chapter 7 of the POPI Act and see Neethling (n 10) at 246.

[132] Penalties for non-compliance amount to fines not exceeding 10 million ZAR or imprisonment of up to 10 years.

(a) 'accountability',

(b) 'processing limitation',

(c) 'purpose specification',

(d) 'further processing limitation',

(e) 'information quality',

(f) 'openness',

(g) 'security safeguards', and

(h) 'data subject participation'

It is a requirement that personal information be processed 'lawfully' and in a 'reasonable manner that does not infringe the privacy' of the person. The Act further provides that 'personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive'. The person from whom data is collected must consent to the processing and be made aware clearly and precisely of the purpose for which the information is to be processed. The information must be collected directly from the person and for a specified, explicit, and legitimate purpose. Additionally, personal information may not be retained for longer than is necessary for the specified purpose, and such information should not be used for any other purpose than that for which it was collected. Moreover, the POPI Act prescribes that the 'responsible party', as defined, has an obligation in terms of the Act to take reasonable steps to ensure that information is complete, accurate, not misleading and is updated where necessary.[133]

Further, it is incumbent upon the responsible party to put security measures in place to ensure that personal information is safeguarded against loss, damage to and unlawful access to or processing of personal information.[134]

d. Sections 19 through 21 – Security measures

Of relevance to the health care environment are the provisions contained in Sections 19 through to 21 regarding the security measures that protect the integrity of

[133] Sections 8 to 18.

[134] Section 16(1).

personal information. As safeguarding security and the maintenance of data integrity are integral to the provision of privacy, this is of utmost importance to emerging eHealth processes.

Section 19 of the POPI Act provides that a responsible party 'must secure the integrity and confidentiality of personal information in its possession or under its control by taking action to prevent (a) loss of, damage to or unauthorised destruction of personal information; and (b) unlawful access to or processing of personal information'.

The POPI Act provides in Section 19(2) that the responsible party is obliged to take 'reasonable measures to (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; (b) establish and maintain appropriate safeguards against the risks identified; (c) regularly verify that the safeguards are effectively implemented; and (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards'.

It is further incumbent upon the responsible party to have 'due regard to generally accepted information security practices and procedures', which may be required in terms of professional rules and regulations in respect of their profession or industry.

Section 20 provides that an operator or any person acting under the authority or on behalf of a responsible party must process information only with the knowledge or authorisation of the responsible party and should 'treat personal information which comes to their knowledge as confidential and must not disclose it unless required by law or in the course of the proper performance of their duties'. This is of particular importance to hospital staff and health care administrators or any person authorised by the health care practitioner to process personal information on their behalf.

Section 21 provides that '[a] responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in Section 19.' Further, it is the responsibility of the operator 'to notify the responsible party immediately' where personal information has been accessed or acquired by any unauthorised person.

e. Sections 26 and 32 – Authorisation of a data subject's health data

Special provision is made for the protection of so-called 'sensitive personal information' relating to children, religion or philosophy of life, race, trade-union membership, political persuasion, *health* and *sexual life*, and criminal behaviour in Chapter 3 of the POPI Act.[135] Section 26 provides: '[a] responsible party may, subject to section 27, not process personal information concerning—(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, *health or sex life* or biometric information of a data subject'.

However, the prohibition contained in Section 26 does not apply to the processing of information by certain categories of persons and institutions, including, but not limited to, 'medical professionals, health care institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned'.[136] This is qualified under Section 32(2) as information processed only by responsible parties subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject. The prohibition does not apply where it is necessary to supplement the processing of personal information concerning a person's health with a view to the proper treatment or care of the person. Information regarding the person's health and sex life, as well as biometric information, may only be processed by responsible parties 'subject to an obligation of confidentiality by virtue of their office, employment, profession or legal provision' or if 'established by a written agreement' between the responsible party and person.

With regard to eHealth applications, any personal information that is processed by a health practitioner for the purposes of his professional activity, including online activities, will be required to comply with the conditions imposed by the POPI Act.

---

[135] My emphasis. Chapter 3 Part B sections 26 to 33, of particular significance are sections 26, 27 and 32.

[136] Section 32(1).

f. The significance of the POPI Act in eHealth in South Africa

South Africa is in the favourable position of realising privacy protection through several legal sources, namely, by virtue of the law of delict, under the right to privacy contained in the South African Constitution and in terms of recent provisions contained in omnibus data protection legislation.[137] The mutually advantageous interaction between these three sources of protection within the South African legal system renders individuals' rights in cases of violation not only protected in terms of law, but it also provides the infringed party with clearly actionable and enforceable remedies.

South Africa has recently adopted statutory protection in the form of the POPI Act. In the preamble to this enactment, the right to privacy contained in Section 14 of the Constitution is recognised. The POPI Act seeks to satisfy the obligation placed on the state to respect, protect, promote and realise this fundamental right, while taking cognisance of the reality that, within the framework of an information society, the 'removal of unnecessary impediments to the free flow of information, including personal information' is required.[138] The POPI Act aims to regulate, in harmony with international standards, the processing of personal information, which gives effect to the right to privacy, subject to justifiable limitations.[139] Additionally, the POPI Act seeks to add a degree of administrative control by means of an 'information regulator', which allows the aggrieved party the option of seeking redress through an alternative means, without needing to resort to litigation. [140]

Pre-emptive caution is required in allowing unfettered access to personal and sensitive data, and the POPI Act is an attempt to achieve this. To facilitate optimal eHealth care, practitioners require more clearly defined access parameters within which to work, as the access to and transferability of a patient's medical records, such as the history of their condition, previous diagnoses and treatments, are imperative in

---

[137] Certain situations cannot be accommodated at common law, with remedies only available under the Constitution, for instance, where the court is required to invalidate a statute.

[138] Preamble to the POPI Act.

[139] Exemption from the conditions for the processing of personal information is provided for in Chapter 4 of the POPI Act, while exclusions are found in Sections 6 (1) (a) through (e), 6 (2) and 7(1).

[140] Chapter 5. See D van der Merwe 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda (2014) 17 (1) *PER* at 298.

providing quality treatment.[141] Certainly, markedly defined strictures are desired, which balance freer access to personal medical data with sensitive patient care.

Also significant is the manner in which personal information is processed, as well as the type of information that is protected. These have been extended by the POPI Act, and they include the processing of 'special personal information', as defined.[142] The POPI Act provides that 'appropriate, reasonable technical and organisational measures' be taken to prevent 'loss of, damage to or unauthorised destruction' or 'unlawful access' to personal information. It is not clear, however, what these 'appropriate and reasonable measures' would be and what would be considered sufficient security in an eHealth environment. Whether it would be considered reasonable and appropriate security, for instance, to use e-mail encryption software available in commercial packages, such as Microsoft Outlook®, which requires little more than the 'unlocking' of an email message by the recipient by means of an encryption key, remains to be seen.

Likewise, the level of security that is considered sufficient for the hard drives of personal computers of health care practitioners where patients' health records are stored, or for practitioners who participate in 'store and forward' e-mail based telemedicine, as well as for those who participate in online eHealth discussion or advice forums, is vague and yet to be determined.[143] It may well be left to the judiciary to establish the precise meaning and extent of these concepts, as greater clarity in this respect will certainly be needed in the future.

III CONCLUSION

In this chapter, the position of privacy and data protection within South Africa was considered. South Africa was discussed as an example of how data protection regulation may be implemented on a national level. This chapter provides the position of South Africa as a case study, mirroring the issues found within the African region as a whole, and considers recently implemented South African data protection

---

[141] Adesina *et al.* (n 122) at 2.

[142] Defined in Chapter 1, Section 1 of the POPI Act.

[143] Jack and Mars (n 99) at 60 and see Kekana *et al.* (n 110) at 33.

legislation. The following chapter will consider various influencers that have affected the adoption of privacy protection within eHealth on the African continent.

CHAPTER 6: DRIVERS OF EHEALTH PRIVACY REGULATION

Privacy is one of the biggest problems in this new electronic age.

Andy Grove

I INTRODUCTION

After analysing the substance of eHealth services and the nature of privacy and data protection in Chapters 2 and 3, data protection regulatory measures pertaining to the African continent and to South Africa were ascertained in Chapters 4 and 5 respectively. This chapter sets out certain recent influencers within the digital environment, which may inform or direct the eHealth privacy and data protection regimes of the future.

Various interrelated themes central to the argument regarding privacy protection in an online health environment are considered. Technological realities, such as big data and cloud computing, and the steady introduction of novel health care platforms and initiatives, such as the establishment of centres of excellence within Africa, as well as the emergence of global health care, directly affect data and the need to safeguard it. Recent medical developments, such as the changing nature of the doctor-patient relationship and the principle of confidentiality, are reviewed.

Additionally, the chapter considers the following questions: whether any boundaries in cyberspace exist; whether privacy is of concern to online users, and particularly, to users in developing countries; and whether data protection is a luxury that we can ill afford in the developing world.

II TECHNOLOGICAL CONSIDERATIONS

Certain technical drivers or influencers have emerged recently, which have an impact on privacy regulation. Questions posed are: are there boundaries in cyberspace? Is privacy a concern to online users generally, and then also specifically, to those found in developing countries? And, lastly, is privacy protection regulation an ill-afforded luxury in countries with more urgent health care needs? The development of cloud computing and big data and its significance to eHealth initiatives is described.

(1) Are there any boundaries in cyberspace?

Considerations of cyberspace governance[1] have been the subject of much recent attention.[2] Attempts at applying traditional privacy and disclosure legal rhetoric to an online, digital environment are problematic. Reservations arise from the nature of the Internet where limitations of distance and location become increasing irrelevant; connections between users are no longer determined by location-dependent processes; and the differentiation between private and public margins of social interaction become obfuscated.[3]

In accessing the cyber environment, a user may unwittingly be subjected to a haphazard and inconsistent quagmire of regulation. Whereas the jurisdictional extent of a country is determined geographically, such notions of physical constraint are meaningless constructs in cyberspace. Nevertheless, this has not hindered geographic sovereigns from enacting regulations, with varying degrees of success, in an attempt to control online behaviour.[4]

For many online transactions, including those involving an eHealth component, multiple sovereigns may have jurisdiction, based on the nature of the activity within their borders.[5] Consequently, questions of how choice of law rules will operate have implications for online activity. It is possible to conduct one's affairs so that key elements of the transaction occur in different countries. Constructing and manipulating elements of online transactions in order to maximise the benefit of 'regulatory havens' is achievable. Thus, users have had the opportunity to 'forum shop', or to select the jurisdiction that is most advantageous to their purposes.

---

[1] J Kang 'Information Privacy in Cyberspace Transactions' (1998) 50 *Stanford Law Rev*iew at 1195 describes cyberspace as 'the web of consumer electronics, computers, and communication networks that interconnects the world'.

[2] DG Post and DR Johnson 'Chaos Prevailing on Every Continent: Towards a new Theory of Decentralized Decision-making in Complex Systems' (1998) 73 (4) *Chicago-Kent Law Review* at 1055.

[3] Ibid and S Papadopoulos 'Revisiting the Public Disclosure of Private facts in a Cyberworld' (2009) 30 (1) *Obiter* at 31.

[4] PP Swire 'Of Elephants, Mice, And Privacy: International Choice of Law and the Internet' (1998) 32 (4) *The International Lawyer* at 991.

[5] M Kekana, P Noe and B Mkhize 'The practice of telemedicine and challenges to the regulatory authorities' (2010) 3 *S Afr J Bioethics Law* at 34.

Moreover, the Internet has effectively enabled 'supra-jurisdictionality', where acts are not subject to any jurisdiction or specific authority.[6] The Internet allows transactions 'in indefinable or undiscoverable geographic space, such that no courts (even of a powerful and bold country) could convincingly claim jurisdiction'.[7] The Internet circumvents traditional barriers of distance and borders, which effectively places it beyond the regulatory reach of any one national state's direct influence. Internet users, 'as long as they share a common language and a reasonably rapid connection', may be generally 'indifferent to the physical location of those with whom they communicate', affording them the opportunity to engage in what Froomkin describes as 'regulatory arbitrage'.[8]

The a-geographical nature of cyberspace, as reported in the Leveson Report, noted that the online social media world remains 'beyond regulation'. It describes the insurgence of social media as 'little short of phenomenal'. The report acknowledged that websites are 'entirely unregulated' and that this situation was 'unlikely to change'. It concluded that '[d]espite the efforts made to comply with national law, it is clear that the enforcement of law and regulation online is problematic'.[9]

Sir Tim Berners-Lee, credited as the inventor of the World Wide Web for his pioneering work conducted at CERN in 1989,[10] in a discussion on the future of the Internet said: 'there have always been forces to try to control the Internet. When you are the government of a country it is very tempting to want to govern the Internet within your country… the trouble is it doesn't work because the Internet is not a thing of countries'.[11]

---

[6] See R Clarke 'Internet privacy concerns confirm the case for intervention' (1999) 42 (2) *Communication of the ACM* at 62 for greater clarification of these terms.

[7] Ibid.

[8] AM Froomkin 'The Internet as a source of Regulatory Arbitrage' in *Borders in Cyberspace* B Kahin & C Nesson (eds) (1997) at 129 and 142–155.

[9] 'Leveson Inquiry on Twitter and Facebook: Social media World remains "beyond regulation"' *Huffington Post UK* 29 November 2012 and the Leveson Inquiry 'Culture, practices and the ethics of the press'.

[10] CERN is the European Laboratory for Particle Physics. Available at http://home.cern/topics/birth-web (accessed 18 July 2016).

[11] See Sir Tim Berners-Lee speaking at a conference sponsored by The Duke Law Center for Innovation Policy on October 17, 2014 to discuss the future of Internet regulation. Available online at https://law.duke.edu/video/internet-regulation-2020-tim-berners-lee-kc-claffy-henning-schulzrinne-daniel-weitzner/ (accessed on 20 February 2017).

Moreover, controlling Internet activities cannot be achieved by simply applying the laws relevant to other forms of telecommunication.[12] This is because information on the Internet can be accessed immediately and distributed globally, and because the Internet differs in nature and scope to other telecommunication channels.[13] The Internet is uncontrolled, unlimited by boundaries and accessible worldwide.[14] The conclusion drawn is that, while most Internet providers indicated 'that the Internet needs regulating', the degree of regulation required remains unclear.[15] As the Internet is a global network operated by countries under their own sets of laws, regulating the Internet on an international level 'may be impossible'.[16]

This is confirmed in Higgins and Azhar, who stated that '[c]yberlaw is, by nature, global'.[17] The Internet is a dynamic ubiquitous information system, with ill-defined boundaries.[18] It is thus impossible to regulate it in any meaningful way. Westphal and Towell indicate that '… the cultural diversity in the world will make it difficult to govern the Internet'.[19] Despite this, when asked who should regulate the Internet, the overwhelming response was '… according to an individual country's legal system'.[20]

Moreover, the Internet is 'forever', in the sense that, which is disclosed and documented online, will potentially have lasting and uncontrollable consequence.[21] Thus, data protection represents a challenge, as acknowledged by policymakers in

---

[12] H Westphal and E Towell 'Investigating the future of Internet regulation' (1998) 8 (1) *Internet Research* 26–31.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] A Higgins and A Azhar 'China begins to erect second Great Wall in Cyberspace' (1996) *The Guardian*.

[18] A Seppälä, P Nykänen and P Ruotsalainen 'Privacy-related context information for ubiquitous health' (2014) 2 (1) *JMIR Mhealth and Uhealth.* See also D van der Merwe 'A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda' (2014) 17 (1) *PER* at 298.

[19] Westphal and Towell (n 12) at 26–31.

[20] Ibid.

[21] S Tobak 'You have no privacy – get over it' (2013) *FOXBusiness*.

their attempts to safeguard user rights.[22] A study conducted in respect of Israeli websites and their compliance with information privacy regulation highlighted these challenges. The research observed the information privacy procedures of 1360 active websites in Israel. They sought to determine the extent to which these websites actually complied with applicable legal requirements with regard to information privacy. Information procedures were investigated on three levels: firstly, they conducted a legal analysis and examined the legal requirements applicable to information practice under the Israeli law of the time; secondly, they investigated the declared privacy policies that were accessible to users on each website; and thirdly, they studied the actual information procedures practiced by each website[23].

The research concluded that data protection regulators have difficulties constructing a single legal measure that is comprehensive enough to regulate the entire Internet. Rather, it was suggested that regulating online behaviour requires tailored regulatory measures.

The discourse amongst European and American regulators has centred on the appropriate limitations to be imposed, and the degree of control required, in regulating online privacy. This remains the subject of rigorous debate. What the Israeli study revealed was that a significant disparity exists between the legal privacy requirements and the actual practice of information privacy.[24] A high level of deviation in compliance with legal rules was observed. The conclusion was overwhelmingly that the law with regard to the protection of personal information is very relevant. In fact, the legal regime should facilitate and promote an open infrastructure and foster an environment of personal 'self-help'.[25]

The most effective form of control of cyberspace is by 'government intrusion' through regulation. This, Greenleaf proposes, is essential in the preservation of important values, as digital libertarianism and its claim of promoting the

[22] M Birnhack and N Elkin-Koren 'Does Law Matter Online? Empirical Evidence on Privacy Law Compliance' (2011) *Mich. Telecomm Tech Law Rev*iew at 337.

[23] Ibid.

[24] Ibid.

[25] Ibid.

'independence' of cyberspace is being manipulated both by private enterprise and by state power.[26]

The problem is whether certain online behaviour should be 'encouraged, discouraged, ignored, or prohibited' and whether such prohibition should be by way of a legally enforceable measure.[27] This gives rise to the following question: 'How does an individual's performance of certain activities affect the well-being of the general population to which that individual belongs?'[28] Once society has decided that online privacy protection is worthy of protection, the legal challenge is to determine the most appropriate method of securing such protection.[29]

(2) Is privacy a concern to online users: The death or decline of privacy?

In advancing arguments with regard to the decline of privacy, certain writers, notably David Brin, are of the opinion that society should accept a concession in personal data protection in favour of the weightier social values of increased transparency and openness. Brin proposes that the powerful (in society) will always possess 'privacy-invasive technologies'. He argues that such privacy protection mechanisms are inherently 'futile', 'impossible' and 'an aberrant notion'. He calls rather for a culture of widespread transparency.[30] Everyone, he believes, should have 'access' to information and the freedom to acquire information, thus promoting freedom and dispelling secrecy. His thinking is that 'if transparency is the norm, the powerful will not be able to hide their own secrets' and that '[s]ociety as a whole is healthier when based on mutual accountability rather than mutual secrecy'.[31] Brin advances the argument that a society of 'glass houses' is sounder than one of 'shields'.[32] By allowing all to be 'watched' freely, the premise is that the watchers (or those in

---

[26] G Greenleaf 'An endnote on regulating cyberspace: Code vs law?' (1998) *University of New South Wales Law Journal* at 1.

[27] Post and Johnson (n 2) at 1064.

[28] Ibid.

[29] Birnhack and Elkin-Koren (n 22) at 383.

[30] See Clarke (n 6) at 62 and see D Brin *The Transparent Society: Will technology force us to choose between privacy and freedom* (1998).

[31] Ibid.

[32] Ibid and see AM Froomkin 'The Death of Privacy?' (2000) 52 (5) *Stanford Law Review* at 1539.

control) will not be able to hide or to preclude others from watching them.[33] Thus, 'the powerful will only be as successful in avoiding observation as they already are in resisting privacy laws that offend their own interests'.[34] Echoing the thinking of Brin, Bernal also suggests that we 'give up on privacy'[35] and accept 'emerging realities'.[36]

On closer inspection, however, this transparency approach is not as beneficial as Brin's initial proposition suggests. His proposition is predicated on the understanding that most, if not all, personal data is to be freely and publically available.[37] Brin's perspective, although intriguing, certainly fails to deliver either immediate or lasting results, as privacy remains, in general, a highly valued and sought after construct in modern society. Criticisms suggest that Brin's view is neither realistically achievable, nor does it advance the core issues relevant to the privacy debate. Froomkin argues that Brin's pessimism about the efficacy of privacy regulations is 'unfounded' or, at least, 'premature'.[38]

Although criticised at the time, the former Sun Microsystems chief executive, Scott McNealy, said nearly 15 years ago, 'you have zero privacy anyway, so get over it'.[39] At the time, McNealy was seeking to denounce government regulation of online consumer privacy in favour of industry self-regulation.

This view was reiterated by Mark Zuckerberg, CEO and co-founder of Facebook, who claimed that, with particular reference to young adults, privacy is 'dead'. Privacy, he suggests is 'no longer a social norm' as '[p]eople have really gotten [sic] comfortable not only sharing more information [of] different kinds, but more openly and with more people'.[40]

Regardless of these sentiments, these views are strikingly incompatible with the attitudes of many individuals who still value privacy highly. As research suggests,

---

[33] Ibid at 63.

[34] Ibid.

[35] See PA Bernal 'Web 2.5: The Symbiotic Web' (2010) 24 (1) *International Review of Law Computers & Technology* at 36.

[36] See Froomkin (n 32) at 1501.

[37] Ibid.

[38] Froomkin (n 32) at 1539.

[39] Tobak (n 21).

[40] B Johnson 'Privacy no longer a social norm, says Facebook founder' *The Guardian* 11 January 2010.

these views are not indicative of the opinion of the vast populace of online users.[41] As noted by Berendt *et al.*, certain users are 'privacy fundamentalists', while others are only 'marginally concerned'.[42] Importantly though, the study revealed that, while many users have 'strong opinions' on privacy, and although they may state specific privacy preferences, they do not necessarily act accordingly.[43] Once engaging online, they 'often do not monitor and control their actions sufficiently' and 'privacy statements seem to have no impact on behaviour'. Users thus place increasing reliance on formalised legal protection.[44]

The move towards rejecting privacy outright is observed by Edwards as an incomplete account of the position. Although acknowledging that conceptions of privacy are changing, the requirement for privacy protection has in no way diminished completely.[45] That people have an expectation of privacy and a definite disquiet about its misuse is also reflected in recent empirical studies.[46] Reflecting critically on the privacy-position, privacy is not generally considered by users as expendable. In fact, Burchell states that, if the law fails to recognise individual privacy protection adequately as a 'hallowed right', a resultant 'governmental knee-jerk reaction' to potential threats and 'individual exploitation' is inevitable. This would lead to a loss of what modest privacy we have had.[47]

Further evidence of the importance of privacy protection is found in a survey conducted by TRUSTe online. According to this report, mistrust is high, with 89% of British Internet users admitting to being concerned about online privacy.[48] More than

---

[41] See Bernal (n 35) at 36.

[42] B Berendt, O Gunther, and S Spiekermann 'Privacy in e-commerce: Stated preferences vs. actual behavior' (2005) 48 (4) *Communications of the ACM* at 101–106.

[43] Ibid.

[44] Ibid.

[45] L Edwards 'Privacy and Data Protection Online: The Laws Don't Work?' in L Edwards & C Waelde (eds) *Law and the Internet* 3 ed (2009) 484. And also at 444.

[46] C Schmierer 'Better late than never: How the online advertising industry's response to proposed privacy legislation eliminates the need for regulation' (2011) 13 *Richmond Journal of Law & Technology* at 6, 7, see also SB Barnes 'A privacy paradox: Social networking in the United States' (2006) 11 (9) *First Monday* 4.

[47] See J Burchell 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* at 1 for more on the threats to privacy.

[48] TRUSTe 2013 Great Britain - Consumer Confidence Privacy Report.

a third of respondents recorded 'frequently' or 'always' being worried about their online privacy. It was recorded that the sharing of personal information with third parties (60%) and tracking online behaviour (54%) were the two largest causes of online privacy concerns.[49] Further, 27% of respondents were concerned about the privacy policies of Facebook and other social media networks, while 21% were apprehensive about the privacy policies of Google and other search engines. A staggering 91% of respondents admitted avoiding conducting business online where they did not believe their online privacy was being protected.[50]

With regard to online health care applications and privacy concerns, a US study reported that 58% of respondents cited the eHealth feature they were most likely to use was to 'communicate with medical practitioners via email, text message of the social media', with 44% of respondents using online access or mobile phones to manage personal electronic health records.[51] Of the respondents interviewed, 49% thought that consumer wariness about privacy violations would deter the adoption of eHealth, while 51% of respondents stated that 'data privacy risks are their biggest concern'.[52]

Likewise, Tachakra *et al.*, in a survey examining the topic of ethical issues and patient confidentiality relating to the use of eHealth, found that patients' concerns regarding telemedicine in their treatment primarily centred on their fears concerning the privacy of transmitted medical records and any data that could potentially identify them.[53] Users are keenly aware and concerned about the threats to their medical data by unwanted disclosure to third parties, such as their employers or insurers, for instance. Indeed, users frequently describe themselves as being 'somewhat' or 'very' concerned about the unwanted use of their data when using mobile devices for medical-related activities.[54]

---

[49] Ibid.

[50] Ibid.

[51] 'Power to the patient: How mobile technology is transforming healthcare' (2015) *The Economist Intelligence Unit Limited* at 20.

[52] Ibid at 14.

[53] S Tachakra, STH Mullet, R Freij and A Sivakumar 'Confidentiality and the ethics in telemedicine' (1996) 2 suppl. 1 *J Telemed Telecare* at 68–71.

[54] Blue Chip Patient Recruitment 'Leveraging Mobile Health Technology for Patient Recruitment: An emerging opportunity' (2012) at 9.

Attempts have been made to describe the tenuous relationship between users, their digital environment, and their privacy. The position in the US is described by Barnes as a 'privacy paradox'.[55] The concept of a 'privacy paradox' was confirmed in research conducted by Lafky and Horan, who reveal that, while consumers express great concern about their privacy online, very few effectively engage in any form of privacy-protecting activities or behaviour.[56] This disconnectedness and inconsistency in users' attitudes and behaviour is 'frustrating' for privacy-focused search engines.[57]

The relationship between an individual's social network and privacy is 'multi-faceted'.[58] Research published revealed that participants experienced high levels of social privacy and psychological privacy because of their 'privacy-protective behavior'.[59] Users are notoriously fickle when it comes to sharing information about themselves. In some instances, they are more willing to reveal personal information than in others, resulting in patterns of personal information revelation being variable across age groups, contexts and different web-site types.[60]

Regardless, the disclosure by users of their personal information should not negate the requirement to safeguard their privacy and protect their data. To infer that privacy is of no concern merely because there is greater user disclosure is to adopt a precarious approach.[61] In fact, increased revelation by a user, and in particular the purpose for which the information was intended, should strengthen, rather than lessen,

---

[55] Barnes (n 46) at 4, where it is explained how the youth in the US freely and unwittingly disclose information about themselves, whereas US adults are more aware and concerned about privacy related issues online. See also A Roos 'Privacy in the Facebook era: A South African legal perspective' (2012) 129 *South African Law Journal* at 393.

[56] DB Lafky and TA Horan 'Personal health records: Consumer attitudes toward privacy and security of their personal health information' (2011) 17 (1) *Health Informatics Journal* at 69. See also A Greenberg 'The privacy paradox' (2008) *Forbes*.

[57] Ibid.

[58] R Gross and A Acquistiti 'Information revelation and privacy in online social networks (the Facebook case)' Proceedings of the 2005 Workshop on Privacy in the Electronic Society (2005) ACM.

[59] M var der Veldan and K El Emam 'Not all my friends need to know: A qualitative study of teenage patients, privacy, and social media' (2013) 20 *J Am Med Inform Assoc* at 16–24.

[60] LA Thompson, E Black, WP Duff, N Paradise Black, H Saliba and K Dawson 'Protected health information on social networking sites: Ethical and legal considerations' (2011) 13 (1) *Journal of Medical Internet Research* at e8.

[61] S Avancha, A Baxi and D Kotz 'Privacy in mobile technology for personal healthcare' (2012) 45 (1) 3 *ACM Computing Surveys* at 3.8.

the need for stringent safeguarding of privacy. Consenting to publication does not signal an abandonment of the right not to consent.

Nevertheless, while acknowledging that conceptions of privacy are shifting, it would appear that the requirement for privacy protection has not diminished at all.

(3) Is privacy a concern to eHealth users in developing countries?

Claims for privacy have long been regarded by certain authors as values that are exclusively the domain of the modern world, with privacy thought to be absent from the social fabric of past and present 'primitive' societies.[62] This unfortunate way of thinking is refuted by various anthropological and sociological studies that conclusively reveal that the need for privacy for individuals and groups is present in virtually every society[63] and that privacy is evidenced in 'primitive' communities.[64] Privacy norms are present at an individual level, a family level and at the level of the community as a whole.[65]

Given that a need for privacy in the vast majority of societies is well established, cultural variants of the concept of 'privacy' do exist. Although privacy is of universal importance, the subject matter of what is regarded as worthy of protection is variable. Differences in interpretation are apparent between various regions with differing societies presenting divergent ideas of what is deemed tolerable, aberrant or abhorrent within a particular society, for instance.

Following Westin's informational control definition of privacy, that is, 'the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others',[66] the term 'privacy' includes aspects of a person's life, which are 'intimate' and/or 'sensitive'.[67] A violation of privacy occurs in the event of sensitive and/or intimate personal data

---

[62] KM Yilma and A Birhanu 'Safeguards of Right to Privacy in Ethiopia: A Critique of Laws and Practices' (2013) 26 (1) *Journal of Ethiopian Law* at 3.

[63] Ibid at 1.

[64] See A Westin *Privacy and Freedom* (1967) at 13.

[65] Yilma and Birhanu (n 62) at 1.

[66] Westin (n 62) at 7.

[67] See L Bygrave *Data Protection Law: Approaching Its Rationale, Logic and Limits* (2002) at 129 and again in JC Inness *Privacy, Intimacy, and Isolation* (1997) at 140.

being disclosed.[68] This is true of personal health data, which, though factually or contextually accurate, may be of such a sensitive and/or personal nature, that it could cause potential harm, embarrassment or ostracism, when disclosed to a third party without the prerequisite data subject's knowledge and/or consent.[69]

The disclosure of medical diagnoses of, for instance, mental health conditions, infectious diseases and diabetes may result in adverse repercussions directed towards persons in developing countries, yet such diagnoses would not necessarily be a cause of sensitivity or shame to persons in developed countries. Particularly problematic are health care issues involving reproductive rights, including sensitivities around sexual activity, sexual orientation and abortion.

An Amnesty International report confirms that: '[m]any Indonesian women and girls, especially those from poor and marginalised communities, struggle to achieve reproductive health in the face of discriminatory laws, policies and practices'.[70] The legal regime in Indonesia requires consent by a woman's husband for various medical treatments.[71]

Similarly, McGirk reports discrimination against those infected with HIV/AIDS, as is widely prevalent throughout Northern Africa and the Middle East.[72] Those infected with HIV/AIDS are often the target of severe prejudice and intolerance and may be subjected to rejection, isolation and even violence from their community.[73] The stigma causes those who are infected to hide their condition and is hampering the effective treatment and prevention of the disease.[74] Social taboo and

---

[68] Ibid.

[69] Policy Engagement Network for the International Development Research Centre 'Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations' (2010) *LSE*.

[70] 'Barriers prevent Indonesian women from achieving reproductive health' (2010) *Amnesty International.*

[71] Ibid.

[72] J McGirk 'Religious leaders key in the Middle East's HIV/AIDS fight' (2008) 372 (9635) *The Lancet* 279.

[73] A Le Roux-Kemp 'HIV/AIDS, to disclose or not to disclose: That is the question' (2013) 16 (1) *PER: Potchefstroomse Elektroniese Regsblad*.

[74] McGirk (n 72) at 279.

homophobia are also widespread, with shame, fear, humiliation and being shunned realistic concerns where privacy is not safeguarded.[75]

In the South African case of *NM v Smith*, the Constitutional Court was invited to address the effect of the South African Constitution on the common law right of privacy and to pronounce on the scope and content of this right.[76] On hearing the case, the Constitutional Court justices were unanimously in agreement regarding the private nature of information regarding a person's medical condition, in general, and the fact that they were HIV positive, in particular.[77] Madala J held: '[t]he disclosure of an individual's HIV status, particularly within the South African context, deserves protection against indiscriminate disclosure due to the nature and negative social context the disease has as well as the potential intolerance and discrimination that result from its disclosure'. He continued in describing the consequences that such a revelation might bring about: 'such a person stands to be isolated and even rejected by others'.[78]

For good reason, sexual orientation is often concealed in certain African communities. Provisions in, for instance, Zimbabwe,[79] Kenya,[80] and southern Sudan[81] criminalise acts of homosexuality with punishment by incarceration in prison, confinement in an insane asylum, fines, and flogging, and, most horrifically in Mauritania[82] and Sudan[83], with homosexuality even being punishable on conviction

---

[75] See the case of *Jansen van Vuuren v Kruger* regarding the position of HIV/AIDS disclosure in South Africa. The intimate nature of such status was reiterated in *NM and Others v Smith and Others*.

[76] Ibid.

[77] T Gidron 'Publication of private information: An examination of the right to privacy from a comparative perspective (part 2)' (2010) 2 *Tydskryf vir die Suid-Afrikaanse Reg* at 271–287.

[78] *NM and Others v Smith and Others* at paras 42 and 63.

[79] Zimbabwe prohibits male homosexual conduct. See Criminal Law (Codification and Reform) Act 23 of 2004, Section 73 (2005) effective July 2006 per Criminal Law (Codification and Reform) Act Cap. 9:23 (No. 23 of 2004), S.I. 152 of 2006, Supplement to the Zimbabwean Government (2006).

[80] The Penal Code of Kenya criminalises sodomy. See Penal Code of 1930 section 162, 15 LAWS OF KENYA Cap. 63 (revised edition 2012).

[81] Penal Code of Sudan Act No. 9 of 2008 section 248 1(1) Act Supplement to the Southern Sudan Gazette (2009).

[82] Article 308 of the Mauritanian Penal Code punishes homosexual acts by Muslim men with death by stoning. See Ordonnance 83–162 du 9 juillet 1983 *portant institution d'un Code Pénal* [Ordinance 83–162 of July 9, 1983, Establishing a Penal Code] Art 308 (July 9 1983).

[83] Ibid.

by death.[84] Only on 17 May 2016 did the Seychelles parliament pass a bill to amend their Penal Code to decriminalise sodomy. The only African country that affirmatively permits same-sex marriages is South Africa.[85]

The Guardian newspaper reported in 2010 that 'human rights activists have warned that the lives of gay people in Uganda are in danger, after a newspaper published a story featuring the names and in some cases photographs of 100 homosexuals under the headline "Hang Them"'.[86] Homosexuality has long been a taboo subject in Uganda, and it is considered by many to be an affront to both Ugandan culture and religion. In fact, the Ugandan parliament has been considering an Anti-Homosexuality Bill, which 'calls for the death penalty for those convicted of repeated same-sex relations, and life imprisonment for others'.[87] The point is that disclosure of certain information in African countries may elicit detrimental consequences not ordinarily experienced in developed countries.

Moreover, the model of personal ownership of a mobile phone that is prevalent in the first world may not be applicable in the developing world, where shared mobile telephone use is common.[88] This is particularly a risk when dealing with sensitive patient related information, for instance, where SMS messages are sent to users, providing them with test results, specific treatment advice, and medication or appointment reminders.[89] The revelation of such content may have dire consequences in communities where mobile phones are shared amongst family members who may inadvertently intercept these messages. It is reported in Aker and Mbiti that a significant number of African mobile phone users have access to mobile phones only

---

[84] See 'Criminal Laws on Homosexuality in African Nations' (2014) *Global Legal Research Directorate Law Library of Congress.*

[85] In terms of the South African Civil Union Act No. 17 of 2006, which legalised same-sex marriages.

[86] X Rice 'Ugandan paper calls for gay people to be hanged' (2010). Available at http://www.theguardian.com/world/2010/oct/21/ugandan-paper-gay-people-hanged (accessed 20 February 2017).

[87] Ibid.

[88] PN Mechael, H Batavia, N Kaonga, S Searle, A Kwan, A Goldberger, L Fu and J Ossman 'Barriers and Gaps Affecting mHealth in Low and Middle Income Countries: Policy White Paper' (2010) *Center for Global Health and Economic Development Earth Institute, Columbia University* at 34.

[89] Ibid.

through sharing them with others.[90] Sharing mobile phones may be challenging to health care interventions, however the exact magnitude of the problem is undetermined.[91] According to a survey conducted by Nokia in 2008 on consumers in emerging markets, mobile phone sharing is on the rise. More than 50% of those surveyed in India and Pakistan and nearly 30% in Vietnam noted that they were currently sharing or would share their mobile phone with family or friends.[92]

The inference is thus three-fold: firstly, what is considered sensitive, personal information in developing countries may differ from that, which is considered private or shameful in developed countries; secondly, disclosure in developing countries may take unusual or different forms to those found in developed countries; and lastly, the implications of such disclosures may have far more severe consequences for users in developing countries than for users in developed countries.

(4) Are data protection and high privacy standards a luxury that the developing world can ill afford, where countries have limited resources and more immediate health care needs?

Clarke states that the slow adoption of e-commerce initiatives in developing countries can be attributed to a lack of trust and confidence by consumers in corporations and governments to safeguard their personal data.[93]

The South African Constitution seeks to act as a bulwark against an oppressive state by supporting the people it serves, while fulfilling an expression of a wider call for social, economic and political progress. As explained by Justice Pius Langa, an understanding of transformative constitutionalism includes 'the pursuit of some form of economic transformation and a change in legal culture'. [94] It seeks to 'heal the wounds of the past' and 'guide us to a better future'.[95] As part of guiding one to a

---

[90] JC Aker and IM Mbiti 'Mobile Phones and Economic Development in Africa' (2010) 24 (3) *Journal of Economic Perspectives* at 212.

[91] WA Kaplan 'Can the ubiquitous power of mobile phones be used to improve health outcomes in developing countries?' (2006) 2 (9) *Globalization and Health*.

[92] 'Nokia unveils two handsets that offer a range of useful features and colours aimed at consumers in emerging markets' (2008).

[93] Clarke (n 6) at 62.

[94] P Langa 'Transformative Constitutionalism' (2006) 17 (3) *Stell Law Review* 351–360 at 353.

[95] Ibid at 352.

better future and, at the very least, attaining the material conditions for a dignified life, one could argue that eHealth can provide substance to the socio-economic right to health care.

The promise of new technologies to revolutionise and drive health care and communications across Africa is well-traversed terrain. eHealth, by enhancing connectivity and facilitating the flow of health information and health care services and delivery, can empower isolated and disenfranchised communities. In light of the weakened health care position experienced in most developing countries, and the need to attain even the most basic right to health care, the question to be asked is whether it is imperative that eHealth be adopted, to the extent that it is possible, and whether there is a place for the adoption of less stringent data protection measures, rather than the ever increasing push for stronger and more robust protection, as experienced by developed countries.

Certainly, data protection measures and policies require a high degree of policymaking innovation and strengthening. [96] Without meaningful regulatory oversight, unregulated data processing poses a threat to individual liberties. Governments can respond to technological developments and provide protection in a variety of ways.[97] By strengthening the privacy rights of individuals – particularly in terms of consent and the right to be informed – the current imbalance can be altered. This shift in power is transformative in its ability to instil user confidence and trust.

Despite one of the most notable features of eHealth being the realisation of significant health care savings (mostly in developed nations) and the provision of health care, treatment and care (to many people in developing countries), the widespread deployment of eHealth initiatives is still remarkably limited, as eHealth service providers are confronted with legal uncertainty with regard to their potential liability regarding personal and sensitive data infringements in the health sector.

The failure of developing countries to adopt data protection measures timeously may reinforce an underlying message and suspicion already prevalent

---

[96] See A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 *South African Law Journal* at 402 and A Roos 'Core principles of data protection law' (2006) 39 *CILSA* 102 at 103, where she concludes that almost all developed countries have data protection laws in place.

[97] Ibid at 402 and CJ Bennett *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (1992) 30–31 at 30.

amongst first world economic operators, including eHealth developers and investors, who perceive an inadequacy in legislative and judicial measures in large parts of the African region.[98]

Developing countries may resist elevated data protection standards by claiming that unrealistically high standards of data protection, as found in developed states, may be obtained at the expense of and impeded eHealth development. Developed countries, in contrast, argue that, by implementing more stringent and higher data protection measures, with fewer flexibilities, international eHealth initiatives and cross-border data transfers may be better promoted, as international organisations can be assured of an adequate privacy and data protection framework. This in turn encourages more technological growth and innovation and, of course, the desirable eHealth services and delivery.

As stated by Ariel Pablos-Méndez: '[f]or a given e-health solution to achieve scale and sustainability, it must be effective and efficient in its own right and it must be seamlessly integrated into the health system'.[99] Potential for abuse, especially with regard to privacy and data protection, cannot be overstated, particularly in societies with traditions of ethnic conflict and unrest.

Apart from theoretical perspectives, the opinion of the user is also powerful and should not be underestimated. If the user demands privacy protection, and deems it important, it is conceivable that they will expect to receive it. Seemingly, the choice to transact and thus to inform the direction of privacy protection criteria may well vest in them.[100] This is also true of users in developing countries.

---

[98] S Mancuso 'The New African Law: Beyond the difference between Common Law and Civil Law' (2008) 14 (1) *Annual survey of International & Comparative Law* 39.

[99] WHO 'The bigger picture for e-health' (2012) 90 (5) *Bulletin of the World Health Organization* 321–400.

[100] Clarke (n 6) at 62, where he states 'we can choose'.

(5) Cloud Computing and the role of Big Data in health care

(i) Cloud Computing

The term 'cloud computing' describes a range of services offered over the Internet.[101] The National Institute of Standards and Technology, an agency of the US Department of Commerce, defines it as: 'a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.'[102]

Cloud computing comprises online applications and services, and the hardware and software systems supporting such applications, which are held in various data centres.[103] The data centre hardware and software are termed a 'cloud'.[104] It refers to the storing, processing and use of data on 'remotely located computers accessed over the Internet'[105] and enables services to be carried out, on behalf of users, on hardware that is neither owned, managed nor controlled by the user.[106] Typically, the user uploads input data[107] to the cloud provider's server.[108] The cloud provider then supplies access to the data at the user's request.[109] Consequently, a

---

[101] See R Berry and M Reisman 'Policy challenges of cross-border cloud computing' (2012) 4 (2) *Journal of International Commerce and Economics* at 1.

[102] Final Version of NIST Cloud Computing Definition Published (2011).

[103] M Armbrust, A Fox, R Griffith, AD Joseph, R Katz, A Konwinski, G Lee, D Patterson, A Rabkin, I Stoica and M Zaharia 'A view of cloud computing' (2010) 53 (4) *'Communications of the ACM* at 50–58.

[104] Ibid.

[105] Moreover, it is defined as hardware and software applications delivered as services over the Internet in a data location in ibid and definition in European Commission 'Green Paper on mHealth' (2014) at 10.

[106] S Pearson, Y Shen and M Mowbray 'A Privacy Manager for Cloud Computing' in *Cloud Computing* (2009) at 90–106.

[107] For instance, e-mails, images, records.

[108] Pearson *et al.* (n 106)) at 90–106.

[109] See Berry and Reisman (n 101) at 1 and Pearson *et al.* (n 106) at 90.

user's data is stored and controlled, in an unencrypted format, remotely on a hardware device. This may pose a threat to a user's data privacy.[110]

Cloud computing enables the cross-border transfer of data, as personal information is hosted and 'transferred' to a foreign jurisdiction or site. With regard to the health care sector, medical data is thus transferred across national or state borders where limited consensus exists, regarding which authorities have jurisdiction over the data.[111] Privacy regulations also vary across jurisdictions, with the resultant possibility of uncertain legal constraints on the management of data by cloud computing providers in the geographical location of the machine.[112] Although cloud computing offers many benefits to the health care sector, including, for instance, electronic health records, telemedicine, ePrescriptions and digital imaging, the difficulty arises where highly sensitive medical data is managed remotely by cloud providers 'who may have operations spanning many different countries or even continents'.[113] Armbrust *et al.* cite security violations as a frequent objection to cloud computing.[114]

As cloud technology evolves, the pace of regulation in the area of data privacy, security and data transference is failing to develop rapidly enough.[115] While Japan,[116] the US[117] and Europe[118] are making significant inroads into the regulation of cloud computing,[119] specific challenges identified are assurances concerning users'

---

[110] Ibid at 90–106. Cloud computing creates challenges for policy-makers, healthcare organisations and the IT industry, see JJM Seddon and WL Currie 'Cloud computing and trans-border health data: Unpacking U.S. and EU healthcare regulation and compliance' (2013) 2 (4) *Health Policy and Technology* at 229.

[111] Ibid at 229.

[112] Pearson *et al.* (n 106) at 90.

[113] Seddon and Currie (n 110) at 229.

[114] Armbrust *et al.* (n 103) at 50–58.

[115] Berry and Reisman (n 101) at 1.

[116] See R Martin 'Japan is best prepared to capitalize on cloud computing' (2012).

[117] The US Health Information Portability and Accountability Act Privacy Rule of 2013 protects the privacy of individually identifiable health information.

[118] The European Commission has released a cloud computing strategy with the purpose of facilitating the rapid adoption of secure cloud solutions in Europe. The aim is to support the secure storage of health data over the Internet. See COM (2012) 529, 'Unleashing the Potential of Cloud Computing in Europe' 27.09.2012.

[119] Seddon and Currie (n 110) at 229.

privacy and the security of their data.[120] Users of cloud technology confront potential breaches in security from both outside and within the cloud.[121]

Berry and Reisman suggest that the best method of addressing these issues is through the development of a regulatory framework of domestic policy, international bilateral and multilateral agreements, and international co-operative forums, and industry arrangements.[122] A systematic review of regulation and compliance of data protection and data flows is required.

(ii) Big Data

The concept of 'big data' is defined as 'high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making'.[123] Related to this is the term 'data fusion', which describes not merely the collection of individual data elements, but the fusing together of multiple data sets. It is recorded in a paper published by Stanford University's School of Medicine that 2.5 exabytes of data are generated from computers, mobile devices and sensors every day. While the Internet comprised a mere 100 terabytes[124] in 1993, it is now estimated to comprise four zettabytes[125] of data.[126]

---

[120] W Venters and E Whitley 'A critical review of cloud computing: researching desires and realities' (2012) 27 *Journal of Information Technology* at 179–197.

[121] Armbrust *et al.* (n 103) at 50–58.

[122] Berry and Reisman (n 101) at 1.

[123] Gartner's IT Glossary. Available at http://www.gartner.com/it-glossary/big-data/ (accessed 20 February May 2017). In addition to volume, velocity and variety, certain commentators have added the 'v' attributes of 'value' and 'variability' to definition of big data, see SD Esposti 'When big data meets dataveillance: the hidden side of analytics' (2014) 12 (2) *Surveillance and Society* 209; O Tene and J Polonetsky. 'Big data for all: Privacy and user control in the age of analytics' (2012–2013) 11 (5) *Northwestern Journal of Technology and Intellectual Property* at 240.

[124] A terabyte is a unit of measurement used for measuring data storage and is defined as 10^{12} or 1,000,000,000,000 bytes. Available at http://www.techterms.com/definition/terabyte (accessed 20 February 2017).

[125] A zettabyte is defined as 10^{21}, or one sextillion (1,000,000,000,000,000,000,000), bytes; 1000 exabytes..Available at http://www.thefreedictionary.com/zettabyte (accessed 20 February 2017).

[126] E Ashley, S Israni and L Minor 'Data science and the practice of modern medicine' (2014) 1 (9) eHealthlaw&policy.

As the quantity of data being digitally collected and stored is growing rapidly, the science of data management and analysis is also advancing, thereby giving organisations the ability to convert this data into information and knowledge that assist in achieving their objectives.[127] This powers the effectiveness of big data.[128] Analysing big data aids in the development of clinically beneficial predictive models,[129] devising strategic health care planning,[130] establishing short-term trends in illness transmission, [131] the long-term remote monitoring of personal health conditions,[132] and advancing the diagnosis, treatment, and prevention of diseases.[133] By leveraging off of big data analytics within the field of health care, it becomes practicable to improve the quality and efficiency of health care delivery and to examine connections across a vast range of data sets for a variety of medical research purposes.[134]

Murdoch and Detsky cite the following ways in which big data may advance health care delivery:[135] Firstly, big data may be instrumental in generating new knowledge. Patient, or user, data is stored in large and complex, albeit unstructured, data sets, which may then be analysed computationally to reveal patterns, trends and associations. Big data facilitates the linking of data, and potentially extracts valuable

---

[127] TB Murdoch and AS Detsky 'The Inevitable Application of Big Data to Health Care' (2013) 309 (13) *JAMA* 1351 and BD Mittelstadt and L Floridi 'The Ethics of Big Data: Current and foreseeable issues in Biomedical Contexts' (2015) *Sci Eng Ethics* 1.

[128] S Cameron 'Q&A: The US big data report and fully utilising big data within healthcare' *eHealth Law & Policy*.

[129] S Choudhury, JR Fishman, ML McGowan and ET Juengst 'Big data, open science and the brain: Lessons learned from genomics' (2014) 8 *Frontiers in Human Neuroscience* at 3.

[130] Tene and Polonetsky. (n 123) at 244.

[131] Ibid at 246.

[132] Mittelstadt and Floridi (n 127) at 4 and also see BD Mittelstadt, NB Fairweather, M Shaw and N McBride 'The ethical implications of personal health monitoring' (2014) 5 (2) *International Journal of Technoethics* 37–60 and BD Mittelstadt, BC Stahl and NB Fairweather 'How to shape a better future? Epistemic difficulties for ethical assessment and anticipatory governance of emerging technologies' (2015) *Ethical Theory and Moral Practice* 1–21.

[133] Mittelstadt and Floridi (n 127) at 3.

[134] Murdoch and Detsky (n 127) at 1351 and L Floridi 'Big data and their epistemological challenge' (2012) 25 (4) *Philosophy & Technology* 435–437.

[135] Ibid.

information from unstructured data in an automated and cost-effective way.[136] Such data compilations, for instance, of measurements, medical images and symptom descriptions can be stored in large databases and, with the aid of data-mining algorithms, can enhance health care research, innovation and provide opportunities with regard to diagnosis, treatment monitoring, surveillance of disease and disease control.[137]

With the proliferation and increasing sophistication of technological platforms, such as mobile phones, it is estimated that personal sensor data will increase from 10% of all stored data in 2009 to an enormous 90% within the next decade.[138] Analysing unstructured data contained within, for example, Electronic Health Records, using computational techniques, permits automated data refinement.[139] Big data offers the capacity to create a large observational evidence data set for quantifiable research, which might otherwise be impossible. Such vast amounts of data are a vital element of epidemiological research, as researchers establish patterns or trends on a larger scale and draw conclusions, thereby improving treatment.[140] This is helpful in issues of clinical generalisability.[141]

Secondly, big data aids the dissemination of knowledge. The digitisation of medical literature improves access to the most recent evidence guiding clinical practice.[142] This approach differs from conventional medical decision support tools, in that suggestions are derived from real-time patient data analysis, rather than solely using rule-based decision trees.

Thirdly, big data allows for the transformation of health care by delivering information directly to patients, thus empowering them to play a more active role in their health care decision-making and treatment options.[143] Big data also offers the opportunity to integrate the traditional health care model, that is, where patients'

---

[136] Green Paper on mHealth (n 105) at 9.

[137] See A Pentland, D Lazer, D Brewer and T Heibeck 'Improving Public Health and Medicine by the use of Reality Mining' A Whitepaper for the Robert Wood Johnson Foundation (2009) at 2 and ibid.

[138] Ibid at 2.

[139] Murdoch and Detsky (n 127) at 1351.

[140] Green Paper on mHealth (n 105) at 9 and Floridi (n 134) at 435–437.

[141] Murdoch and Detsky (n 127) at 1351.

[142] Ibid.

[143] Ibid.

primarily paper-based records are stored with health care professionals, with the social basis of directing health care towards a patient-centric fashion. It is envisaged that medical records reside with the patient themselves.[144] Understandably, this will give rise to privacy concerns, which will require ostensibly more extensive data protection solutions, as the fundamental right to personal data protection applies equally in the context of big data.[145]

Such is the importance and growth of the big data driven economy that the European Commission committed, on 13 October 2014, in a public-private partnership with the Big Data Value Association, to make available an investment of €2.5 billion to 'put Europe at the forefront of the global data race' by supporting research and innovation in big data technologies and infrastructures. Such development indicates that the European Union intends to strengthen privacy protections for European users, while acknowledging and capitalising on the huge market advantage inherent in big data.

A 2016 WHO report noted that only six EU member states have a national policy or strategy regulating the use of big data in the health sector. Only 9% of EU member states have a national policy or strategy regulating the use of big data by private companies.[146] The survey questioned EU member states on barriers to the adoption of big data in health care, and found that the three most critical barriers (rated as very or extremely important) are, firstly, 'a lack of data privacy and security laws', 'limited integration between different health services and other systems collecting data' and, lastly, 'a lack of support for new analytical methods'.[147] These barriers reflect a lack of adequate data governance.[148]

---

[144] Ibid.

[145] Green Paper on mHealth (n 105) at 10, where it is stated: '[t]he fundamental right to personal data protection fully applies in a big data context'. See J Jonas 'Interview: Data protection challenge of the future: Big Data'.

[146] WHO 'From innovation to implementation: eHealth in the WHO European Region' (2016).

[147] Ibid at 72.

[148] Ibid.

III MEDICAL DEVELOPMENTS

The changing nature of the doctor-patient relationship, the emergence of a globalised health regime, and the establishment of centres of excellence are medical developments, which drive the development of privacy regulation within health care. These are discussed in turn.

(1) The nature of the doctor-patient relationship and the principle of confidentiality

(i) The changing nature of the doctor-patient relationship

In the 1950s, sociologist Talcott Parsons described the concept of the 'sick role'; he found that the doctor's role in the health care encounter was based on a high degree of specialisation, professionalism and the application of expert medical knowledge and technical competence.[149] Doctors maintained a 'dominant autonomous authority', while patients occupied a 'more passive, submissive role'. This entrenched power imbalance continued well into the late 1970s.[150]

Discussions of trust and confidentiality were frequent topics in medical ethical forums prior to the 1970s.[151] Medical ethics focused on questions of professionalism and the role that ethics played in the formation of trust between a doctor and patient. Trust presupposes the belief that a person will render continued and absolute integrity, justice, and confidentiality. Ethics is a 'branch of philosophy dealing with what is morally right or wrong'.[152] Many professions, including medical professionals, lawyers and priests, have embraced strong confidentiality principles in their ethical codes.[153] The principle of confidentiality has as its basis competence, respect, and

---

[149] MZ Varul 'Talcott Parsons, the Sick Role and Chronic Illness' (2010) 16 *Body & Society* 72–94.

[150] SE Burke *The doctor-patient relationship: An exploration of trainee doctors' views* (PhD Thesis University of Birmingham) (2008) at 45.

[151] MA Hall 'Law, Medicine, and Trust' (2002) 55 *Stanford Law Review* at 469.

[152] *Merriam-Webster Dictionary*. Available at http://www.merriam-webster.com/dictionary/ethics (accessed 28 January 2017).

[153] I Goldberg, A Hill and A Shostack 'Trust, Ethics and Privacy' (2001) 81 *Boston University Law Review* at 111.

confidence.[154] Medical trust and confidentiality have value because of the personal, sensitive and emotional content.[155] This arises from the deep vulnerability experienced during illness, which consequently necessitates a considerable degree of confidentiality.[156] As a medical ethical construct, the doctor-patient relationship ultimately had a corrosive effect on patient health privacy in a broader sense.[157]

The conventional doctor-patient relationship has been essentially contractual in its metaphor and paternalistic in policy.[158] During the 1980s, a fundamental shift occurred, away from the passive acceptance of doctor's advice and unquestioning admiration and acceptance of the medical practitioner's authority, together with a degree of disillusionment with the traditional health care structures. With extensive and more vocal consumer protection in the 1980s, the sick abandoned the role of the 'child' in accepting medicine from a paternalistic doctor and began to assume the role of 'adults', capable of independent thought and informed decision-making. This trend of people taking greater responsibility for their health, increased information seeking and involvement in decision-making, along with the need for self-determination and autonomy, coupled with a willingness to challenge the power that doctors exercised over them, altered the dynamic between doctor and patient. Thus, the doctor-patient relationship and the notion of trust and confidentiality has transformed in contemporary western society.[159]

Interactions between doctors and patients do not exist in a vacuum; they are influenced by the socio-cultural context within which they occur.[160] Although patients have become more consumerist and the balance has shifted towards greater patient autonomy, it is argued 'that the medical profession remains firmly in control of key

---

[154] NP Terry 'What's wrong with health Privacy?' (2009) 5 *Journal of Health and Biomedical Law* 1–32 at 16.

[155] Hall (n 151) at 470.

[156] Ibid.

[157] Terry (n 154) at 15.

[158] Ibid at 16.

[159] Ibid.

[160] Ibid.

decisions concerning treatment and that patients continue to expect this to be the case'.[161]

Clearly, though, health care interactions today are unlikely to take the form of the 'medical dominance' of health care professionals over patients, as was the case in the past.[162] Interactions are anticipated to be far more complex in the future, with relationships based primarily on that of 'health partnerships', with an 'active or expert patient' being seen as the way forward.[163] As Coulter has suggested, paternalism, though widespread and as well intentioned as it may be, creates an unhealthy dependency on health professionals that is 'out of step' with other trends in society. Patients are maturing and professionals are required to accommodate this.[164]

A relationship based on partnership would thus be one where patients are more empowered, sharing in the decision making processes, promoting self-management of their conditions and, more importantly, having access to and control of their personal medical information.

(ii) Confidentiality

Given the altered nature of the patient-doctor relationship and the inherent weaknesses in the disclosure-centric confidentiality model, a transformative approach to eHealth privacy protection is needed from that of mere 'soft' ethical guidelines to protection that comprises reinforcement that is more expansive.[165]

The traditional role of confidentiality progresses as follows: patients disclose information to doctors in the belief that it will aid their diagnosis and treatment, while doctors respect such confidences, to encourage patients to reveal personal and medical information that will make diagnosis and treatment easier and more effective. The difficulty is that this notion of confidentiality becomes unstable when it exists outside

---

[161] M Bury 'Researching patient-professional interactions' (2004) 9 suppl. *Journal of Health Services Research and Policy* 48 at 52.

[162] Ibid at 48.

[163] Ibid at 52.

[164] A Coulter 'Paternalism or partnership? Patients have grown up and there's no going back' (1999) 319 *BMJ* at 719–720.

[165] S Gritzalis 'Enhancing Privacy and Data Protection in Electronic Medical Environments' (2004) 28 (6) *Journal of Medical systems* at 535–547.

of the doctor-patient paradigm. This is the case when it is applied in, for instance, institutional or industrial models of care or in eHealth contexts. As the context changes, the simple and innocuous traditional approach becomes increasingly utilitarian and complex.[166] eHealth poses a threat to privacy that cannot be resolved through traditional confidentiality models alone.

A 2011 World Health Organization report identified 'health information security' and 'patient confidentiality' as pertinent policy challenges to overcome for eHealth promotion and validation.[167] The security of data 'is a particularly important issue to address within the area of policy' with data security and privacy key areas requiring 'legal and policy attention' thus ensuring that users' data are not compromised.[168]

While the development of eHealth holds promise, difficulties persist that are impeding its adoption. A concern identified is 'the privacy and security of data transmitted and accessed' both online and via electronic devices.[169] eHealth technologies have the ability to collect, store, disseminate and use vast quantities of personal and medical data. Such technologies have a potentially deleterious influence on patients' data privacy rights.[170]

eHealth policy frameworks necessitate an appropriate balance between the promoting of entrepreneurship and the maintaining of patients' and users' data security.[171] Reiterated in Mechael *et al.* is that a significant barrier to eHealth development is data security and confidentiality.[172] As quoted by Ronald Plesser: '[m]edical records are a top priority "due to the sensitivity of the data …".'[173]

Moreover, difficulties arise in determining liability for breaches of confidentiality for medical practitioners involved in eHealth consultations. In eHealth and telemedicine consultations more than one doctor is frequently involved, the

---

[166] Terry (n 154) at 9.

[167] WHO 'mHealth: New horizons for health through mobile technologies' in the second *Global Observatory for eHealth Series* vol 3 (2011) at 64.

[168] Ibid at 2 and 6.

[169] K Congdon 'The rise of mHealth' (2013) *Health IT Outcomes*.

[170] Terry (n 154) at 14.

[171] Mechael *et al.* (n 88) at 59.

[172] Ibid at 22.

[173] C Piller 'Privacy in peril' (1993) 10 (7) *Macworld* at 124–130.

referring doctor, usually at the same location as the patient, together with the doctor consulting via telemedicine. The patient is still ostensibly under the care of the referring doctor. This differs from traditional referrals, where a doctor refers the patient to a specialist, who then takes over the responsibility for diagnosis and continued treatment of the patient. Patient information then flows freely between locations using various technological platforms and is transferable and accessible by various parties, with no guarantee or legal obligation to ensure its protection or safekeeping.

Crucially, while the ethical notion of confidentiality would suffice in the simplistic delivery paradigm of the traditional doctor-patient relationship, the myriad of new relationships and structures brought about by the evolution of eHealth services and the industrialision of medical practice, the traditional professional confidentiality model has been relegated to primarily an operational concept with a dearth in patient data protection.[174] The resultant metamorphosis in health care delivery systems and industrial providers encounters few of the traditional ethical or legal constraints, and both systems and providers are positioned to exploit patient data for utilitarian or commercial purposes.[175] Consequently, the conventional, traditional approach to data protection within the patient-doctor relationship and the responsibility to ensure confidentiality does not necessarily sit comfortably with the advancement of eHealth. Social media can 'dramatically blur the line between public and private spaces'.[176] The permanent nature of postings online means 'that the control over information dissemination, once posted, differs significantly from a fleeting and local interaction within a hospital or outpatient office'. [177]

Confidentiality, synonymous with a simpler model, in the context of an ongoing relationship of care and treatment, remains an essential element in the ethical professional practice between doctors and their patients and this is likely to remain

---

[174] Terry (n 154) at 14.

[175] Ibid.

[176] See GT Bosslet 'Commentary: The Good, the Bad, and the Ugly of Social Media' (2011) 18 *Academic Emergency Medicine* 1221 at 1222 and GT Bosslet AM Torke SE Hickman CL Terry and PR Helft 'The patient-doctor relationship and online social networks: results of a national survey' (2011) 26 *J Gen Intern Med* 1168 at 1172.

[177] Ibid.

unchanged.[178] The concept of privacy-confidentiality protection inherent in a single physician-patient relationship is likely to fail, however, when the doctor-patient relationship is extended and replaced by fragmented care, or where various physicians administer care at differing stages of the treatment process.[179] As 'continuity of care' diminishes, denoting a relationship of impermanence, for instance, in the prescribing relationship that a patient would have with a doctor prescribing medicine over the Internet, arguably so do the levels of accountability compared to those found in more traditional delivery channels.[180]

In traditional medical practice, the ethical, legal, and operational domains were largely synchronised. Contextually, the parallelism between legal, ethical, and operational domains was not particularly harmful.[181] However, the nature of the doctor-patient relationship, while formerly an ethical and moral dilemma, which could be easily regulated using principles of confidence, has now evolved into a far more complex relationship within the context of eHealth delivery, with sensitive medical data transmitted over a variety of technological communication channels, and involving many more participants, both medical and non-medical.

Non-traditional health care providers such as, for instance, those engaged in eHealth services, may not provide shelter by disclosure-centric confidentiality principles. The danger in relying on confidentiality provisions contained in medical ethical guidelines or codes of conduct in the practice of eHealth is that medical and personal data is often managed and processed by people other than medical practitioners. While medical practitioners may be governed by confidentiality guidelines, other third parties are not necessarily bound by such duties.

A further difficulty in relying solely on the medical ethical principle of confidentiality is that, as the advancement of patient-centred health care increases, the core value of preserving trust and confidence is replaced with a heightened awareness by patients of doctors', perceived or otherwise, lack of or diminished

---

[178] D Knapp van Bogaert and GA Ogunbanjo 'Ethics in Health care: Confidentiality and information technologies' (2014) 56 (1) Supp. 1 *SA Family Practice* at S3 and Terry (n 154) at 16.

[179] Terry (n 154) at 18.

[180] Ibid at 17 and 18.

[181] Ibid at 17.

trustworthiness.[182] Ethicist Mark Hall states that the modern theoretical approach to privacy and confidentiality in respect of health law principles has changed considerably and that it is predicated on, and supported by, a healthy scepticism of trust and understandable caution by patients.[183] With the steady demise of the traditional, long-standing and personal relationship between doctor and patient, the rules around confidentiality and privacy have had to be transformed too. The deterioration of the traditional doctor-patient relationship, and the consequential shift from a relationship between intimates to one based on medical encounters between strangers, is noted.[184] Childress and Siegler confirm this:

> 'Whether medicine is now only a series of encounters between strangers rather than intimates, medicine is increasingly regarded by patients and doctors, and by analysts of the profession – such as philosophers, lawyers, and sociologists as a practice that is best understood and regulated as if it were a practice among strangers rather than among intimates'.[185]

While a supportive legal regime is achievable where its foremost benefit is in its regard for confidentiality and trust as virtues worthy of protection in a traditional doctor-patient relationship, as the relationship becomes more multifaceted a greater threat to breach in confidentiality follows.[186] Terry states:

> '[a] concept of privacy-confidentiality protection that is bound to an outdated conception of the confidence inherent in a single physician-patient relationship was bound to fail when the physician-patient relationship was replaced by fragmented care'.[187]

The legal protection of patient data, previously achieved primarily by virtue of the nature of the doctor-patient relationship and the disclosure-centric principle, expressed as breach of confidence and actionable through implied contract or delict, is

---

[182] Terry (n 154) at 29.

[183] Hall (n 151) at 463, 464–66.

[184] Terry (n 154) at 18.

[185] JF Childress and M Siegler 'Metaphors and Models of Doctor-Patient Relationships: Their Implications for Autonomy' (1984) 5 *Theoretical Med and Bioethics* at 22.

[186] Hall (n 151) at 498.

[187] Terry (n 154) at 19.

a paradigm now affording inadequate protection, as it is overwhelmed by the realities of modern medical and personal data complexities. Patient data in eHealth systems is 'comprehensive, portable, and manipulatable' and the resultant potential for privacy abuse is enormous.[188]

(2) The emergence of a globalised health regime

A defining factor of the 21st century is the increasingly rapid integration of economic, social, medical and political activity worldwide.[189] Additionally, a steady transference from the individual to the global has been noticed.[190] 'Global health' refers to the point at which '... determinants of health or health outcomes circumvent, undermine or are oblivious to the territorial boundaries of the state and this beyond the capacity of individual countries alone to address through domestic institutions'.[191] To facilitate a new global approach to health care, Benatar *et al.* advise that a 'common set of principles to deal with global health threats' should be agreed upon. [192] These principles form the corpus of what is understood as 'global health ethics'. 'Global health ethics' are an attempt to conceptualise the 'process of applying moral value to health issues that are typically characterised by a global level effect or require action coordinated at a global level'.[193]

Globalisation is vital for cultural uniformity and restructuring and seeks, innocuously perhaps, to eradicate cultural diversity in the world.[194] In the opinion of Yankuzo the cultural variations between ethnic divisions in Africa have been

---

[188] Ibid at 23.

[189] JH Thrall 'Globalization of Health Care' (2008) 247 (1) *Radiology* 3–7.

[190] J Prah Ruger 'Good medical ethics, justice and provincial globalism' (2015) 41 *Journal of Medical Ethics* at 103–106.

[191] See K Lee & J Collin *Global change and health* (2005).

[192] S Benetar, AS Daar & P Singer 'Global health ethics: the rationale for mutual caring' in S Benatar & G Brock (eds.) *Global health and global health ethics* (2011) at 129–40.

[193] G Stapleton, P Schroder-Back, U Laaser, A Meershoek and D Popa 'Global health ethics: An introduction to prominent theories and relevant topics' (2014) 13 (7) *Global Health Action*.

[194] KI Yankuzo 'Impact of globalization on the Traditional African Cultures' (2014) 4 *International Letters of Social and Humanistic Sciences* at 7.

weakened by forces of globalisation and at particular risk are African traditional cultural values as they are being replaced by 'global cultural values'.[195]

Nevertheless, various authors have contradictory perspectives on the benefits of globalisation and much has been written on its impact on the world both positively and negatively. Whichever approach is adopted, the reality is that globalisation is a multi-dimensional process, the impact of which is that cultural, economic and political relations are being dramatically transformed on a global basis. Yankuzo likens it to '... an uncontrollable wildfire … it has started and nobody knows where it is taking us'. Moreover, Yankuzo reflects on how 'the world is being compressed into a single space now referred to as a global village'.[196] He states '[g]lobalization is a reality for all of us because; we are forced with no other option but to live in a global village.' [197]

The trend suggests a movement from that of a 'tribal village' to a 'global village'.[198] Countries at differing stages of development are being forced to impose an ever-expanding interconnection of socio-cultural related issues and policies in the management of their national affairs. Consequently, states are losing their governing capacity and sovereignty in a world that is gradually becoming borderless, and they are being coerced into assuming universal global cultures and policies. Ip suggests that global processes are stretching and transforming national law significantly, causing the lines demarcating global and national law to become increasingly blurred.[199]

The value of globalisation lies in its ability to inform essential information policy issues. In leveraging off of lessons learned elsewhere in the world, growth can be facilitated, as expansion is accelerated into Africa. The application of international law has been intentionally directed away from the national and domestic concerns of sovereign states, as it is regarded as their exclusive preoccupation and dominion.[200]

---

[195] Ibid at 1.

[196] Ibid.

[197] Ibid at 3.

[198] A Brysk *From tribal village to global village: Indian rights and international relations in Latin America* (2000).

[199] E Ip 'Globalization and the future of the law of the sovereign state' (2010) 8 (3) *Oxford University Press and New York University School of Law* at 636–655.

[200] Ibid.

Although the scope of electronic transactions and the newly forged perception of 'global health' is clearly international in nature, where substantial overlap will inevitably occur, the onus still remains on the national legislation enacted by the sovereign state to provide the bulk of legal and regulatory reform, control and management.

Despite the best efforts of the realms of international and national law to remain detached from each other, the absolute juridical sovereignty of a state's autonomy in creating its own national law is slowly being eroded.[201] A steady but progressive transnationalisation of international law is gaining momentum.[202] Globalisation has had an enormous impact on the sovereign state and is the greatest perceived threat. Khrebtukova states:

> '[i]n a globally integrated world, national borders no longer confine the diverse views that prioritize subjects of international law… it is imperative that these regimes themselves be made to take account of one another, to understand one another, and to go about their respective decision-making processes in a way that places them within the scheme of one cohesive international legal system.'[203]

A global regulatory approach prevents the opportunity for regulatory arbitrage, which enables individuals to arrange and structure their communications and transactions so as to evade more restrictive national regulations in favour of the advantages offered by less stringent foreign regulatory regimes.[204]

The dynamic between national, international, transnational and global institutions is 'complicated and interwoven'.[205] International law has evolved over time into a framework to accommodate the emergence of global governance. Transnational processes have created a new legal model, that of 'global law'.[206]

---

[201] Ibid.

[202] Ibid at 637.

[203] A Khrebtukova 'A call to freedom: Towards a philosophy of international law in an era of fragmentation' (2008) 4 (1) *Journal of International Law and International Relations* 51–103 at 101.

[204] AM Froomkin (n 8) at 127.

[205] Ip (n 199) at 637.

[206] P Le Goff 'Global law: A legal phenomenon emerging from the process of globalization' (2007) 14 *International Journal of Global Legal Studies* at 119, 121–126.

Rather than the fragmentation prevalent in international law,[207] global law is not a formalised legal system but represents a 'multi-cultural, multi-national, and multi-disciplinary' system.[208]

(3) The introduction of centres of excellence

A centre of excellence can be described as a network of participating countries, which target local or regional health challenges. The expectation is that participating countries within a regional network will provide specialised medical services in one particular discipline. Each centre of excellence is committed to referring patients for treatment to the various partner countries, and to share experiences, protocols and management policies with one another.[209] The intention is to engage in regional cooperation in various areas of medical specialties, thereby strengthening health care systems at a national and regional level. The regional networks of excellence have as their primary objective the efficient and rapid response to regional diseases and threats through synergy, co-operation and multi-disciplinary collaboration.[210]

The Republic of Rwanda, reputed to be the technology hub in East Africa, has recently been appointed as the region's centre of excellence in eHealth, biomedical engineering and immunisation procurement, supply and maintenance. Within the East

---

[207] M Koskenniemi 'Global Governance and Public International Law' (2004) 37 *Kritische Justiz* at 241, 242–245.

[208] Le Goff (206) at 127–128.

[209] In 2009, the African Network of Medical Excellence was launched. The aim was to promote the construction of medical centres of excellence on the African continent. The participating countries are to establish centres of excellence in a medical discipline of their choice.

[210] See GM Miiro, OOM Oukem-Boyer, O Sarr, M Rahmani, F Ntoumi, K Dheda, A Pym, S Mboup and P Kaleebu 'EDCTP regional networks of excellence: Initial merits for planned clinical trials in Africa' (2013) 13 *BMC Public Health* at 258. Further examples of networks are the EACCR, comprising 34 East African regional institutions including Kenya, Tanzania, Uganda, Sudan and Ethiopia. The TESA network, which includes 10 institutions across 6 Southern African countries including Botswana, Malawi, Mozambique, South Africa, Zambia and Zimbabwe. The West African network of excellence WANETAM for research into Tuberculosis, HIV/AIDS and Malaria located in Senegal and CANTAM the Central African Network for Tuberculosis, HIV/AIDS and Malaria, in Brazzaville, Republic of Congo. Each network has a governance structure and is multi-disciplinary, and multi-disease-oriented for the furtherance of research coordination and resource sharing across Anglophone, Lusophone and Francophone countries in Africa. See too S Nwaka *et al.* 'Analysis of pan-African centres of excellence in health innovation highlights opportunities and challenges for local innovation and financing in the continent' (2012) 12 *BMC International Health and Human Rights* at 11.

African region, Uganda has been selected as the centre of excellence in treating cancer, Kenya with issues of urology, Tanzania with the service of cardiac issues and Burundi has been charged with nutritional issues.

In establishing these centres of excellence, eHealth systems are transcending national boundaries and becoming transnational.[211] Encouraging patients to utilise these facilities requires them to be tracked and treated within and between regions. Transnational platforms for collaboration in eHealth systems require continent wide and global eHealth debates, defining the challenges in cross-border eHealth and health care delivery systems. The argument in favour of the development of an overarching legal and regulatory framework addressing eHealth challenges, particularly the unrestricted movement, safekeeping and security of data across national borders, becomes compelling.

IV CONCLUSION

This chapter considered certain drivers in an online health environment. These included the establishment of centres of excellence, the emergence of global health care, the changing doctor-patient relationship, and the influence of all of these on online eHealth data protection. The chapter examined whether there exist any boundaries in cyberspace; whether privacy is of concern to online users; whether privacy is of concern to eHealth users in developing countries and whether data protection is a luxury that the developing world can ill afford.

The chapter indicated that states no longer exercise the exclusive domain of being the sole legislators and enforcers of laws, and that this duty is now shared among states, as transnational law alters international law and its governance, which in turn ripples down to affect law at a national level. As the application and enforcement of national law cannot extend beyond its borders, a law is required that is effective across boundaries and jurisdictions.[212] This is primarily a reactionary response to the nature of data and its inherent ability to flow freely across boundaries.

---

[211] T Gerber, V Olazabal, K Brown and A Pablos-Mendez 'An Agenda for Action on Global E-Health' (2010) 29 (2) *Health Affairs* at 233–236.

[212] Ip (n 199) at 637.

Additionally, the chapter described that the decentralised and ubiquitous global Internet network, together with the flexibility and mobility of treatment and services offered by eHealth initiatives, allows for a seemingly effortless transcendence of borders and jurisdictions, all of which require the application of regulation at a regional, international or global level.

The following chapter will consider the solutions to the privacy dilemma within electronic health care in the developing world. It will describe data protection regulatory measures and the factors that inform them, and it will assess the Malabo Convention as an option for solving the predicament faced by data protection eHealth in Africa.

CHAPTER 7: DATA PROTECTION MEASURES AND CRITICISMS OF THE MALABO CONVENTION

Without privacy there was no point in being an individual.

Jonathan Franzen

I INTRODUCTION

This chapter explores options that may assist in finding a solution to the privacy dilemma in the field of electronic health care in the developing world. The purpose of this chapter is three-fold: Firstly, it sets out to describe international data protection and the questions confronting data protection regulators. Secondly, it introduces and assesses alternative protective regulatory methods to those more usually applied to information policymaking. These alternative, or extended, models may prove useful in informing a comprehensive, albeit layered, approach to a solution. Thirdly, in the concluding part of this chapter, I assess the Malabo Convention.[1] This convention is the obvious choice when seeking assistance in unravelling the dilemma of eHealth data protection in Africa, most particularly because it already exists, and has been well received by various sectors.[2] Moreover, it affords a degree of protection under human rights law, which until now has been unprecedented outside of the European Union and thus is something of a triumph for the African continent. While acknowledging this achievement, I set out certain shortcomings in the Convention.

My goal is not to identify all the inconsistencies contained in the Malabo Convention. Rather I propose that, although the Convention is a welcome start, for it to be useful in providing a solution, review and reform are necessary. The details of such amendments I discuss in the following chapter (Chapter 8).

II THE FUTURE OF DATA PROTECTION

The development of data protection internationally and the questions facing regulators are considered in an attempt to drive data protection forward.

(1) Development of international data protection

The stated mission of Google, for instance, is to 'organize the world's information and make it universally accessible and useful'.[3] The power to access and manipulate

[1] The Malabo Convention is discussed in Chapter 4.

[2] G Greenleaf and M Georges 'The African Union's data privacy Convention: A major step toward global consistency?' (2014) 131 *Privacy Laws and Business International Report* at 18.

[3] See 'About Google'. Available at http://www.google.com/about/ (accessed 20 February 2017).

data is enormous.[4] Of late, there has been unprecedented activity around the development of data protection regulation worldwide.[5] More recently, scripted constitutions, such as the South African and the Hungarian, include explicit rights to access and control personal information.[6] Where privacy and data protection is not specifically recognised by the constitution, such as in the US, Ireland and India, courts have found the right to privacy in other provisions and in international agreements, such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights, which were adopted into law.[7]

In the 1970s, a general movement emerged with the intention of wider privacy protection, and with the adoption of comprehensive privacy laws primarily setting the framework for protection.[8] The genesis of modern data protection laws can be traced to those originally enacted in a separate legal instrument in the German federal state of Hesse in October 1970.[9] This was followed by a wave of regulatory legislation, largely based on the models introduced by the OECD and the Council of Europe, including legislation found in Sweden,[10] Germany[11] and France.[12] The incidence of

---

[4] See B van der Sloot & F J Zuiderveen Borgesius 'Google and Personal Data Protection' in A Lopez-Tarruella (ed) *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*. Series: Information Technology and Law Series vol 22 VIII (2012) 75–111.

[5] See G Greenleaf 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (2013) *Journal of Law, Information & Science* at 1. D Banisar and S Davies 'Global Trends in Privacy Protection: An international survey of privacy, data protection, and surveillance laws and development' (2012) 18 (1) *John Marshall Journal of Computer & Information Law* and D Banisar and S Davies 'Privacy and Human Rights**:** An International Survey of Privacy Laws and Practice' *Global Internet Liberty Campaign*.

[6] Ibid at 3.

[7] Ibid.

[8] Ibid.

[9] *Hessisches Datenschutzgesetz* (or The Data Protection Act of Hersse) of 1970. This was the first legal instrument bearing the name of '*Datenschutz*', which was later translated into English as 'data protection'. The etymological origin of 'data', observed in the plural form of the Latin word 'datum', echoes the English interpretation of the word data as being 'in general any given piece of information', much like the French word '*donnée(s)*' or the Dutch word '*gegeven(s)*'. This is strictly speaking not consistent with the German term '*Daten*', which is not understood to refer to any data but specifically only to data that has been processed by computers. See G González Fuster *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (2014) at 56 and 57, and also FW Hondius *Emerging Data Protection in Europe* (1975) at 84.

[10] (Swedish) Data Act of 1973, subsequently repealed by the Personal Data Act of 1998 and the supplementary regulations contained in the Personal Data Ordinance of 1998.

enactments slowed down in 1981, with the adoption of the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[13] and the OECD's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.[14] By early 2014, as reported in Greenleaf, 101 countries across the world had data protection laws.[15]

This has had a profound impact on the way in which global businesses are required to approach the collection, dissemination and management of personal information, and it has encouraged topical debates around the right of people to be forgotten, the right of data to be deleted, and the right to data portability. Moreover, new developments in medical research and care, and health data transfers, have dramatically increased the level of information generated.[16] Consequently, existing paradigms of privacy and data protection have shifted and are undergoing scrutiny, with a global response aimed at reviewing and redesigning data privacy laws.[17]

Specific law reform proposals and recommendations are emerging, or are in the process of being implemented, by for instance, the Australian Government, which enacted the Privacy Act of 1988 (which seeks to regulate the handling of personal information about individuals), the Information Privacy Act of 2014 and the Personally Controlled Electronic Health Records Act of 2012 (which create the legislative framework for the Australian Government's personally controlled electronic health record system),[18] the EU Regulation [19] and the Consumer Privacy

---

[11] The *Gesetz gegen missbrauchliche Datennutzung* (Act Against the Misuse of Data) adopted in January 1974.

[12] *Loi no 78–17 du 6 janvier 1978 relative á l'informatique, aux fichiers et aux libertés* (Law on Computers, Files and Freedoms of 6 January 1978).

[13] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS no. 108 Strasbourg 1981.

[14] OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data Paris (1981).

[15] With the 101st country with data protection legislation that of South Africa. See Greenleaf (n 5) at 28.

[16] Banisar and Davies (n 5) at 4.

[17] G Gunasekara 'Paddling in unison or just paddling? International trends in reforming information privacy law' (2014) 22 (2) *International Journal of Law and Information Technology* at 141.

[18] For a critical summary, see N Waters and G Greenleaf 'Australia's 2012 Privacy Act revisions: Weaker Principles, More Powers' (2012) 121 *Privacy Laws & Business International Report* at 12. See for an update to the Australian Privacy Principle guidelines issued by the Office of the Australian

Bill of Rights proposed in 2012 by the Obama Administration in the US.[20] Outside of Europe, the 1993 Privacy Act of New Zealand is considered to be one of the most comprehensive privacy acts.[21] In the Asia Pacific region, Japan, Hong Kong, South Korea and Taiwan have also adopted data protection measures, while Singapore,[22] Vietnam and Indonesia have privacy legislation applicable to certain sectors.[23] In the People's Republic of China, great strides have been made in the new focus of a judicial interpretation issued in The People's Republic of China's Supreme People's Court, which became effective on 10 October 2014 with regard to the infringement of privacy rights on the Internet.[24] As China has no comprehensive data protection law, with limited data protection and privacy regulation in terms of sector-specific laws, this judicial interpretation is a significant development in data privacy regulation.[25] Generally, the interpretation serves to prohibit Internet users and Internet service providers from disclosing or publishing personal information on the Internet (or other

---

Information Commissioner http://www.oaic.gov.au/privacy/privacy-act/other-legislation (accessed 20 February 2017).

[19] European Commission 'Proposal for a Regulation 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 (General Data Protection Regulation)' Brussels 25.1.2012 COM (2012) 11 final 2012/0011 (COD).

[20] The White House 'Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy' (Washington, February 2012). Additionally, the US HIPAA has the federal Health Insurance Portability and Accountability Act of 1996.

[21] S Avancha, A Baxi and D Kotz 'Privacy in mobile technology for personal healthcare' (2012) 45 (1) 3 *ACM Computing Surveys* at 3.10.

[22] Health data protection is provided by the Computer Misuse Act, the common law and codes of practice.

[23] Avancha *et al.* (n 21) at 3.10.

[24] The interpretation is entitled 'Provisions of the Supreme People's Court on Several Issues concerning the Application of the Rules regarding Cases of the Infringement of Personal Rights over Information Networks' and clarifies the December 2012 position of the Standing Committee of the National People's Congress on Strengthening Network Protection. See in this regard 'Chinese Supreme People's Court Issues Interpretations Regarding the Publication of Personal Information on the Internet' *Privacy and Information Security Law Blog.* Available at https://www.huntonprivacyblog.com/2014/10/articles/chinese-supreme-peoples-court-issues-interpretations-regarding-publication-personal-information-Internet/ (accessed 20 February 2017).

[25] Banisar and Davies (n 5) at 31–34. This firewall serves to block certain western news web sites including the BBC, New York Times and the Voice of America.

information networks). [26] The personal information protected by this prohibition includes, *personal genetic information, medical records, health examination materials*, home addresses and information regarding private activities.

Unfortunately, although they may find general application, few data protection laws address eHealth issues directly. Most privacy laws contain broad data protection provisions, which may find general application to eHealth issues. Alternatively, eHealth privacy protection may be provided for more generally within wider health care legislation.[27]

The enactment of countries' own specific data protection laws has been influenced by and developed in parallel with collective, multinational instruments.[28] Of interest is that eHealth regulations frequently do not originate in public or private international law concerning eHealth but that they rather have their roots in traditional international law-making entities, such as non-governmental organisations. In developing new technologies, such as eHealth, reliance is increasingly placed on general policies and operating procedures developed by participating groups that have a firm grasp of the technology.[29] Despite these policies and standards being self-serving, they do provide a basis and assistance to the likes of the WTO and the United Nations in crafting legal policies in areas of technology.[30]

---

[26] My emphasis. Disclosure or publication on the Internet (or other information network) may, however, be permissible under the following circumstances: where the relevant individual consented in writing; the disclosure or publication is in the public interest to a necessary extent; an educational or scientific entity makes the disclosure or publication for purposes in the public interest, academic research or statistical analysis, the relevant individuals have consented in writing to the publication or disclosure and the method of disclosure or publication will not result in the identification of any individual; the relevant personal information has already been published by the individual on the Internet, or has already become public via other means; or the personal information is obtained through legitimate methods.

[27] For instance, the US HIPAA or Health Insurance Portability and Accountability Act of 1996. See too Avancha *et al.* (n 21) at 3.8.

[28] FH Cate 'The EU Data Protection Directive, Information Privacy, and the Public Interest' (1994–95) 80 *Iowa Law Review* at 431.

[29] JD Blum 'The role of law in Global e-health: A tool for development and equity in a digitally divided world' (2002) *Saint Louis University Law Journal* at 86.

[30] Ibid. For example, the WTO and the United Nations are both working with a private organization, the Global Information Infrastructure Commission (GIIC), to facilitate the development of policies underpinning telecommunications based commerce.

Of all the legal challenges affecting the global eHealth arena, the one inciting the most widespread reaction on the part of policymakers worldwide is that of privacy.[31] Like other areas of eHealth, feasible privacy policies will require universal global and regional agreements to develop a common set of international practical and workable principles and objectives.[32]

(2) Questions facing regulators

The five key challenges confronting policymakers are as follows: Can existing laws be applied successfully to new activities or are entirely new laws required to address data protection developments adequately? Secondly, what are 'reasonable' and 'proportionate' responses when legal reformation is necessary to accommodate societal objectives in a new context? Thirdly, how do regulators craft new laws that are flexible to changing circumstances? Fourthly, how are fundamental human values protected in practice, notwithstanding social and technological pressures? And, lastly, how is policymaking, on a broader scale, coordinated between nations so that a consistent global legal environment is fostered?[33]

These questions pose challenges to regulators that require their resolution within a given set of circumstances. In an attempt to answer these questions, firstly, policymakers must determine whether in fact to regulate at all, and if so, what specific kind of regulation is appropriate. If regulation is indeed necessary, then regulators have a choice not only between the existing law and the creation of new law, but also between 'multiple existing regulatory forms'.[34] In relation to the first three questions, Samuelson provides the following insight. She states that, where the creation of new law is desirable, the challenge for regulators is to adopt a 'reasonably proportionate response' to the problem. The proposal by Samuelson is that regulation should be 'predictable, minimalist, consistent, and simple', thus avoiding disproportionate laws

---

[31] Ibid at100.

[32] Ibid at 86.

[33] P Samuelson 'Five Challenges for Regulating the Global Information Society' at 2. Available at SSRN: https://ssrn.com/abstract=234743 or http://dx.doi.org/10.2139/ssrn.234743 (accessed 20 February 2017). And P Samuelson 'A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy' (1999) 87 *Calif Law Review* at 751.

[34] Ibid.

that create 'more problems than they can solve'.[35] A further reason to enact such legislation is that they should be more 'flexible and adaptable than those that are more complex and ambitious'.[36] In an endeavour to cast as broad a net as possible, Samuelson suggests that legislation implemented should be as 'technology-neutral' as possible, that is, it should not endorse any particular technological approach.[37]

The fourth challenge facing regulators is to incorporate the claim to the universal human right of privacy within data protection laws. How are such values integrated into new law? Are human rights instruments too general a method of protection to provide an adequate response? Lord Hoffmann argues that 'human rights are universal in abstraction but national in application'.[38] Whereas at a level of abstraction, human rights may be considered universal, at the level of application, the detail required in addressing concrete human rights difficulties necessitates a national approach. The application of human rights, it is suggested by Lord Hoffmann, requires 'trade-offs and compromises, exercises of judgment, which can be made only in the context of a given society and its legal system'.[39] The fact that a country has subscribed to a statement of human rights in the same terms as contained in a human rights instrument does not automatically mean that it has agreed to uniformity in the *application* of those abstract rights in its country.[40] Although not wishing to minimise the importance of aspirational international statements of abstract human rights, such as the Universal Declaration, Lord Hoffmann concedes that human rights instruments provide a 'recognised standard against which governments may be criticised and are effectively criticised by other governments and international organisations'.[41]

Although he applauds the use of human rights instruments as a benchmark for compliance with human rights by subscribing countries, he criticises human rights judicial bodies. The difficulty, he suggests, is in enabling a foreign court, for instance

---

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] L Hoffmann 'The Universality of Human Rights' (2009) *Judicial Studies Board Annual Lecture* at 1.

[39] Ibid at para 24.

[40] Ibid. Lord Hoffman states '[t]he situation is quite different from that of the European Economic Community, in which the Member States agreed that it was in their economic interest to have uniform laws on particular matters which were specified as being within European competence'.

[41] Ibid at para 40.

the European Court of Human Rights, to 'intervene in the details and nuances of the domestic laws' of countries.[42] With regard to domestic human rights law, caution should be exercised in relying merely on rights provisions, as this may 'blind us when envisioning a more balanced picture of the privacy strands at stake'.[43] Perritt too notes the blurring effect that technology may have on human rights law.[44] International instruments, including human rights instruments, remain helpful within the data protection discourse, and a valuable contribution to attaining a solid basis of domestic data protection law.

III ALTERNATIVE OR EXTENDED REGULATORY PROTECTION MEASURES

I shall now consider three extended or additional measures of controlling behaviour and protecting data that may run concurrently with more traditional forms of information regulation. These approaches may provide a partial solution or, when used together with more formalised governance measures, may assist in strengthening traditional regulatory models.

(1) Global legal pluralism

'Legal pluralism' is the presence of more than one legal order in a social field. It is defined in Griffith as '…the coexistence of legal orders in the same space, and quite independent from … formal recognition by state law'.[45] With the advent of globalisation, the opportunity for legal pluralism, or the 'intermingling of normative legal systems with global legal systems', has become noticeable. The challenges and themes imposed by globalisation – the definition of law, the role of the state, the role of the community, and that of space – are expanded in the global sphere. Pluralism in

---

[42] Ibid at para 44.

[43] V Mayer-Schönberger 'Strands of Privacy: DNA databases and informational privacy and the OECD Guidelines' in *DNA and the Criminal Justice System: The Technology of Justice* (2004) at 225–246.

[44] HH Perritt 'The Internet is Changing International Law' (1998) 73 *Chicago-Kent Law Review* at 997.

[45] See J Griffiths 'What is Legal Pluralism?' (1986) 24 *Journal of Legal Pluralism and Unofficial La*w at 1. See R Michaels 'Global legal pluralism' Duke Law School Public Law & Legal Theory Research Paper No. 259 (2009) 5 *Annual Review of Law & Social Science* at 3.

society radicalises issues of rights and sovereignty. While the concepts of local, national, and international are fluid,[46] legal pluralism accepts the concurrent co-existence of several divergent legal orders within one social space.[47] It seeks to reconcile a hybrid legal position, where various normative legal systems occupy a single social field.[48] As such, Cover puts pluralism as being 'a bridge in normative space' connecting 'the world that is … with worlds-that-might-be'.[49] He continues that the law '… *is* the bridge – the committed social behaviour, which constitutes the way a group of people will attempt to get from here to there'.[50]

For some legal pluralism theorists, global legal pluralism represents more than classical pluralism and new legal pluralism.[51] An emerging global legal pluralism has arisen that transcends traditional legal boundaries. It focuses beyond the individual localised state or community toward an international sphere: a paradigm that entails inter-legality and a shift from national to regional and/or global legal orders.[52] Teubner cites the *lex mercatoria*, or the transactional law of economic transactions, as a successful example of an autonomous legal system: a global law without a state.[53]

---

[46] S Benhabib *Another Cosmopolitanism* (2008) at 74.

[47] E Ip 'Globalization and the future of the law of the sovereign state' (2010) 8 (3) *Oxford University Press and New York University School of Law* at 640.

[48] PS Berman 'The New Legal Pluralism' (2009) 5 *Annual Review of Law and Social Science* at 226.

[49] RM Cover 'The Folktales of Justice: Tales of Jurisdiction' (1985) *Yale Law School Legal Scholarship Repository*: *Faculty Scholarship Series Paper 2706* at 181.

[50] Ibid.

[51] Whereas the classical phase relates to only the interplay of Western and non-Western laws in colonial and postcolonial settings, while treating the indigenous non-state law as subordinate to that of the law of the colonising state, the new legal pluralism extends the concept to Western societies and the interplay between official and unofficial law more generally. See further SE Merry 'International law and socio-legal scholarship: toward a spatial global legal pluralism' (2008) 41 *Studies in Law, Politics and Society* at 156 and 157; F von Benda-Beckmann 'Who's afraid of legal pluralism?' (2002) 34 (47) *The Journal of Legal Pluralism and unofficial law* 37–82 and Michaels (n 45) at 2 for his clarification of the value and limitations of legal pluralism.

[52] See Merry (n 51) at 156 and Berman (n 48) at 226.

[53] See G Teubner 'Global Bukowina: Legal pluralism in the world society' in G Teubner (ed) *Global Law without a State* Brookfield: Dartmouth (1997) at 3–28 for a discussion on the *lex mercatoria.* See P Zumbansen 'Piercing the legal veil: Commercial Arbitration and Transactional Law' (2002) 8 *European Law Journal* at 400 and KP Berger 'The Law Merchant and the New Market Place: 21st Century view of transnational commercial law' (2000) *International Arbitration Law Review* at 91 for a theoretical discussion on the *lex mercatoria.* See also GP Calliess 'Reflexive Transnational Law: The privatization of civil law and the Civilisation of private law (2002) 23 *Zeitschrift für Rechtssoziologie*

How to define what the law is and the manner in which it is distinguishable from other normative systems and modes of governance is not as simplistic as arguing that multiple legal forms exist side by side. Questions arise: How do these legal forms exercise power and authority? What is their connection to each other? How do they express local normative standards and regulate social interactions?[54] As described in Merry, 'international regulations, agreements, human rights conventions, and other forms of law are increasingly merging with domestic law'. She states that '[i]t is no longer possible to study domestic law in isolation from these influences'.[55] A stable system of law coupled only to a particular national law is 'no longer adequate'. It is the fluidity and plurality of law found particularly in international law that provides the answer to the ordering and grounding required in regulating a highly mobile and fragmented set of social relationships.[56] Sloss likewise states that, as nations become increasingly interdependent, greater reliance is sought of international instruments to regulate matters previously considered domestic in nature,[57] as does the view of Berman, who suggests that legal pluralism may provide a valuable alternative framework for addressing conflict of laws issues, which are unfolding in areas of, for instance, Internet jurisdiction.[58] As inter-systemic law-making has grown more complex, the use of legal pluralism as a solution in the global arena becomes viable.[59] Jurisdictional overlap, a predictability of the growth of informational communications technologies, along with the mobility of data across borders all indicate that jurisdictions will now feel the 'effects of activities around the globe, which will inevitably lead to multiple assertions of legal authority over the same act, without regard to territorial location'.[60]

---

at 185, where the nature and subsequent rise of transnational law within the modern territorial state is considered in greater detail.

[54] Merry (n 51) at 156.

[55] Ibid.

[56] Ibid.

[57] D Sloss 'Non-self-executing treaties: Exposing a constitutional fallacy' (2002) 36 (1) *UC Davis Law Review* at 3.

[58] Berman (n 48) at 225.

[59] Ibid. This is because it has 'always sought to identify hybrid legal spaces, where multiple normative systems occupied the same social field'.

[60] Ibid.

Legal pluralism is a product of social processes and a context for social interaction at a specific point in time and location.[61] The proposed shift in law is not from one system, the political, to another, the economic, but instead is 'an expansion toward numerous autonomous global functional subsystems of world society, with which different legal orders are coupled'.[62] Other forms of inchoate global law, which reinforce this view have been identified,[63] most significantly for this work, the *lex digitalis* (a self-administered law of the Internet). Siegal states that '[t]he technical advances in communication have underpinned the advance of globalization in all spheres of the economy, and health should be no exception'. [64] He proposes that 'the promise of IT-globalization has something to offer all parties involved: patients, providers, insurers, national health systems, and the international community'.

Likewise, Reidenberg argues that a 'set of rules for information flows imposed by technology and communication networks form a "*lex informatica*" that policymakers must understand, consciously recognize and encourage'.[65] He continues that the establishment of a *lex informatica* may provide 'a single, immutable norm for information flows on the network or may enable the customization and automation of information flow policies for specific circumstances that adopt a rule of flexibility.'[66]

He advocates that policymakers should look to the *lex informatica* as a solution and 'a useful extra-legal instrument that may be used to achieve objectives that otherwise challenge conventional laws and attempts by governments to regulate across jurisdictional lines.'[67]

Although heavily contested in the realm of traditional legal theory as nothing more than a 'quasi-legal phenomenon of soft law', existing merely in the shadows of the national legal regime, a 'third way' between market and state should not be

---

[61] Von Benda-Beckmann (n 51) at 72.

[62] Ibid.

[63] E.g., the *lex sportive* (an autonomous law of sport) and the *lex constructionis* (an autonomous law for construction projects).

[64] G Siegal 'Enabling Globalization of Health Care in the Information Technology Era: Telemedicine and the Medical World Wide Web' (2012) 17 (1) *Virginia Journal of law and technology* at 1.

[65] JR Reidenberg 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 (3) *Texas Law Review* at 555.

[66] Ibid.

[67] Ibid at 556.

immediately dismissed, a possible 'regulated self-regulation'.[68] Understandably, in developing any legal system, it is to be expected that particular local, social contexts and sensitivities may both be considered in a way possible by their national counterparts. Thus, sovereign national law will continue to find legitimacy and relevance.[69]

Certainly, implementation, enforcement measures and sanctions are immediately apparent as potential Achilles heels in the establishment of any legal system of this sort.[70] Unless political legitimation and effective enforcement are furnished by national courts, little prospect of legal traction is envisaged. Informal sanctions, as recognised in the *lex mercatoria* and applied by the market, are often insufficient mechanisms for redress. Consequently, the core of its legality risks being placed in dispute.

(2) Self-regulation

An alternative method of regulation is that of 'self-regulation'. In a self-regulatory system, the choice to comply with the guidance and direction of a code of conduct or set of industry principles, or not, is at the sole discretion of the respective industry member with little or no formal enforcement mechanisms beyond that of corporate peer pressure. Put concisely, 'self-regulation only works for those who agree to be self-regulated'.[71] Nevertheless, Goldman and Hudson view a self-regulatory approach as a 'useful stepping stone' to the introduction of legislation.[72]

Swire uses the interesting, albeit unusual, metaphor of 'elephants' and 'mice' to describe Internet legal regulation and enforcement. Curiously, 'elephants' are

---

[68] Or 'reflexive law', i.e. 'an action directed back at itself', e.g. 'thinking of thinking' or 'communicating about communication' or 'regulating self-regulation', see Calliess (n 53) at 189 and 190. Reflexive law is described '[l]ike self regulation it is a concept, which potentially fits all kinds of policies, from neoconservative subsidiarity, over neo-liberal spontaneous ordering in free markets, to neo-socialist or communitarian ideas of democratic self-government in small parts of society'.

[69] Ip (n 47) at 651.

[70] See V Karavas and G Teubner 'http://www.CompanyNameSucks.com: The horizontal effect of fundamental rights on 'private parties' within autonomous internet law' (2003) 4 (12) *European & International Law* at 1356.

[71] ME Boulding 'Perspective: Self-Regulation: Who Needs It?' (2000) 19 (6) *Health Affairs* at 132.

[72] J Goldman and Z Hudson 'Virtually exposed: Privacy and e-Health' (2000) 19 (6) *Health Affairs* at 144.

understood to be large, powerful organisations, which 'have a thick skin, but are impossible to hide'. Without exception, 'elephants' are subject to a country's jurisdiction and are, in all likelihood, compliant with any regulations in place. On the other hand, 'mice' are smaller, more mobile participants, for instance, pornography sites or copyright violators, which 'can reopen immediately after being kicked off of a server or can move offshore'. Mice, he goes on to suggest, 'breed annoyingly quickly – new sites can open at any time'. As traditional law enforcement over the Internet is difficult, Swire suggests that alternative legal enforcement agents be sought. These include 'the individual users, Internet service providers, the financial intermediaries that transfer money to the mice, and the offshore countries that provide the mice a cozy nest'.[73] Moreover, it fosters a more robust, participatory society, while a 'watched society is a conformist society'.[74] Likewise, Boulding asserts: '[w]hile self-regulatory systems may help policymakers to understand complex new areas or take on some of the government's burden of enforcing agreed standards of conduct, they cannot replace laws'.[75]

Certainly, an industry effort to self-regulate in the area of eHealth and privacy may convey a positive and powerful message to the user. It is a tacit acknowledgment that it is a problem worthy of addressing. It also illustrates and reinforces a willingness on the part of industry to act ethically and justly, and adopt a thoughtful approach to the given situation, despite a lack of legal enforcement or obligation to do so.[76]

Despite these benefits, the concern expressed by Clarke, is a valid one. He states that industry self-regulation 'has continually demonstrated itself to be inadequate, and only of value if it is instituted within a context'.[77] Although the influence of online users has gained momentum in the recent past, it is suggested by Clarke that it is 'premature to anticipate the present imbalance of power between

---

[73] PP Swire 'Of Elephants, Mice, And Privacy: International Choice of Law and the Internet' (1998) 32 (4) *The International Lawyer* at 993.

[74] See J Goldman "Health at the Heart of Files?" Brandeis Lecture delivered at the Massachusetts Health Data Consortium's Annual Meeting in September 2001.

[75] Boulding (n 71) at132.

[76] Goldman and Hudson (n 72) at 144.

[77] See R Clarke 'Internet privacy concerns confirm the case for intervention' (1999) 42 (2) *Communication of the ACM* at 64.

organizations and individuals will be overturned soon'. Therefore, some form of government intervention and regulation is still realistically necessary for adequate data protection.[78] Understandably, a concern may be that relying on a model of self-regulation is effectively to 'allow the fox to guard the henhouse'. Thus, a self-regulatory system should not prevent the development of new legislation but, in fact, should assist policymakers in creating a well-reasoned and practical one.[79]

Relying on a system of self-regulation, in an era of hyper-connectivity and distributed networks, although this may play a useful role in the short term, is deemed in the opinion of the European Data Protection Supervisor and as expressed in the EU-US Privacy Shield, an insufficient method to safeguard the rights and interests of individuals in the long term, or to wholly 'satisfy the needs of a globalised digital world where many countries are now equipped with data protection rules'. [80] Transformation of privacy regulation is more important than trying to create a faultless system.[81]

(3) Technological model

The 'technological model' uses private technological systems to provide data protection to the user. The approach is merely a tool empowering government and individuals to control the use and distribution of their data.

The European Commission, on evaluating various technologies in an online environment, stated that technological tools and technical platforms should not in themselves act as sufficient replacements to protect privacy.[82] For any tangible protection to be provided, technological tools should be applied within the context of a formalised legal framework of enforceable data protection rules, providing a minimum and non-negotiable level of privacy protection.[83] Failing such minimum levels of privacy protection, the position reverts to one of self-regulation. Legislation

---

[78] Ibid.

[79] Boulding (n 71) at 137.

[80] European Data Protection Supervisor Opinion on the EU-US Privacy Shield draft adequacy decision (May 2016) at 2.

[81] Ibid.

[82] See Chapter 3 of this thesis.

[83]Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS).

should obligate health software vendors to provide base level security mechanisms and precautions for safeguarding user information.

Realistically, users are unlikely to alter pre-configured privacy settings on their online technological platforms, and the 'default' position set by the software developers regarding the user's preferences will usually reflect the overall level of online privacy protection. These settings may not necessarily reflect a high level of privacy protection, even if they are subject to user modification. Internet software developers could implement technological tools that enhance rather than reduce levels of privacy protection.[84] Relying on the industry to set appropriate privacy standards and then to comply with them creates an obvious risk. While the utilisation of technology as an initial safeguard is viable, it does not provide a complete answer to privacy protection.[85] Given the sensitive nature of medical data, the need exists to provide specific and appropriate security safeguards, for instance, the encryption of user data and user authentication mechanisms to mitigate breaches in security.[86] Encryption methods may provide a degree of security and privacy protection for users; of itself, however, it is incomplete without a formalised governance framework.[87] Likewise, the safeguarding of privacy and data protection requires more than the implementation of a specific technical algorithm.

Moreover, where legislation calls for the rather vague requirement to adopt 'reasonable security standards', it is not immediately apparent as to what exactly this means or how one is to go about fulfilling such a legal obligation. It may then be prudent for industry itself to assist in setting and dictating security levels embedded in technology driven models, particularly as the threat imposed on data protection is evolving constantly and rapidly.[88]

---

[84] Ibid.

[85] T Sahama, L Simpson and B Lane 'Security and Privacy in eHealth: Is it possible?' (2013) *e-Health Networking, Applications & Services (Healthcom)* 247–253. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6720676&isnumber=6720623 (accessed 5 January 2017) who 'hypothesize that the major concerns regarding eHealth security and privacy cannot be overcome through the implementation of technology alone'.

[86] European Commission 'Green Paper on mHealth' (2014) at 8.

[87] Banisar and Davies (n 5) at 6 and S Pearson, Y Shen and M Mowbray 'A Privacy Manager for Cloud Computing' in *Cloud Computing* (2009) at 90–106.

[88] 'Patient Privacy in a Mobile World: A framework to address privacy law issues in mobile health' (2013) at 11.

A legal framework accommodating considerations of legislative constraints, together with technologically based protection measures, is valuable in acquiring data protection within an eHealth system that is both measurable and accountable.[89] However, for such initiatives to be productive requires 'a bold, forward looking legislative framework'.[90] Whether individual states can deliver this framework, depends largely on their commitment and willingness 'to listen to the pulse of the emerging global digital economy and to recognise the need for strong protection of privacy'.[91]

IV CRITICISMS OF THE MALABO CONVENTION

Of late, the Pan-African Parliament, the legislative body of the African Union,[92] has facilitated striking growth in the protection of human rights in Africa. It is an obvious choice of institution to initiate data protection reformation measures on the African continent. To this end, and in the first instance, the Malabo Convention is an attempt by the African Union to provide for the establishment of an appropriate normative framework for the protection of personal data, consistent with the African legal, cultural, economic and social environment.[93] It presents a welcomed human rights protection agenda that Greenleaf and Georges regard as 'potentially [the] most important development in Africa'.[94] The Convention positions Africa as the first region and continent outside of Europe to adopt a data protection convention as international law.[95]

---

[89] Sahama *et al.* (n 85) at 1.

[90] Banisar and Davies (n 5) at 6.

[91] Ibid.

[92] The Pan-African Parliament is one of the nine organs proposed in the 1991 Treaty Establishing the African Economic Community (Abuja Treaty). Its purpose, as set out in Article 17 of the AU Constitutive Act, is 'to ensure the full participation of African peoples in the development and economic integration of the continent'.

[93] Preamble to the Malabo Convention at 2. The Malabo Convention is discussed in Chapter 4 of this thesis. See also T Maluwa 'The Constitutive Act of the African Union and Institution-Building in Postcolonial Africa' (2003) 16 (1) *Leiden Journal of International Law* at 157–170.

[94] Greenleaf and Georges (n 2) at 18.

[95] Ibid.

The Malabo Convention is not without weaknesses, however. In its current form, it fails to address the provision of data protection on the African continent adequately. It is not sufficiently comprehensive and requires refinement and extension. Essentially, the critical issues are lack of enforcement and governance mechanisms, ineffectual data transference provisions, and the insufficiency in recognising obstacles pertaining specifically to the African continent, such as cultural sensitivities and issues of consent. These criticisms are discussed in turn below. In the following chapter, possible solutions to these difficulties are advanced.

(1) The Convention's alignment with sub-regional African frameworks is unclear and greater standardisation is necessary

The extent to which the Malabo Convention is aligned with the provisions contained in regional instruments in Africa, particularly those of the ECOWAS Supplementary Act and the SADC 'Data Protection Model Law' requires further investigation.[96] Greater consistency and harmonisation across the regions is much needed and would prevent regulatory fragmentation and discrepancies in development and implementation.

(2) Lack of an Afro-centric approach: Concepts like 'consent' and 'privacy' are not described with cultural and contextual sensitivity

The Convention fails to appreciate or integrate the notion of privacy prevalent within the rich tradition of indigenous African law and its contextual philosophy. Simply transposing and adopting regulatory approaches appropriate elsewhere in the world, may be unsuitable and impractical within an African context.[97]

As reported in a paper written by Gwagwa on lessons drawn during Conectas XIV International Human Rights Colloquium, 'African countries need to develop effective legislative, administrative, judicial and/or other measures to ensure the

[96] Greenleaf and Georges (n 2) at 18–21.

[97] In Chapter 3 of this thesis, the concept of 'privacy' is discussed from an African perspective.

protection of human rights in cyberspace', as the 'cyber discourse in the Global North … [is] often *far removed from Africa's realities*'.[98]

African legal systems comprise differing strata of laws from a variety of sources over time, which have been imposed upon one another, thus creating a complex manifestation of legal regimes shaped by strong cultural influences.[99] Determination of the legal reality within which each country in Africa is found is further guided by their Francophone, Anglophone, Hispanophone or Lusophone heritage. Difficulties arise when attempts are made to explain or transplant concepts and assumptions prevalent within one particular historical culture or system into others.[100] Many African countries have 'hybrid' legal systems formed by the interweaving of a number of distinct legal traditions, derived from their diverse origins. Indigenous, or African customary law, to the extent that it is possible to speak of a single 'African customary law', finds application in many African legal systems.[101] As described in Lévy-Bruhl, 'it is impossible that tribes from the savannah have the same legal rules of those from the tropical forest, and that those are all bound by the same law, which rules the life of people living on fishing or maritime commerce'.[102]

Mention of 'African customary law' is understood with reference to the 'different rules, having "legal" value, of different African populations, which are

---

[98] My emphasis. See A Gwagwa 'Internet Governance lessons Africa can learn from Brazil's success story'. Available at http://www.opennetafrica.org/?wpfb_dl=29 (accessed 20 February 2017). See also C Eberhard 'Towards an Intercultural legal theory: The dialogical challenge' (2001) 10 *Social and Legal Studies* 173 states: '[o]n the national levels, the illusions of the realization of the *État de Droit* or Rule of Law all over the world, through a transplantation of the western state model have been shattered. Even those who still believe that the western model is the answer acknowledge the need to take local traditions into consideration'.

[99] A Mancuso 'African Law in Action' (2014) 58 (1) *Journal of Africa Law* at 1. As identified by Mancuso, '[t]he ways in which the African state is evolving transform it into an extremely complex social (and consequently legal) field in which state and non-state, formal and informal, local and transnational relations interact, merge and confront each other in dynamic and even volatile combinations, making the legal framework even more complex, and where, in extreme cases, multiple, unofficial microstates existing within the same state can be born'.

[100] Ibid.

[101] AN Allott 'What is to be done with African customary law?' (1984) 28 (1–2) *Journal of African Law* at 57 states '... the customary laws could vary greatly as between themselves'.

[102] H Lévy-Bruhl 'Introduction à l'étude du droit coutumier Africain' [Introduction to the study of African customary law] (1956) 8 (1) *Revue Internationale de Droit Comparé* 67 at 68 and in Mancuso (n 99) at 1.

grouped because they share the same characteristics'.[103] These complex legal structures often antedate the establishment of colonial or modern states and vary between cultures.[104] Such traditional laws may be very different to those familiar to the western jurist. Mancuso states that 'social phenomena are undifferentiated, so that it is impossible (and probably useless) to separate that which is juridical from what is religious, supernatural or economic'.[105] The role played by indigenous law, as influenced by religious law (for instance, *Shariia* law) combined with traditional influences, yields African legal systems that are both diverse and distinctive.[106] Customary laws thus accommodate a case-dependent and selective application of rules. These are not predictive and determinative, and are often mutually contradictory.[107] Mancuso describes that 'most of the laws copied from the western model failed to adapt to African legal culture', largely because 'the western approach does not embrace the same values of the people in the area to which it has been transplanted'.[108] A resistance to 'westernisation' or 'modernisation' and a desire to protect cultural values is widespread in African countries.[109] Thus, the danger in the modernisation of African law, in an attempt to adopt western patterns, is that it may not amount to tangible, effective, long-term legal reform, but merely a means to

---

[103] Ibid.

[104] Von Benda-Beckmann (n 51) at 39.

[105] Mancuso (n 99) at 1.

[106] AN Allott 'Towards the unification of laws in Africa' (1965) 14 (2) *The International and Comparative Law Quarterly* at 368 for the types and varieties or differences in African legal systems. See '[a]nother important factor in the development of the customary laws was the possibility of appeal from the traditional courts to superior courts and authorities applying English, or at least western, legal principles. This was especially noteworthy in the West African territories of what are now Ghana, Nigeria and Cameroon. In these countries appeal lay in many customary law cases to the regular law-courts of the English type; and the West African law reports are full of cases where the superior courts, manned by English-style judges, have decided customary-law issues. These superior courts inevitably applied their own principles, both for ascertaining what the rules of customary law were, and for formulating those principles in legal English' in Allott (n 101) at 60.

[107] Ibid at 81–82, 84.

[108] Mancuso (n 99) at 1.

[109] E Grant 'Human rights, cultural diversity and customary law in South Africa' (2006) 50 *Journal of African* at 2.

present 'an outward image of a modern country and legal structure', while the legal reality evolves very differently within the country.[110]

As stated in a 2010 report prepared by the Policy Engagement Network for the International Development Research Centre, '[j]ust as security and privacy cannot be ignored, we equally cannot transplant security and privacy techniques from abroad that may not be adaptable, particularly as legal frameworks may be lacking'.[111] Before applying 'modern' or 'universal' standards to 'privacy', one should be cognisant of and sensitive to the cultural norms, customary values and historical context within the divergent groupings.

The concept of 'consent' within an African context is problematic, for instance. The Convention fails to address the difficulties of providing consent within an African context, and the issue of consent for eHealth data protection thus remains largely unresolved.[112] Consent is not explored in any detail, save to say it should be express, unequivocal, free, specific and informed. Unfortunately, the opportunity to develop and extend specific privacy-related concepts in a uniquely technological environment is not embraced in the Convention.

(3) Data mobility and transfer between member states is inadequately addressed

Save for where the data controller has obtained authorisation from the relevant national protection authority,[113] Article 14 (6)(a) provides that '... the data controller shall not transfer personal data to a non-Member State of the African Union unless such a State ensures *an adequate level of protection* of the privacy, freedoms and fundamental rights of persons whose data are being or are likely to be processed'.

---

[110] Mancuso (n 99) at 1. See also WMJ van Binsbergen 'Dutch anthropology of sub-Saharan African in the 1970s' (1982) 16 African Studies Centre Leiden, The Netherlands at 11 for the effects of 'modernisation', industrialisation and rural-urban migration on the social relationships within rural African communities.

[111] 'Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations' A report prepared by the Policy Engagement Network for the International Development Research Centre (2010) at 7.

[112] See the writing on the position in South Africa: CL Jack and M Mars 'Informed consent for telemedicine in South Africa: A survey of consent practices among healthcare professionals in Durban, KwaZulu-Natal' (2013) 6 (2) *South African Journal of Bioethics and Law* 55–59.

[113] Article 14 (6) (b) of the Malabo Convention.

What exactly constitutes an 'adequate' level of protection? The Convention is silent on this. The treatment of data export in Article 14 (6) is incomplete and inadequate. Co-operative agreements or arrangements between member states are not canvassed, thus little is done to encourage the safe and effective free flow of information across borders.

(4) Enforcement and execution of the Convention

The relationship between international and domestic law also requires consideration. Bradley describes two views of the relationship between international and domestic law: firstly the 'monist' view, which is that 'international and domestic law are part of the same legal order, ... and international law is supreme over domestic law'. This is contrasted with the 'dualist' view, which holds that 'international and domestic law are distinct, ... and the status of international law in the domestic system is determined by domestic law'.[114] A state can be described as having a 'monist' legal system in instances where the provisions of an international treaty are automatically converted into domestic law without the need for an act of parliament implementing such legislation. What is required in states with 'dualist' legal systems, however, is the implementation of legislation to convert obligations within the convention into national law.

A regional instrument, such as the Malabo Convention, resonates with international law norms, in that state practice determines what eventually become settled as norms, values and rules in international law, while simultaneously respecting the sovereign equality of states. In the case of the Malabo Convention, it is apparent that the drafters of the Convention did not intend to create a self-executing instrument. A 'self-executing treaty' is enforced directly into national law without enactment by domestic legislation, on the treaty becoming binding on the state in terms of the state's international law obligations. The Convention does not create such an agreement; instead, it offers a malleable template or guide for advancing legislation, which can be modified by member states to fit their national peculiarities. Any intention to create primary domestic law by the Convention drafters would be irrelevant, as the individual states' constitutional rules would determine whether a

[114] CA Bradley 'Breard, Our Dualist Constitution and the Internationalist Conception' (1999) 51 *Stanford Law Review* at 529 and 530.

particular provision of a ratified treaty creates primary domestic law or not; and treaty makers lack the power to alter those constitutional rules.[115]

Member states who accede to, and ratify, the Malabo Convention, however, commit to 'establishing a legal framework' based on its provisions. In terms of Article 36, the Convention can only come into force 30 days after the last of fifteen ratifications have been received by the Chairperson of the Commission of the AU from member states. As member countries are required to accede to and ratify the Convention and then provide a national legal framework based on its provisions, the Convention, like many international treaties, reflects an aspirational model.

However, as reported in Greenleaf and Georges, no accessions or ratifications appear to have occurred within the first three months of its adoption.[116] As at June 2016, the Status List published by the AU for the Malabo Convention, indicates that, of a total number of 54 member countries, only eight have signed the Convention and no ratifications or accessions have been forthcoming.[117] The slow response in accession and ratification of the Convention may be indicative of a lack of commitment of member states to this process.

Instruments of this nature and the obligations created therein may provide a useful catalyst for the evolution of legal frameworks. This being said, the Malabo Convention is not a model law and does not establish an explicit model legal framework of standard provisions, which African states can easily adopt in their entirety.[118] Thus, room for great disparity exists in the interpretation and implementation by the member states of the provisions. Moreover, the adoption and ratification of the Malabo Convention by African states may be ineffectual, unless individual states establish data protection laws that are sufficiently equivalent and consistent, thus facilitating regional standardisation and harmonisation in accordance

---

[115] Sloss (n 57) at 7 and SA Riesenfeld 'The Doctrine of Self-Executing Treaties and US v Postal: Win at Any Price' (1980) 74 *American Journal of International* Law at 892, 895–96.

[116] Greenleaf and Georges (n 2) at 18–21.

[117] Available at https://www.au.int/web/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf (accessed 20 February 2017).

[118] UJ Orji 'Examining Missing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection' (2014) (5) *CRi* 129 at 132.

with the directives contained within the Convention.[119] The opportunity exists for certain states to enact legislation of a lower standard than others do, thus allowing states too much room for policymaking manoeuvres.

(5) Failure to create a regional data protection authority

The Malabo Convention compels member states to establish an authority in charge of protecting personal data in the form of a national protection authority.[120] These national protection authorities are empowered in terms of the Convention and are responsible for the establishment of mechanisms for 'co-operation with the personal data protection authorities of third parties' and for 'participating in international negotiations on personal data protection'.[121]

Of concern is that no provision is made for the co-operation of national protection authorities between other member states or for the provision of a supervisory authority at a regional level. The absence of establishing a regional supervisory authority is also troublesome.

VI CONCLUSION

While it has been established that the challenges facing privacy protection in eHealth in Africa are numerous, many of these obstacles are inter-related. However, when taken together, these obstacles create a considerable impediment to the achievement of eHealth implementation and are a potential threat to individual rights to privacy.

Certain shortcomings are apparent within the Malabo Convention. I have discussed the following criticisms: the Convention's lack of synergy with sub-regional African data protection frameworks; the failure to adopt an Afro-centric approach; the failure of concepts, such as 'consent' and 'privacy' being described with cultural and contextual sensitivity; the inadequacy in addressing data mobility and data exchange between member states and internationally; the failure to provide enforcement mechanisms within the Convention, and lastly the failure to create a

[119] Ibid at 133. Orji advances a similar argument with regard to the Malabo Convention's cybersecurity provisions.

[120] Article 11(1) of the Malabo Convention.

[121] Article 12 (1), 12 (2) (m) and (n) of the Malabo Convention.

regional data protection authority. In the following chapter, I shall recommend how such insufficiencies in the Convention be corrected, what such a framework should address and the form it should take.

CHAPTER 8: RESOLUTIONS FOR THE REGULATION OF DATA PROTECTION IN EHEALTH IN AFRICA

When the rhythm of the drum beat changes, the dance movement must also change accordingly.

Ghanaian proverb

I INTRODUCTION

The central theme throughout this chapter is to advance a solution to the multitude of regulatory complexities arising where privacy legal frameworks lag behind the rapidly maturing health care technology initiatives, particularly in the developing world. An attempt to bring about a transformative response is made by offering recommendations, which assist in the realisation of the human right to privacy within eHealth.

In proposing a solution, there are three considerations: firstly, the privacy baseline criteria across various societies and cultures differ enormously; secondly, there is a consistent and rapid transformation by technology of the global environment, which creates something of a moving target;[1] and lastly, without user confidence and trust in data protection policies and measures, nascent eHealth initiatives can never gain any sort of viable traction or reach their full potential.[2]

The proposition contained in this chapter is twofold: firstly, I propose the adoption of multiple layers of regulatory measures around data protection, using a combination of more formal methods of regulation, together with various extended regulatory measures, such as self-regulation and technological approaches. Additionally, I propose that the foundation of data protection be a formal regional regulatory instrument that is fashioned within an African context. In Chapter 7, I question whether the existing Malabo Convention provides assistance in this regard, and found it lacking in many respects. Accordingly, my questions now are simply: Firstly, how can the Malabo Convention be improved and what should such a revised framework address? Secondly, I ask what form should such an instrument take?

II THE PROPOSAL

The proposed solution is to adopt a multi-layered approach to privacy protection and to introduce an amended regional data protection instrument.

---

[1] D Banisar and SG Davies 'Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments' (2012) 18 (1) *John Marshall Journal of Computer & Information Law* at 15.

[2] Ibid, where 'without adequate oversight and enforcement, the mere existence of a law may not provide individuals with adequate protection'.

(1) A multi-layered approach

Despite the proliferation of data protection regulatory measures of differing enforceability, the question is whether users are afforded the data privacy, which they deserve.[3] The indication is that, in reality, providing data protection is not easily achievable. Additionally, there is considerable commonality and duplication between the different legal disciplines and data protection measures and their implementation.

To attach significance to one protection model and exclude all others is to adopt an incomplete position, given that an online environment system comprises 'a rich and complex cross-coupling of elements'.[4] Any proposed system may be 'caught in a web of conflicting constraints' in which 'each small part of the system affects other parts of the whole system,' and 'changing [the state of a single element] ... will have effects that ripple throughout the system'.[5] The challenge is to address these ripples in an insightful way.

What should be borne in mind is the dual enquiry required in the analysis of privacy protection. The first is the *ex post* examination of existing regulatory methods and whether such regulation achieves satisfactory protection. We have established that existing regulatory measures offer only partial solutions. The second is the *ex ante* predicting or imagining of an ideal informational privacy framework, which balances the need for privacy against the practicalities within which the need for privacy protection exists. This is an attempt at using the existing framework and then extending it to an envisaged position. Thus, after an evaluation of the various options, one is called upon to contemplate what the ideal position would look like. A determination is made of which approach, or which combination of approaches, best serves data protection within the context.

Clearly, none of the data protection methods addresses all of the obstacles nor do they provide a holistic solution. Moreover, a tension between vagueness and practicality remains. Abstract notions of privacy and the human rights contained

---

[3] L Edwards 'Consumer Privacy, On-Line Business and the Internet: Looking for Privacy in all the Wrong Places' (2003) 11 (3) I*nternational Journal of Law and Information Technology* at 226–250.

[4] L Haynes, D Legge, L London, D McCoy, D Sanders and C Schuftan 'Will the struggle for health equity and social justice be best served by a Framework Convention on Global Health'?' (2013) 15 (1) *Health and Human Rights The President and Fellows of Harvard College* 111–116.

[5] S Kauffman *The origins of Order: Self-organization and Selection in Evolution* (1993) 173–206.

within, for instance, international human rights instruments exist side by side with the more practical provisions found in a technological approach, for instance, the provisions contained in 'privacy-by-design' and 'privacy-by-default' measures.[6] Nevertheless, both perspectives have merit and fulfil a function. Similarly, endorsing themes of global consistency and industry self-regulation are helpful and cannot be discredited. However, can these approaches be used on their own as the sole means of regulating the protection of data? I would suggest not. The solution lies in an attempt to bring together the various themes of global consistency, technological expediency and self-regulation with a formalised legal framework in a multi-layered approach. The solution lies in fusing all approaches together in a meaningful way. Thus, the utilisation of the best of the various methods in a coordinated and overlaid practice to data protection regulation is recommended.

Granted, establishing the optimal balance between data protection levels (and thus the safeguarding of privacy rights) and the promotion of innovative eHealth services (and thus the delivery of health care benefits, particularly to people in countries in dire need of health care) is not easily resolved. The range of possible incentives for compliance with data protection principles falls along a continuum. At the one end is the voluntary code, in which there is limited compulsion to develop, adopt or enforce. At the other, is the policy, existing within a comprehensive set of statutory obligations and liabilities? It is argued that a combination of legislation and self-regulation may provide the optimum solution. This offers the flexibility and low compliance of a self-regulatory system with the formalised legislative oversight and remedies. The solution is to make provision for comprehensive legislative, and self-regulatory, sectoral mechanisms that complement one other.

Moreover, for any regulatory solution to be effective, it has to be 'flexible, dynamic and, responsive and sensitive to changing circumstances'.[7] The complex and sensitive nature of the many facets of privacy and data protection necessitates a

---

[6] 'Privacy-by-design' means that data protection measures ought to be built into products and services from the time of their very inception, while 'privacy-by-default' indicates that any products or services should have the strictest privacy settings automatically as their default or norm.

[7] See C Bennett & C Raab *The Governance of Privacy: Policy instruments in Global perspective* (2006) at 184 for the distinction between co-regulation and enforced self-regulation. I Rowlands 'Understanding information policy: Concepts, frameworks and research tools' (1996) 22 (1) *Journal of Information Science* 13–25 at 15.

combined approach: the transcendence of legal pluralism and international agreements, the purposefulness of self-regulation, and the practicality of the technological method. Protection would entail the employment of multiple layers of protection of various types, whilst adjusting the strength, scope and suitability of the protective coverage and its appropriateness within a given framework. This would build on patterns and wider associations that have been previously established and tested. An overlaying of such models used in conjunction with the more formalised option discussed hereunder is envisaged.

(2) A regional data protection instrument

Greater regional integration within Africa and the establishment of a consolidated regional instrument, which forms a baseline standard of legal validity, protecting the intrinsic human right of privacy generally and protecting personal data processing more specifically, is advocated. Such an instrument should extend to the protection of eHealth data applications. The instrument ought to comprise clearly defined, non-negotiable, yet contextually and culturally sensitive data protection standards and principles, relevant specifically to health care delivery in an eHealth environment in the developing world, whilst still accepting and incorporating internationally agreed upon human rights norms.

Although the Malabo Convention achieves much as a regional data protection instrument, I have illustrated its inadequacies in a previous chapter. I am building on the good already attained, and I thus address only its most apparent deficiencies. I have selected specific issues that in my view ought to be amended. First, I consider what should be included within such a regulatory framework. I then explore the form this revised regulatory framework should take.

III WHAT SHOULD BE INCLUDED IN THE REGULATORY FRAMEWORK?

The regulatory framework requires greater alignment and integration with data protection measures within the African region. Additionally, an approach that is Afro-centric or culturally and contextually sensitive is called for. The notion of ‘consent’ requires further clarity and adaptation. Data mobility and its significance in enhancing

eHealth also require consideration and inclusion within an amended framework. Lastly, issues of enforcement and execution need to be addressed within the framework.

(1) Alignment with regional data protection measures and greater integration

Regional integration presupposes the agreement by states to co-operate through supranational or inter-governmental institutions for the purpose of improving their relationships and obtaining mutual benefit.[8] Problematically, the act of integration necessitates the willingness on the part of the individual states to relinquish a degree of sovereignty.[9] Certainly, achieving the harmonisation of laws is a tediously slow process. This process can be expedited by way of mutual cooperation. Integration and a collaborative approach to the adoption of unified policies on certain international issues is advantageous to both the individual states and to the region as a whole.[10] To this end, African states have expressed their commitment to a more united Africa by signing and, with a couple of exceptions, ratifying the Constitutive Act.[11] The African Union is a response to the challenges presented by globalisation and an attempt at regional integration. [12] It is an endeavour to resolve the historic quest for deeper African unity. The purpose of the African Union, in facilitating greater African integration and strengthening human rights, is predicated on principles that suggest novel approaches between the African member states.[13] The question is whether the African Union represents enough of a plausible effort in the management of

---

[8] TW Bennett & J Strug *Introduction to International Law* (2013) at 248.

[9] Ibid.

[10] In an attempt to pursue a path of greater integration, the AU in July 2016 launched a common electronic passport for all its 54 member states with the aim of facilitating free movement of persons, goods and services around the continent – 'in order to foster intra-Africa trade, integration and socio-economic development'. See the AU press release of July 2016.

[11] The Constitutive Act of the African Union can be found at http://www.ohchr.org/EN/Issues/Education/Training/Compilation/Pages/8ConstitutiveActoftheAfricanUnion(2000).aspx (accessed 20 February 2017).

[12] T Maluwa 'The Constitutive Act of the African Union and Institution-Building in Postcolonial Africa' (2003) 16 (1) *Leiden Journal of International Law* 157–170 at 157.

[13] Ibid.

globalisation and regional cooperation, in a manner similar to that reflected by the European Union.[14]

The harmonisation of national data protection laws in Africa is a recent phenomenon.[15] Similar efforts at economic and financial integration can be witnessed through policy harmonisation within the region. A justification for strengthening and standardising legal systems within Africa is to enhance the confidence of technical and software applications developers in the regulatory regimes within the region, thus encouraging investment and economic growth.[16] The unification of African laws is cited as a possible solution, and by certain authors as the only and most plausible one, to removing the developmental obstacles caused by the juridical differences amongst the various African territories.[17] Such transformation can give 'the countries joining the process of regional integration the opportunity to assert their interests in a stronger and more confident manner within the international arena'.[18]

Post and Johnson identify the need for a new fundamental organising of ideas around the role of law. They recognise the 'death of distance', that is, distance is becoming increasingly irrelevant or redundant in transactional arrangements, and report that technology initiates a 'spillover effect' across national boundaries or 'federal lines'.[19] Consequently, human interactions are increasingly unrelated to their physical constraints.[20] In reality, data protection regulation is among the few, relatively new, fields of law, which have been developed largely across national

---

[14] Ibid at 158.

[15] AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* at 81. See NJ Udombana 'A Harmony or a Cacophony? The Music of Integration in the African Union Treaty and the New Partnership for Africa's Development' (2002) 13 (1) *Indiana International & Comparative Law Review* at 185.

[16] See PS Mistry 'Africa's Record of Regional Co-operation and Integration' (2000) 99 (397) *African Affairs* at 553 on why regional integration is important in Africa.

[17] S Mancuso 'The New African Law: Beyond the difference between Common Law and Civil Law' (2008) 14 (1) *Annual survey of International & Comparative Law* at 40.

[18] Ibid.

[19] See DG Post and DR Johnson 'Chaos Prevailing on Every Continent: Towards a New Theory of Decentralized Decision-Making in Complex Systems' (1998) 73 *Chicago-Kent Law Review* at 1055 and further in AM Froomkin 'Empire strikes back' (1997–1998) 73 *Chicago-Kent Law Review* at 1101.

[20] Ibid.

borders.[21] This rapid and informal trans-border regulatory development prompted the creation of formal international instruments.[22] These instruments remain relevant in attempting to address the complexities of the contemporary processing environment.[23]

The following examples highlight the necessity for greater African integration. The introduction of cloud computing and location-based services demonstrates that the trans-border personal data flows model, as implemented, is incomplete and lacking in its ability to address the complexities arising from the cross-jurisdictional nature of the new technology. The need for a regionally coordinated approach is also apparent with the emergence of 'centres of excellence', where the establishment of proposed 'hubs' or 'cores' of ICT proficiency, or centres of medical expertise, are being created. Essentially, these centres of excellence may exist only in a few selected sub-regions and not in each individual country, although they are serviced by or supporting various countries within their sub-regions. This transference of skills, knowledge and procedures illustrates that the need for standardisation and harmonisation of trans-border policies and legal standards in privacy policies across countries within Africa is essential.

To reduce weaknesses in privacy protection, a recent solution has been for individual states to introduce inter-related integrated privacy provisions and instruments. Various means are used to achieve such integration. One method is to attenuate differences in national laws through policy harmonisation. Integration comprises two strands of thought: the replacement of domestic laws with common regional policies, and the coordination of such national policies.[24] However, initiating the incorporation of provisions into various regulatory instruments without broader cooperation creates opportunities for fragmentation, inconsistencies and contradiction

---

[21] P de Hert and V Papakonstantinou 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?' (2013) 9 (2) *I/S: A Journal of Law and Policy for the Information Society* at 272.

[22] Ibid.

[23] Ibid.

[24] Udombana (n 15) at 189. For more clarity on these terms, see J Li 'Privacy policies for health social networking sites' (2013) 20 (4) *Journal of the American Medical Informatics Association* 704–707.

between the various documents. Many such instruments already exist at a sub-regional level within Africa.[25]

Moreover, greater regional cooperation and policy integration will remove the potential for 'races to the bottom', that is, a desire for states to adopt the least restrictive laws and encourage the most economic activity, or alternatively, 'races to the top' where the most stringent rules become a 'baseline for applying pressure to get international adoption by others'.[26] Both of these scenarios are undesirable.

Thus, contemporary personal data processing issues require strengthened regional instruments, which can then filter down to effective data protection legislation at a national level.[27]A WHO report cites legal frameworks for eHealth as fundamental to the 'effective use of and patient trust in eHealth'.[28] These frameworks for data protection and security regarding the collection and use (and reuse) of patient data are understood to 'create legal clarity and certainty' in the medical relationship.[29] Caution should be exercised, however, as such frameworks 'must adapt to current needs in order to work efficiently and continue to evolve as their use by technology and society evolves'.[30]

A WHO report suggested that those working in health technologies within a specific community 'would be best positioned to understand specific regional or national clinical approaches, legal frameworks, and cultural approaches to health services delivery', while greater collaboration with international institutions[31] would ensure that 'innovative ideas and practices brought from outside the local context could be introduced and integrated with local support'.[32] Thus the benefit of both approaches may be harnessed.

---

[25] For instance, the ECOWAS Supplementary Act on Personal Data Protection of 2010, the EAC Legal Framework for Cyber Laws 2008/2011 and the SADC Data Protection Model-Law 2012.

[26] P Samuelson 'Five Challenges for Regulating the Global Information Society' at 13.

[27] Ibid.

[28] WHO 'From innovation to implementation: eHealth in the WHO European Region' (2016) at 77.

[29] Ibid.

[30] Ibid.

[31] International agencies, such as mHealth Alliance, are in the process of developing globally recognised standards and metrics that are relevant, for instance, in the storage and transmission of electronic health records.

[32] WHO 'mHealth: New horizons for health through mobile technologies' in the second *Global Observatory for eHealth Series* vol 3 (2011) at 64.

(2) Afro-centric approach: cultural and contextual sensitivity

Africa's biggest problem is that there are 'too many people going around the continent with solutions to problems they don't understand'.[33] It is suggested that a data protection instrument should reflect the cultural and contextual sensitivities of the people it wishes to protect. Principles of health care privacy enshrined in international or regional policies should be supported by a 'local awareness of privacy responsibilities'.[34] Developing countries 'have a wide range of social, ethical and gender considerations related to medical privacy'.[35] It is essential for eHealth practitioners providing eHealth services using personal data in foreign jurisdictions not only to be informed about aspects of the domestic law, but also to have a firm grasp of the sensitivities, language barriers and culture-specific aspects of the particular community in which they practice.[36] An understanding of the population's values and sensitivities should be sought.

An illustration of such a contextual barrier is in the frequent use of shared mobile phones. Kaplan explains:

> '[t]he developed world model of personal ownership of a phone may not be appropriate to the developing world in which shared mobile telephone use is important. Sharing may be a serious drawback to the use of mobile telephones as a healthcare intervention in terms of stigma and privacy'.[37]

To address this, Kaplan adds:

---

[33] L Timberlake *Africa in Crisis: the Causes, the Cures of Environmental Bankruptcy* (1985).

[34] Policy Engagement Network for the International Development Research Centre 'Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations' (2010) *LSE* at 3.

[35] Ibid.

[36] A Le Roux 'Telemedicine: A South African legal perspective' (2008) 1 *TSAR* 99 at 104 and 105.

[37] My emphasis. WA Kaplan 'Can the ubiquitous power of mobile phones be used to improve health outcomes in developing countries?' (2006) 2 *Globalization and Health* at 1.

> '***[r]egulatory reforms*** required for proper operation of basic and value-added telecommunications services ***are a priority*** if mobile telecommunications are to be used for healthcare initiatives'.[38]

Furthermore, societies have divergent ideas of what is acceptable, aberrant and abhorrent. Sensitivities are relative to sociocultural context.[39] Social status, status in terms of a particular illness, sexuality, mental health, and even diabetes are sensitive topics in certain cultures, with potentially adverse ramifications of wrongful disclosure.[40] The influence of the extended family, social obligations and values cannot be divorced from what is private to an individual in an African society. These represent challenges to the understanding of eHealth privacy issues. Cultural values also influence the adoption of standardised provisions from one culture to another. A report commissioned by the European Commission acknowledges this:

> 'A final difficulty is that of cultural and institutional non-equivalence... Despite the growing convergence of international data protection policy, privacy still means something very different in various cultural and national traditions, perhaps particularly in non-Western jurisdictions but by no means there alone'.[41]

An African approach based on a privacy and data protection framework that is sensitive to a developing market and shaped by the myriad of compelling health care restraints is essential,[42] particularly in, for instance, describing notions of 'privacy' and 'consent'. To resort simply to transplanting international model laws into African data protection legislation is misguided. Regulations should mirror the customary and community needs of the people whom they are to benefit. Basu suggests: '[t]here can

---

[38] Ibid.

[39] WW Lowrance Privacy, Confidentiality and Health Research (2012) at 19.

[40] J McGirk 'Religious leaders key in the Middle East's HIV/AIDS fight' (2008) 372 (9635) *The Lancet* 279–280 and 'Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations' A report prepared by the Policy Engagement Network for the International Development Research Centre (2010) at 15.

[41] CD Raab, CJ Bennett, RM Gellman and N Waters 'European Commission Tender No XV/97/18/D: Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to the Processing of Personal Data' (1998) *European Commission* at 202.

[42] A Seppala, P Nykanen and P Ruotsalainen 'Privacy-Related Context Information for Ubiquitous Health' (2014) 2 (1) *JMIR Mhealth and Uhealth* at e12 where '[c]ontext-sensitive privacy policies are needed to regulate information'.

never be a purely legislative solution to privacy, neither can there be a "model" legislative framework as socioeconomic issues are unique to countries and have to be considered in their own right for alleviating concerns over privacy'.[43]

Despite this, the urge exists to adopt readily developed regulatory solutions. Much may be learnt from other countries' experiences, particularly where policies developed in one country are emulated by others and then disseminated worldwide. Policymakers learn from both the positive and negative experiences of their counterparts elsewhere, permitting improved and more efficient decision making and thus enabling them to resolve their policy-making dilemmas better.[44] This can be helpful within an African context so long as the cultural traditions and sensitivities particular to the region are accommodated.

Sir Tim Berners-Lee advocates that principles of privacy, free speech and responsible anonymity be explored in a 'digital bill of rights for the web', which would be aimed at protecting and enshrining the independence of the Internet and the rights of its users worldwide. He continues that '[w]hile regional regulation and cultural sensitivities would vary', he believes that 'a *shared document of principle could provide an international standard for the values* of the open web'.[45]

Additionally, engagement in collaboration with international data protection agencies is a worthwhile endeavour. This offers an opening up of synergy between international, regional, and local regulators, health administrators, health professionals, academic institutions and communities. By doing so, it is expected that eHealth may find its recognised place within the current health care sector. Marsden proposes that '…co-regulation is becoming the defining feature of Internet regulation in Europe. It may prove the most appropriate model to respond to other dynamic technologically led and globalized fields of regulatory activity…'.[46]

In fact, the development of policy provisions appropriate within the African region may potentially inform other international jurisdictions. An example of synergy between international and domestic regulatory reform processes is illustrated

---

[43] S Basu 'Policy-Making Technology and Privacy in India' (2010) 6 *The Indian Journal of Law and Technology* 65–88 at 86.

[44] R Rose 'What is lesson-drawing' (1991) 11 *Journal of Public Policy* 4.

[45] My emphasis. 'An online Magna Carta: Berners-Lee calls for bill of rights for web' *The Guardian*.

[46] CT Marsden 'Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace' (2011) at 242.

in Brazil, which has recently provided normative input at an international level in relation to Internet governance. Its role clearly demonstrates how 'domestic reforms can provide a framework within which human rights in foreign policy can sit and find strength'.[47] By raising its credibility, it effectively increased its influence in shaping global human rights decisions.[48] The Brazilian framework demonstrates the importance of determining a strategy that is driven by the desire to establish realisable solutions.

As stated by Bennet:

> '[i]n the world of privacy protection, no government is an island. Decisions made anywhere in the world about system architecture, about standards, about international regulatory rules constrain, and will continue to constrain, how governments can and cannot process personal information to achieve programmatic goals'.[49]

Inclusion in an emerging and economically beneficial global privacy framework and the introduction of international standards, by drawing on lessons afforded by existing international protection of eHealth privacy policymaking, is significant.[50] The possibility of attaining regulatory alignment may be found in 'policy interoperability'. The concept of 'policy interoperability' is helpful in preserving the uniqueness of a country's social values within a legal framework. The concept presupposes that nations agree on the broad objectives of a policy, while acknowledging that different regulatory means may be implemented to achieve these goals. The wider purpose of the regulation is accepted rather than the specific details of its implementation. The idea is thus to avoid the threat that incompatible regulatory regimes may derail the benefit of convergence and globalisation.[51]

---

[47] Brazil's constitution of the Internet, known as the Marco Civil, establishes principles, rights and obligations of the parties to the Internet in Brazil. The Marco Civil was premised by the realisation that Brazilian people rejected a criminal framework for Internet governance in favour of a civil one. Of significance is that the framework evolved out of the needs of the population, as rooted in a contemporary, digital society. See A Gwagwa 'Internet Governance lessons Africa can learn from Brazil's success story'.

[48] Ibid.

[49] CJ Bennett 'What Government Should Know about Privacy: A Foundation Paper' (2001) Paper prepared for the Information Technology Executive Leadership Council's Privacy Conference at 29.

[50] Rose (n 44) at 3.

[51] Samuelson (n 26) at 13.

The paradox is that the need for a more global approach emphasises the need for a new form of local approach. Common interests at a global level in turn feed into the formation of regulations in a 'glocal' way, that is, in the creation of eHealth privacy policy that is 'tailored to the specific needs of a given locality and population', albeit with due consideration of global implications and influences. This provides the opportunity for the cultural uniqueness of a region to be acknowledged, whilst supporting a broader, common purpose.

Thus, rather than slavishly following the ever increasing push for more robust protection endorsed by developed countries, together with the resistance to adopting a 'one-size-fits-all approach' to privacy and data protection,[52] an uniquely African approach may be facilitated. For instance, the 'adequacy requirements' should be incorporated in a way that is both practical and functional in execution, and which emulates the essence of its inclusion. It should not merely be a means of appeasing the EU and expediting EU accreditation.[53]

(3) Rethinking the notion of 'consent'

An obstacle in the digitalised environment of the developing world is that of obtaining consent. It necessitates marrying the developing world (which is often illiterate) with the more developed and digitised world (which is highly literate). In determining consent in an environment that is both 'developing' and 'digital', the following questions remain unresolved.

Central to the enquiry regarding consent is, firstly, whether all personal data ought to be treated the same, or whether there is any justification in treating certain categories of sensitive personal data with greater compliance obligations. If certain categories of data require heightened protection, the definitions of such data and the concomitant compliance obligations require clarification. The nature of the consent and purpose for which consent is being sought require clarity. In what form should such consent be expressed? Should consent then be 'specific', 'informed' and 'in

---

[52] N Friederici, C Hullin & M Yamamichi 'Chapter 3: mHealth' in T Kelly (ed) *Information and Communications for Development 2012: Maximizing Mobile* (2012) at 53.

[53] See AB Makulilo 'Data Protection Regimes in Africa: Too far from the European "adequacy" standard?' (2013) 3 (1) *International Data Privacy Law* at 42–50.

writing'? However, can 'consent' be obtained a range of valid consent models, which exist on a continuum from the very stringent to the more lenient?

Secondly, in communities with significant rates of illiteracy, what alternatives can be found to guarantee effective consent? Can valid consent be obtained while avoiding unnecessary barriers to eHealth provision?

Lastly, how are the practical difficulties that hinder the effectiveness of consent as a mechanism for safeguarding online data protection rights to be addressed? How can consent be obtained through electronic processes, and are data messages, e-consent and electronic transactions valid methods of obtaining consent?

(i) 'Consent' in the Convention

The notion of 'consent' is problematic. 'Consent by a data subject' is defined in Article 1 of the Convention as *'any manifestation* of express, unequivocal, free, *specific and informed* will by which the data subject or his/her legal, judicial or treaty representative accepts that his/her personal data be subjected to manual or electronic processing'. Article 14 (2)(b) requires '*written* consent, by any means', which includes the requirement for consent to be in writing where sensitive data is processed. What is meant by 'by any means' is unclear. The inclusion of the words 'by any means' in the Convention alludes to the validity of the written equivalence in electronic form, as contemplated in Section II Article 6.[54] While this suggests that consent is sufficiently granted when manifested in any form, that is, verbally, on paper or electronically, the specific requirement of 'written consent' in respect of Article 14 indicates that a more onerous and strengthened indication of consent is required in cases of 'sensitive data' processing. For consent to be valid, therefore, it must satisfy the cumulative criteria of being specific, informed, freely given, and unambiguous. In certain instances, consent must also be in writing.

EU law attaches weight to user consent.[55] The European approach to consent is worthy of consideration, as EU data protection reforms have consciously sought to

[54] Writing in electronic form and functional equivalence is discussed hereunder.

[55] E Carolan 'The continuing problems with online consent under the EU's emerging data protection principles' (2013) 32 *Computer Law & Security Review* 462–473 at 462.

deal with the issue of online consent.[56] EU jurisprudence identifies three models of user consent: presumed consent; informed consent; and active consent.[57] The active consent model is an attempt to address the empirical realities associated with the presumed and informed consent models.[58] The introduction of newer forms of consent is an effort to cast consent as a 'reliable proxy for user privacy preferences online'.[59]

In comparison to the definition of 'consent' that is envisaged by the EU Regulation, however, the Convention falls short. While the Recitals to the EU Regulation include that consent is not freely given in instances where the data subject has no genuine and free choice, or where they are unable to withdraw or refuse consent without detriment, no such provision is included in the Convention. The Convention also fails to address the difficulties of providing consent in a developing world context, and the issue of consent specifically for eHealth data protection remains unresolved.[60] Consent is not explored in any detail in the Convention, save to say it should be 'express, unequivocal, free, specific and informed'. A significant failure of the Convention is the adoption of a consent-based approach constructed on the traditional doctrine, which takes no account of the changing context of online interactions, particularly those in the developing world.[61] Unfortunately, the opportunity to enhance the efficacy of the consent requirement in a uniquely technological environment is not fully developed in the Convention.

---

[56] Ibid at 463.

[57] Ibid.

[58] Ibid. Proposed by the Article 29 Working Party and favoured in the EU Regulation.

[59] Ibid at 463. Consent under the EU Regulation is 'any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.' See P de Hert and V Papakonstantinou 'The new General Data Protection Regulation: Still a sound system for the protection of individuals?' (2016) 32 *Computer Law & Security Review* 179–194 at 187.

[60] See CL Jack and M Mars 'Informed consent for telemedicine in South Africa: A survey of consent practices among healthcare professionals in Durban, KwaZulu-Natal' (2013) 6 (2) *South African Journal of Bioethics and Law* 55–59.

[61] Carolan (n 55) at 463, where a similar criticism is made of the EU Regulation.

(ii) Nature of consent

In modern forms of political democracy, those governed have the 'right to consent'. The core of democracy is the engineering of consent. Informed consent is a widely accepted legal, ethical, and regulatory requirement for most health care transactions.[62] Additionally, consent is a requirement for the lawful processing of a person's data. Consent underpins the ethical principles of respect for persons and individual autonomy.[63] Respect for autonomy and self-determination diminishes in instances of limited consent.[64] Besides autonomy, Otlowski lists 'respect and protection as the primary ethical principles underpinning consent'.[65] Consent can cause the imposition of new obligations, or the release from existing obligations.[66] Consent is the justification for allowing certain behaviour or action. With the necessary consent, certain previously unauthorised action is sanctioned. In the UK case of *Chester* v *Afshar*, Lord Steyn underlined the reason, from a legal perspective, why informed consent matters: 'in the context of attributing legal responsibility, it is necessary to identify precisely the protected legal interests at stake'.[67] Consent, thus, is a distinctive method of communicative transaction, which is used to waive ethical and legal requirements in specific ways.[68] It demonstrates a specific and uninhibited approval, acceptance and/or affirmation to engage in or waive prohibitions on actions, which may otherwise be intrusive.[69]

---

[62] N Chomsky *Profit Over People: Neoliberalism and Global Order* (2011) at 43. See C Grady 'Enduring and Emerging Challenges of Informed Consent' (2015) 372 *New Engl J Med* 855–862.

[63] OECD 'Guidelines on the Protection of Privacy and Transborder of Personal Data' (1980).

[64] K Sørensen, B Schuh, G Stapleton and P Schröder-Bäck 'Exploring the ethical scope of: a critical literature review' (2013) 2 *Albanian Med Journal* 71–83.

[65] MFA Otlowski 'Tackling legal challenges posed by population biobanks: Reconceptualising consent requirements' (2012) 20 *Med Law Rev* 191–226.

[66] SD Pattinson 'Consent and informational responsibility' (2009) 35 *J Med Ethics* 176–179.

[67] Ibid.

[68] NC Manson & O O'Neill 'Chapter 5: Informational privacy and data protection' in *Rethinking Informed Consent in Bioethics* (2007) 97–129.

[69] Ibid and see too L Curren and J Kaye 'Revoking consent: A blind spot in data protection law?' (2010) 26 *Computer Law & Security Review* 273–283 at 274.

Applying a traditional legal approach to consent in an online environment is challenging, however.[70] Pachter *et al.* advocate the introduction of the practice of health care that respects ethnic and cultural values. The question worth asking is whether, in a pluralistic society like, for instance, South Africa, and considering the impact of language and culture on eHealth initiatives together with the use of complex technological terminology, the notion of informed consent is adequately addressed.[71]

(iii) Feasibility of obtaining consent in developing countries

The feasibility of obtaining informed, written consent within developing countries is controversial.[72] Can the stringent concept of consent currently advocated in the Convention achieve the objective of attaining legitimate consent? Various authors question the appropriateness of obtaining individual informed consent in non-Western cultures.[73] The application of standardised consent models to various and differing cultural and social settings is certainly a challenge.[74]

Broadly speaking, the appropriateness of informed consent in developing countries turns on two arguments. The first is that individually based consent is

---

[70] Carolan (n 55) at 463.

[71] Ibid. See LM Pachter, J Sheehan and MM Cloutier 'Factor and subscale structure of a parental health locus of control instrument for use in a mainland United States Puerto Rican community' (2000) 50 (5) *Social Science and Medicine* 715–721 and C Jack, Y Singh, B Hlombe and M Mars 'Language, cultural brokerage and informed consent – will technological terms impede telemedicine use?' (2014) 7 (1) *South African J BL* 14–18 at 15.

[72] The doctrine of consent is entrenched in South African common law, case law and legislation, in which effect is given to the protection of an individual's right to physical integrity and self-determination provided in the Constitution. See M Mars and C Jack 'Informed Consent for Telemedicine in South Africa: Clinical Practice versus the Legislators' in *South African Telemedicine Conference* Cape Town 2010. And see Jack *et al.* (n 71) at 15.

[73] See MP Preziosi, A Yam, M Ndiaye, A Simaga, F Simondon and SGF Wassilak 'Practical experiences in obtaining informed consent for a vaccine trial in rural Africa' (1997) 336.5 *The New England Journal of Medicine* 370–373. See also CB IJsselmuiden and RR Faden 'Research and Informed Consent in Africa: Another Look' (1992) 326 *The New England Journal of Medicine* 830–834; M Barry 'Ethical considerations of human investigation in developing countries: The AIDS dilemma' (1988) 319 *The New England Journal of Medicine* 1083–1086 and EO Ekunwe and R Kessel 'Informed consent in the developing world' (1984) 14 (3) *Hastings Cent Rep* 22–24.

[74] IJsselmuiden and Faden (n 73) at 830.

'culturally or anthropologically inappropriate'.[75] As elucidated in research on a HIV/Aids trial drug in the Democratic Republic of the Congo (formerly Zaire)[76], the Western principle of informed consent, as set out in the Belmont report, is 'predicated upon the notions of respect for persons as individuals and as autonomous agents'.[77] This is at variance with the notion of personhood understood in African societies, which emphasises the embeddedness and integration of the individual within their community, where individuals define themselves largely in relation to others. Viewing oneself as a part of a greater whole thus effectively transfers the consent process from the individual to the family or to the larger community.[78] The findings suggest that many community members consent solely on the grounds of established trust and because of the associated benefits, which accrue to individuals and community members. A complete comprehension of the disclosed information is not their immediate priority. Community members who feel that a project's risk/benefit ratio is unacceptable, will usually refuse verbally, while others may adopt strategies of avoidance, like passive non-compliance, which are more creative.[79]

The second argument against the appropriateness of informed consent in developing countries is the inability of subjects to appreciate fully that to which they are consenting.[80] This is brought about largely by the complications in communication. Lack of understanding of technical or medical processes can compromise valid consent.[81] Moreover, language barriers and the poor literary levels of users may hinder the attainment of a desired specific outcome. Consent requiring the signing of informed consent documents containing medical, legal or technical

---

[75] Ibid, where it is stated that 'it is argued that insistence on first-person informed consent in group-oriented cultures is a form of medical-ethical imperialism that is morally unacceptable'.

[76] NA Christakis 'The ethical design of and AIDS vaccine trial in Africa' (1988) *The Hastings Center Report* at 31.

[77] Council for International Organizations of Medical Sciences and the WHO Proposed International Guidelines for Biomedical Research Involving Human Subjects (1982) at 32.

[78] JM Janzen *The Quest for Therapy in Lower Zaire* (1978) at 169 and 189.

[79] Ibid.

[80] See G Joubert, H Steinberg, E van der Ryst and P Chikobvu 'Consent for Participation in the Bloemfontein Vitamin A Trial: How Informed and Voluntary?' (2003) 93 (4) *American Journal of Public Health* at 582–584.

[81] C Jack, Y Singh, B Hlombe and M Mars 'Language, cultural brokerage and informed consent – will technological terms impede telemedicine use?' (2014) 7 (1) *South African J BL* at 16.

terminology risks being misunderstood in illiterate or semi-literate populations.[82] Obtaining valid informed consent is thus unlikely.[83] A Ghanaian study concluded that research and discussion on improved consent procedures were urgently needed, particularly in communities where subjects had little education.[84] The study found that education is one of the factors most consistently associated with an understanding of what the trial entailed and that consent appeared to be inadequate for ensuring comprehension amongst those less well educated.[85]

Further research concluded in Kenya illustrated a range of inter-related issues worthy of reflection. These issues included *conceptual and linguistic barriers* to communicating effectively about research, the critical and *complex role of communicators* (fieldworkers and nurses) in consent procedures, features of research unit-community relations that affect these processes, and the *special sensitivity of certain issues* such as blood sampling.[86]

Likewise, the inadequacy of users' health knowledge or technological literacy presents an obstacle in acquiring the requisite consent.[87] Users are often poor, illiterate, unfamiliar with the conduct of medical research or specific treatment, and have various opinions on disease causality.[88] These difficulties undermine the consent required for the processing of their data. Where consent is focused only on the choice rather than on the circumstances under which the choice was made, it presents obvious flaws as a determination of individual autonomy.[89] Clearly, how to reconcile the appropriateness of consent within these contexts requires rethinking.[90]

---

[82] Christakis (n 76) at 31.

[83] Jack *et al.* (n 81) at 15.

[84] Z Hill, C Tawiah-Agyemang, S Odel-Danso and B Kirkwood 'Informed consent in Ghana: What do participants really understand?' (2008) 34 *J Med Ethics* 48–53.

[85] Ibid at 52.

[86] My emphasis. See CS Molyneux, N Pershu and K Marsh 'Understanding of informed consent in a low-income setting: Three case studies from the Kenyan coast' (2004) 59 (12) *Social science and medicine* 2547–2559.

[87] See JJ Flinn 'Personalizing Informed Consent: The Challenge of Health Literacy' (2008) *Louis UJ Health Law and Policy* at 379 and Sørensen *et al.* (n 64) 71–83.

[88] N Lynoe, Z Hyder, M Chowdhury and L Ekstrom' Obtaining informed consent in Bangladesh' (2001) 344 *New England J Med* at 460.

[89] Carolan (n 55) at 464.

[90] Hill *et al.* (n 84) at 52.

(iv) Rethinking consent

A tension exists between the theoretical prerequisite for consent and the practicality in securing it. Debates with regard to the manner of obtaining valid consent follow a range of possible outcomes. The dichotomy between the very stringent consent methods, on the one hand, which require particular stipulation as to what the nature of the consent should look like, and the more lenient approach, which is a loosely defined notion of obtaining consent, on the other, together with the numerous permutations along a spectrum combining the two approaches is evident. Additionally, a tiered approach may be implemented, which ranges from the use of specific, stricter consent in certain circumstances, to the use of a broader, extended consent model in other contexts.

In rethinking the concept of consent and its application, certain questions arise. Should high expectations of obtaining consent be reduced and should we approve of a 'different' standard for developing countries? If so, what would that mean for the notion of consent and the validity thereof? How do we go about meeting expectations securely? Accordingly, in seeking and providing limited forms of consent, can they of themselves afford sufficient ethical justification? Could consent requirements vary according to a particular country or region, or across different communities within a country? Do all African jurisdictions have to adhere to the same consent rules? And finally, can consent given electronically be valid?

Since consent functions by waiving normative values in a particular way and with regard to a particular purpose, it should be understood against a broader background of norms and standards, both ethical and otherwise. Ethical issues embracing the concept of informed consent frequently present in subtle forms.[91]

'Consent' talks to us in various ways and takes a myriad of forms. Consent as a means of legitimation in the traditional sense gives rise to a formalistic system of privacy regulation. No perfect solution is clear, with distortions and special accommodations pointing in different directions. Are we to despair or can the situation be rescued? The range of possibilities extends from a basic acceptance, offering less protection, to a comprehensive consent model that offers more protection. Within these two extremes, a variety of standards of consent options is

[91] Sørensen *et al.* (n 64) at 71–83.

found, some of which are more appropriate to a given situation than others. Aspirations and realities do not always easily meet the proposition of high standards of consent. 'Pragmatic' considerations should influence the implementation of standards of consent, bearing in mind that consent is the pivotal issue around which the justification for the infringement of the individual's rights hinges.

On the one hand, the danger in accepting a more limited version of consent is the inherent risk in offering justifications that 'are less than convincing', and pegging standards that 'are less than feasible'.[92] On the other hand, however, insisting on the implementation of unobtainably high standards, in the full knowledge that practice and standards diverge, is to acknowledge that proper consent is not being validly or sufficiently obtained in any event.[93] Although high expectations are needed, what is required practically is a way of reliably acceding to that bar. Ultimately, rules, techniques and methods regarding consent should describe a process of explanations and achievements, presenting an awareness of a reality reflecting imperfections and incompatibilities. A traditional consent-based approach, when applied to an online environment within the context of a developing country, is flawed. A consent model that addresses contextual and empirical issues is thus sought, where it is understood that consent givers are subject to a variety of specific situational influences that intuitively impel the giving of consent.[94]

Unfortunately, few practical guidelines on how best to inform users are available, particularly in less developed countries.[95] Practically, consent functions as a 'weak and poorly-correlated proxy for individual autonomy'.[96] Consent cannot always be obtained in a format that adheres to the very strict parameters set down for its attainment.[97] Thus, often consent is either not given at all, or where it is given, it fails on procedural and legal grounds and, in any event, is invalid. This is confirmed in a research study conducted in South Africa in 2005, which concluded that informed

---

[92] Ibid.

[93] See a survey conducted in KwaZulu-Natal, South Africa by C Jack and M Mars 'Informed consent for telemedicine in South Africa: A survey of consent practices among healthcare professionals in Durban, KwaZulu-Natal' (2013) 6 (2) *S Afr JBL* 55–59.

[94] Carolan (n 55) at 463.

[95] Lynoe *et al.* (n 88) at 460.

[96] Carolan (n 55) at 464.

[97] Manson & O'Neill (n 68) at 97–129.

consent in disadvantaged communities may often be 'inadequate'; the study advocated that new ways to 'improve understanding' should be explored.[98] Confirmation of this is also to be found in research by Jack and Mars, who conclude in a survey of consent practices in South Africa that written informed consent is 'not routinely obtained from patients during clinical examination or when using ICT for the transfer of patient information'.[99]

Failures are exacerbated rather than remedied by imposing increasingly higher and supposedly better standards of consent.[100] South African law, for instance, represents the strictest point on the spectrum of consent models. The excessive pursuance of driving impractical conceptions of consent, such as 'informed, written consent', 'fully explicit' or 'fully specific' consent, particularly within technologically, developing countries, is troublesome. As suggested in Manson and O'Neill, 'invoking implausible or underground conceptions of individual autonomy or of informational privacy' cannot ease difficulties.[101] The evidence gathered from research conducted by Whitley and Kanellopoulou indicates that informed consent rarely operates satisfactorily in online interactions, as it is unlikely to be 'truly informed and freely given'.[102]

Critically, ethical and legal thinking with regard to the integration of informed consent within emerging health information technologies predominantly concerns privacy and security.[103] Informed consent is intrinsically linked to confidentiality.[104] A move to an implied consent model, as proposed by Mars and Jack,[105] may be of some benefit, especially in the practice of synchronous telemedicine; this, however, is not canvassed in the Malabo Convention. Of interest is the case made internationally

---

[98] K Moodley, M Pather and L Myer 'Informed consent and participant perceptions of influenza vaccine trials in South Africa' (2005) 31 *J Med Ethics* 727–732.

[99] Jack and Mars (n 93) at 55.

[100] Manson & O'Neill (n 68) at 97–129.

[101] Ibid.

[102] EA Whitley and N Kanellopoulou 'Privacy and Informed consent in online interactions: Evidence from Expert focus groups' (2010) *ICIS 2010 Proceedings Paper 126* at 15.

[103] MM Goldstein 'Health Information Technology and the Idea of Informed Consent' (2010) 38 *Journal of Law, Medicine and Ethics* 27–35.

[104] C Jack and M Mars 'Telemedicine: A need for ethical and legal guidelines in South Africa' (2008) 50 (2) *South African Family Practice* 60a at 60c.

[105] Ibid.

for the incorporation of 'dynamic consent', which combines both technical and policy flexibility.[106]

Mars and Jack suggest that the imposition of written informed consent by regulators in countries with low literacy levels will be unduly 'onerous' and that it will have the undesirable effect of hampering telemedicine and eHealth usage, rather than enabling it. In an age where data is shared digitally on a worldwide scale, traditional systems of informed consent are static, paper-based and largely organised around national borders and domestic legal frameworks.

Finally, four points emerge: firstly, obtaining consent from an individual cannot always be regarded as an accurate articulation of the individual's choice; secondly, a consent-based approach is, at best, incomplete; thirdly, a specific difficulty exists when applying consent in an online environment; and lastly, there is an additional difficulty with the obtaining of consent in developing countries.[107] From this, the obvious question arises in conclusion: what might be an alternative approach to obtaining consent in an online eHealth environment in developing countries?

The following is clear: in practice, neither information nor greater action reliably signify the presence of true and valid consent. Moreover, insisting on increasingly rigorous evidential markers and standards of attaining consent proves insufficient in an online health care environment in the developing world. Consequently, the law should avoid any reliance on measures that assume all users are comparable rational optimisers of their online privacy. Instead, a more flexible approach, which is situationally and contextually appropriate, is warranted to obtain optimal and worthy consent. These mechanisms could take the form of the strategic use of default privacy settings and various 'choice architectures', thus encouraging users to engage in various understandable decision making. For individuals to make choices, one should consider the social contexts, the relations that inform the volume and nature of the information disclosed, as well as the timing, manner and impact of the decisions made.[108] Where it is to be said that an individual has granted 'implicit

---

[106] See J Kaye, EA Whitley, D Lund, M Morrison, H Teare and K Melham 'Dynamic consent: A patient interface for twenty-first century research networks' (2015) 23 *European Journal of Human Genetics* 141–146, who define 'dynamic consent'.

[107] Carolan (n 55) at 472.

[108] See CS Molyneux 'Trust and Informed Consent: Insights from Community Members on the Kenyan Coast' (2005) 61 (7) *Social Science & Medicine* 1463–1473. See also D Elbourne, C Snowdon and J

consent' to disclosure, the safety mechanism should place the onus on the responsible party to prove that the individual has made a positive decision in the circumstances. Lastly, the implementation of a culture- and behaviour-centric approach to consent, which is sensitive to the context within which it is granted, requires, as a prerequisite, greater clarification of the position and boundaries relating to online privacy than has previously existed.

(vi) The validity of eConsent and electronic transactions

Obtaining valid consent by using electronic processes should be established. Are data messages, e-consent and electronic transactions valid? 'Consent of a data subject' is defined in the Malabo Convention as meaning '…any manifestation of express, unequivocal, free, specific and free will…'[109]

The EU Regulation defines consent as 'any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed'.[110] In terms of the EU Regulation, consent can thus be an oral or written statement, and may take electronic form. Recital 25, however, provides that pre-ticked boxes on a website, silence or inactivity on the part of the user do not constitute valid consent.

A defining characteristic of eHealth applications is that they are carried out at a distance, where the provider and the user are for the most part in different locations. Noticeably, then, a contractual relationship in eHealth may be conducted partially or wholly electronically in an online environment. Consequently, difficulties that do not arise in traditional paper-based contractual arrangements or where services are provided personally may well develop. Issues pertaining to, for instance, the validity and enforceability of electronic transactions, contracting online and providing consent electronically as well as the admissibility of, for instance, consent documents, may become problematic.

Garcia 'Informed consent. Subjects may not understand concept of clinical trials' (1997) 315 (7102) *British Medical Journal* 248–249.

[109] Article 1 of the Malabo Convention.

[110] Article 4(8) of the EU Regulation.

The UNCITRAL Model Law on E-Commerce adopts the principles of non-discrimination, technological neutrality and functional equivalence. The principle of non-discrimination provides that any document would not be denied legal effect, validity or enforceability solely because it is in electronic form. The principle of technological neutrality enforces provisions that are neutral with regard to the technology used, and functional equivalence establishes the criteria under which electronic documents may be considered equivalent to paper-based documents. The UNCITRAL Model Law on E-Commerce has been largely influential in the drafting of the provisions of many of the e-legislations found in Africa.[111]

Where there is a requirement that consent be 'in writing', it is expected that Article 6 of the Malabo Convention may provide some relief to eHealth practitioners, where data messages are recognised as the functional equivalence of written ones and as having the same legal value as a message written on paper.[112]

(4) Data mobility and data transfer between states[113]

The elements to be determined are threefold. Firstly, how do African standards coincide with international privacy standards, so that exchanges outside of the continent may be efficiently expedited? Secondly, how are standards within the African continent constructed, so that an equivalent level of protection is available to all member states wishing to permit the free flow of data across borders? And thirdly, how are these measures to be implemented?

The debate surrounding the creation of eHealth data regulation transcends geographical or organisational boundaries. Issues around *inter alia* privacy and data security across borders are essential components of the very nature of eHealth applications and are cited as requiring a transnational approach in order to find workable solutions.[114]

---

[111] For instance, Uganda, Rwanda and Zambia.

[112] Article 6 (2) of the Malabo Convention.

[113] M Kekana, P Noe and B Mkhize 'The practice of telemedicine and challenges to the regulatory authorities' (2010) 3 *S Afr J Bioethics Law* at 33.

[114] See T Gerber, V Olazabal, K Brown and A Pablos-Mendez 'An Agenda For Action On Global E-Health' (2010) 29 (2) *Health Affairs* at 236 for the 'transnational efforts' in eHealth development.

eHealth involves the application of law to a borderless technology that moves fluidly between countries and across state borders.[115] With the establishment of designated 'centres of excellence', this becomes even more apparent. Data mobility inhibits the ability of any solitary nation to enforce its data protection laws effectively, as the application and enforcement of national law cannot extend beyond its borders. This is primarily a reactionary response to the nature of data and its inherent ability to flow freely across boundaries.

Additionally, an inherent component of the practice of eHealth applications is the vast accumulation of personal data, and therefore the need to manage and store this. While considerations of public and private international law, as they relate to eHealth, are useful in that they inform privacy law developments, specific unifying public and private global eHealth privacy laws governing inter-jurisdictional data exchanges do not exist.[116] Instead, principles drawing on a combination of laws affecting trade, telecommunications and, to a more limited extent, health care, not all of which are appropriate or relevant, are relied upon.[117] Adopting standardised data exchange and 'adequacy' requirements, model contract clauses, and establishing local protection authorities may achieve data exchange compliance regulation.

(i) Data havens

'Data havens' are jurisdictions with no or limited data protection laws, to which personal data can be transferred, for the purpose of circumventing the national laws of the country of origin of the data. The establishment of 'data havens' undermines national data protection laws by allowing the storage and management of data in a manner that may be otherwise unlawful, or subject to restrictions, in countries elsewhere.

The OECD has acknowledged the threat inherent in such 'data havens'. While preventing them from arising, the intention is simultaneously to enable the free and secure flow of data across national boundaries.

---

[115] JD Blum 'The role of law in Global e-health: A tool for development and equity in a digitally divided world' (2002) *Saint Louis University Law Journal* at 2.

[116] Ibid.

[117] Ibid.

To obviate the creation of 'data havens', it is necessary for different countries to provide an equivalent level of data protection, thereby ensuring that information can be passed between them unrestricted and under the same rules of storage and passage. The thinking is that, where a consensual and standardised approach to data processing and data exchange is adopted between countries, the benefit of 'opportunistic data havens' will be removed. The cross-border dimension of eHealth requires stronger support for 'regulatory convergence' in this field and the exchange of 'good practice internationally'.[118]

(ii) Adequacy requirements

In an attempt to persuade other jurisdictions to adopt comparable personal data protection measures, certain regimes, such as the EU, have implemented reciprocity-based rules. The intention is to curtail transnational data flows into and out of nations, which the EU considers not to provide 'adequate' protection of personal data.[119]

Such reciprocity-based measures are a means to achieve harmonisation between nations exchanging personal data. With regard to the EU requirements, the provisions are contained in Chapter V of the EU Regulation. The Regulation sets out the new framework for data transfers and is a significant driver of the emerging global data protection regime. The EU Regulation, like its predecessor, the EU Directive, provides that the transfer of personal data to third countries, that is, to non-European Union member states (which would include African countries) can only occur, where such country can guarantee an 'adequate' level of data protection. Thus, countries that wish to engage in data transactions and exchanges with EU member states are required to provide an 'adequate' level of data protection.[120]

Understandably, this has enormous influence and implications for eHealth initiatives in African nations that wish to engage in data transactions with the EU. To date, all African countries fall short of these 'adequacy' standards. Does this position

[118] Green Paper on mHealth (2014) at 18.

[119] Samuelson (n 26) at 1.

[120] Article 45(1) provides that '[a] transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.'

perhaps illustrate a key example of a failure to exhibit a sensitivity to an African context? Is there a need for a lower standard or a 'different' set of standards that is more accommodating of African countries?

In circumstances where countries do not comply with the 'adequacy' requirement, additional enquiries are made into whether legal grounds for transfer may apply, such as, whether transfers use the appropriate EU Commission approved model transfer terms.[121] For the purposes of Article 45 of the EU Regulation, standard data contractual clauses (known as model contract clauses) may be adopted by a supervisory authority and recognised by the European Commission as offering adequate safeguards. The European Commission has developed four sets of approved model contracting clauses.[122] Use of the model clauses, whether as an independent contract or whether incorporated into other contracts, where the wording is altered (despite the meaning or effect of the changed clause remaining the same), will disqualify the use of the clauses, as authorised by the Information Commissioner, from constituting adequate safeguards.[123] The use of model contract clauses, given that the Commission has determined that such clauses offer adequate safeguards, will be safe from challenge regarding the effectiveness of the protection offered.[124] Additionally, Article 45 describes the conditions under which transfers grounded on binding corporate rules, and based on current practices and on the requirements of supervisory authorities are permitted.[125]

(iii) Safe harbour agreements

A possible solution to difficulties with data transference lies in the establishment of safe harbour agreements between nations. While data export is allowed between countries within the European Economic Area, and those approved as adequately

[121] See Articles 40 through 45 of the Regulation.

[122] See http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010D0087&from=EN (accessed 20 February 2017).

[123] 'Model Contract clauses: International transfers of personal data' (2012) *Information Commissioners Office* 1 at 6.

[124] Ibid.

[125] 'Proposal for a Regulation 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 (General Data Protection Regulation)' (2012) *European Commission*.

compliant, countries could until recently exchange data with the EU in terms of principles set out in a 'safe harbour' agreement.[126] Certain 'safe harbour' agreements, such as that between the US and the EU, have recently been the subject of attack, however.[127] In 2015, the Court of Justice of the European Union held, in *Maximillian Schrems v Data Protection Commissioner and Digital Rights Ireland Limited*,[128] that the transfer of data of European subjects, in this case Facebook subscribers, to the United States was to be suspended on the grounds that the US did not afford an adequate level of protection of personal data within the meaning of Article 25 of the Data Protection Directive. Significantly, the Court of Justice declared that the Commission Decision 2000/520/EC[129] on the EU-US safe harbour framework was invalid.[130] The Court of Justice moreover affirmed that the threshold for the adequacy assessment is 'essential equivalence' and demanded a strict assessment against this high standard. The outcome of this judgment is that it renounces both EU data controllers' and US recipients' reliance on the 'safe harbour' agreement in an attempt to legitimise their data transfers. This places them in an immediately precarious position.[131]

To introduce safe harbour agreements in this way within Africa would, by all accounts, require that such agreements and their provisions be assessed as to whether they are indeed the 'essential equivalence' of the standards set out in the 'adequacy requirements'. If such provisions do not afford an adequate level of protection, as set

---

[126] A 'safe harbor' agreement is a policy agreement concluded between the US Department of Commerce (or other country) and the EU, which seeks to regulate the manner in which US (or the other country's) companies manage the personal data of EU citizens.

[127] This in part following Edward Snowden's revelations regarding the US National Security Agency surveillance of data held by 'safe harbour' participants. These revelations severely undermined the credibility of US 'safe harbour' members. For more in this regard, see 'ECJ rules that the EU-US Safe Harbor arrangement is invalid' (2015) *Practical Law*.

[128] The High Court of Ireland held that, in determining a complaint, which has been made to an independent office holder, that personal data transferred to another third country (in this case, the United States of America), the laws and practices of which did not contain adequate protections for the data subject.

[129] Article 1 of the *Commission Decision 2000/520/EC* (Decision 2000/520) provides that adequate protection is provided by US undertakings who self-certify their adherence to the 'safe harbour' principles.

[130] See the Court of Justice of the European Union Press Release No. 117/15 of 6 October 2015.

[131] See ECJ rules (n127)

out in the African regional instrument, such safe harbour agreements could also risk being set aside and data transfer suspended.

(iv) Privacy Shields

In response to the EU Court of Justice ruling of 6 October 2015 in *Schrems*, the European jurisprudence on fundamental rights,[132] the letter of the Working Party to the European Commission on Safe Harbour of 10 April 2014 and the Working Party's Working Document on transfers of personal data to third countries,[133] in February 2016, the European Commission and the US Department of Commerce announced that a new framework for transatlantic data flows, the EU-US Privacy Shield, was to replace the safe harbour arrangement.[134]

The Privacy Shield imposes stronger obligations on US organisations who seek to process Europeans' personal data and requires that monitoring, oversight and enforcement mechanisms be established that are more robust.[135] Additionally, it tightens the conditions under which data can be transferred onwards to third parties.[136]

To this end, and in recognition of the shared goal of the US and the EU of enhancing privacy protection and to provide US organisations with a reliable mechanism for personal data transfers to the US from the EU, the US Department of Commerce issued a list of Privacy Shield Principles, including certain Supplemental Principles, it terms of its statutory authority to 'foster, promote, and develop international commerce'.[137]

---

[132] Available at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf (accessed 20 February 2017).

[134] EU-US Privacy Shield (2016). Aso see 'EU-US Privacy Shield: Stronger protection for transatlantic data flows' (12 July 2016).

[135] Ibid.

[136] Ibid.

[137] The Privacy Shield Principles are available at http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf (accessed 20 February 2017).

On 30 May 2016 the European Data Protection Supervisor issued an Opinion on the EU-US Privacy Shield, calling for a more sustainable solution.[138] In the press statement Giovanni Buttarelli, the European Data Protection Supervisor, stated:

> 'I appreciate the efforts made to develop a solution to replace Safe Harbour but the Privacy Shield as it stands is not robust enough to withstand future legal scrutiny before the Court. Significant improvements are needed should the European Commission wish to adopt an adequacy decision, to respect the essence of key data protection principles with particular regard to necessity, proportionality and redress mechanisms. Moreover, it's time to develop a longer-term solution in the transatlantic dialogue.'[139]

While the Statement of the Working Party acknowledges certain improvements offered by the Privacy Shield compared to that of the safe harbour agreement, it nevertheless expresses various concerns and seeks greater clarifications in order to ensure that the draft adequacy decision and the protections offered under the Privacy Shield are indeed equivalent to those of the EU, and most particularly those offered in the EU Regulation.[140] Article 45 of the EU Regulation provides new conditions for the transfer of data based on an adequacy decision.

With the EU Regulation becoming fully implementable across the EU in May 2018, it should be borne in mind that it finds application to all data protection related matters, including those involving the transfers of data. In this regard, a review of the literary content and substance of the Privacy Shield can only occur, once the EU Regulation has become applicable in law in the course of 2018, in order to ensure that the higher levels of data protection offered by the EU Regulation are consistent with those provided for in the Privacy Shield.

Despite the Privacy Shield being seen as useful, it has not been without criticism. In its current formulation, the Shield is considered not comprehensive enough, nor does it include all appropriate safeguards to protect the rights of EU

---

[138] European Data Protection Supervisor Press Release EDPS/2016/11 (2016).

[139] Ibid at 1.

[140] Statement of the Article 29 Working Party on the Opinion on the EU-US Privacy Shield (13 April 2013). See the European Data Protection Supervisor Opinion on the EU-US Privacy Shield draft adequacy decision (May 2016) at 2.

individuals to privacy and data protection.[141] The Shield is also viewed as feeble in its provision of judicial redress and oversight mechanisms.[142] It is stated that 'significant improvements are needed should the European Commission wish to adopt an adequacy decision'.[143]

As the Privacy Shield extends to data use and transfer outside the US, the Article 29 working party insists that onward transfers from a Privacy Shield party to third party country recipients should only be permissible, where such third party countries provide an equivalent level of protection pertaining to all matters contained in the Privacy Shield (including those of national security), and that such protection measures should in no way lower, circumvent or compromise the high standards imposed by the EU data protection principles. This has grave implications for Africa.

(5) Enforcement and execution

A less cumbersome approach for member states would be for the Malabo Convention explicitly to establish a model legal data protection framework, which states could adopt and ratify into their domestic legislation.[144] Thus, states would not have to initiate the arduous process of developing new laws, or amending existing ones, but could rather have the option of expediting the process by simply adopting the model law as is, and then ratifying it into their law.[145] In the absence of such model law, it may take a considerable length of time before African states have developed and harmonised their respective data protection laws to the extent necessary to afford effective regional cooperation between the members. Additionally, a model law would eradicate inconsistencies in terminology and phraseology. As the position stands now, it is unlikely that member states' interpretation and development of national laws will be sufficiently uniform in order to facilitate the necessary effective regional harmonisation.[146]

---

[141] Ibid.

[142] Ibid.

[143] Ibid.

[144] UJ Orji 'Examining Missing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection' (2014) 5 *Cri* at 132.

[145] Ibid.

[146] Ibid.

Enforceability of a regional instrument is also problematic.[147] The most obvious tension is between the role of a 'domestic' court and that of a 'regional' or 'international' court. The first question is what the role of the domestic courts should be in assisting in the enforcement of what are primarily national laws, and then in the enforcement of the provisions of any incorporated international or regional laws. The second question is whether there is any justification in establishing a regional or international court to complement national judicial systems to attend to such matters, in the event of certain conditions being met. The implication seems to be that domestic African courts first attempt to enforce international and regional law, failing which enforcement in a regional or international court is required.

However, the establishment of a coercive means to secure and enforce a regional African Union law is difficult. Additionally, how such enforcement mechanisms would 'fit' within existing African Union institutions requires consideration.[148] These considerations have resonance with the process of institution building in Africa. The question posed is, what is the nature of integration demanded in the idea of the African Union, and what is, if anything, its role in policy enforcement? Is its role that of a supranational institution or merely one of an intergovernmental agency? Moreover, reform of the function of the AU court, and possibly even the establishment of a new African regional court, should be considered. Perhaps the African Court of Justice and Human Rights[149], which has the objective of complementing and strengthening the protective mandate of the African Commission on Human and Peoples' Rights, may provide benefit.

Effective enforcement centres on the question regarding the site of the enforcing authority. Which tier represents the appropriate location of authority for enforcement in a matter involving the breach of data protection provisions? The doctrine of subsidiarity is relevant in this regard. This principle seeks to safeguard the ability of member states to take decisions and act accordingly. It authorises intervention by the regional institution only when the objectives of an action cannot

---

[147] C Heyns and F Viljoen 'An Overview of International Human Rights Protection in Africa' (1999) 15 *South African Journal on Human Rights* at 421–445.

[148] Maluwa (n 12) at 157.

[149] The OAU adopted the protocol to the African Charter establishing the African Court in Burkina Faso on 10 June 1998.

be sufficiently achieved by the national states themselves, or when they can be better achieved at a regional level. This presupposes the making and implementing of decisions at the lowest level of the institutional scale as possible.[150] The purpose of subsidiarity is to sustain a degree of independence for lower authorities in relation to higher regulatory bodies. In other words, national government should not take action, if provincial government can do so, and provincial government should not take action, if municipal government will suffice. This thus favours the allocation of power between numerous tiers of authority. Pragmatically, the concept of subsidiarity legitimises the extension and constraint of authority by connecting governance to particular competencies within a tiered system. Although not explicitly promoted, the principle of subsidiarity has been applied in Africa.[151]

When applied in the context of enforcement, the principle of subsidiarity serves to limit regional intervention, when a matter can best be addressed by states themselves at a domestic national level. Only if national states are unable to achieve the objectives of a proposed action satisfactorily, or if additional value can be provided, where an action is carried out at a regional level, is intervention by the regional institutions appropriate. This encourages decisions to be made as far down the institutional chain as possible. International courts or tribunals should thus not be involved in decisions, where regional courts are competent decision makers and enforcers. Likewise, if domestic courts can perform regulatory enforcement satisfactorily, this should be promoted. Such reinforcement may prove to be a more realistic option. Strengthening regional and sub-regional decision-making and enforcement mechanisms may enhance international collaboration in supporting data protection actions. While there is evidence of greater regional cooperation, applying the principle of subsidiarity would presuppose that affected national governments are committed to preventing and protecting data processing, and thus to promote the enhancement of African intergovernmental capacities.

---

[150] Article 5(3) and Protocol No. 2 of the Treaty on European Union, Treaty of Maastricht, 7 February 1992, Official Journal of the European Communities C 325/5 24 December 2002. See D O'Brien 'The search for subsidiarity: The UN, African regional organizations and humanitarian action' (2000) 7 (3) *International Peacekeeping* 57–83 at 58.

[151] D Helly 'Africa, the EU and R2P: Towards Pragmatic International Subsidiarity?' (2009) *Journal for International Relations and Global Trends* 45–58 at 56.

IV WHAT FORM SHOULD THIS TAKE?

What form should such amendments take? The various possibilities are discussed below. They include the amendment of the Malabo Convention, a new *sui generis* regional data protection instrument, and a eHealth specific privacy code of conduct.

(1) Amendment of the Malabo Convention by means of additional protocols

A possible solution may lie in strengthening the Malabo Convention, given that the Convention has already been effected. Developing an additional protocol or guidance notes may thus provide member states with a model legal framework with regard to data protection, which could become the standardised foundation from which the individual African member states' data protection legislations can evolve.

An attempt to formulate and define key unifying and standardised principles will not only circumvent confusion, but also carefully avoid the tortuous, protracted process of legal and regulatory development within each individual African nation. It is suggested that it would be more intellectually sound and doctrinally satisfying, if regulations or guidelines based on data protection principles and tailored specifically to the management of sensitive data, were developed and adopted within Africa. The regulatory challenges of implementing a privacy framework, in a multifaceted and advancing environment, will require careful consideration of the role of consent and data exchange.[152]

To address matters of extradition, mutual assistance, and enforcement measures between AU member states, an additional protocol to the Malabo Convention may be necessary.[153]

(2) A new regional sui generis data protection instrument

The second option may be to redraft the Malabo Convention in its entirety. The Malabo Convention comprises three chapters – electronic transactions, data protection

---

[152] D McGraw, JX Dempsey, L Harris and J Goldman 'Privacy As An Enabler, Not An Impediment: Building Trust Into Health Information Exchange' (2009) 28 (2) *Health Affairs* 416–427. See also J Li 'Privacy policies for health social networking sites' (2013) 20 (4) *Journal of the American Medical Informatics Association* 704–707.

[153] Orji (n 144) at 134.

and cybersecurity. The Convention is thus a commercial, human rights and criminal law instrument. It is exceptionally broad in its scope. Moreover, it is not specific to the data processing of health care related information, or eHealth related services, as its provisions are general in application.[154]

Difficulties around privacy and data protection in eHealth may be resolved through a comprehensive framework that balances the implementation of strengthened and clearly defined privacy principles and statutory direction, adopts trusted technological mechanisms, includes industry best practice and establishes oversight, accountability and enforcement measures.[155] The evolution of clear principles would thus translate into a privacy-based action, with a well-defined recourse for remedies and legal redress for damages. To engender trust and confidence in eHealth activities, policymakers will need to craft policies and regulations that encourage enforceable fair-information and privacy practices within an emerging and underdeveloped health care environment.[156] This could take the form of a regional *sui generis* data protection instrument.

Finally, as asserted by Mizani and Baykal, the solution in summation is to be found in regulations, standards and procedures, inter-organisational efforts and multi-disciplinary specialised interventions.[157] The development of a consolidated African instrument specifically for that purpose may well provide such a baseline solution.

(3) A code of conduct specifically for eHealth privacy protection

Regulation may additionally be advanced by the introduction of a code of conduct that is aimed at a specific sector of the eHealth industry. Such a code may assist eHealth service providers in complying with data protection principles when developing eHealth applications, for example, by providing rules on obtaining consent for data use, and by providing for and describing the notion of transparency.

---

[154] Article 1 Malabo Convention at 5. However, it does contain specific principles for the processing of sensitive data in Article 14.

[155] Ibid.

[156] J Goldman and Z Hudson 'Virtually exposed: Privacy and e-Health' (2000) 19 (6) *Health Affairs* at 145.

[157] MA Mizani and N Baykal 'Policymaking to preserve privacy in disclosure of public health data: A suggested framework' (2015) 41 *J Med Ethics* at 263.

Although such a code is often industry specific and limited in application, a code may raise awareness of the data protection rules in relation to eHealth applications, and thus could facilitate and increase compliance with the more general regional data protection instrument. Guidance can be targeted at eHealth application designers, for instance, individuals, companies or organisations who make available (either directly or via application stores) software applications for mobile devices, which are intended to process data concerning health.

Building a governance regime of this sort may seek to ensure effective monitoring and enforcement where required and promote standards of good practice across the industry. Although useful in providing practical measures of privacy implementation, voluntary compliance is required for an instrument of this nature. This unfortunately does not always guarantee compliance, however, and it cannot provide a complete solution to the eHealth privacy debate.

A code of conduct for mobile health privacy was submitted to the EU Article 29 Working Party on 7 June 2016.[158] Issues covered by the EU code of conduct, which may be useful in a similar African code, include user's consent, purpose limitation and data minimisation, privacy by design and, by default, data subjects' rights and information requirements, data retention, security measures, principles on advertising in eHealth applications, use of personal data for secondary purposes, disclosing data to third parties for processing operations, data transfers, personal data breach, and data gathered from children.

A further example is the publication, on 27 September 2016, of a data protection code by the Cloud Infrastructure Service Providers in Europe. This code takes into account the specific role of European Cloud Infrastructure Service Providers. The self-regulatory code lists data protection requirements to be complied with by cloud service providers under current and future EU law.[159] In terms of the EU Regulation, associations and bodies are encouraged to develop codes of conduct, the purpose of which is to facilitate the effective application of the EU Regulation.[160] A further example of a code of conduct emerging out of the EU is the code of conduct

---

[158] 'Code of Conduct on privacy for mHealth apps has been finalised' (2016).

[159] 'Data Protection Code of Conduct for Cloud Service Providers' (2015) *EU Digital Single Market*.

[160] Article 40 of the EU Regulation.

for mobile health privacy. This code was finalised and submitted to the EU Article 29 Working Party on 7 June 2016.[161]

The Malabo Convention defines a 'code of conduct' in Article 1. However, no mention is made of it in the section on data protection. As is found in the EU Regulation, industry associations and other bodies should be encouraged to develop codes of conduct to facilitate the application of the provisions contained in the Malabo Convention. Codes of conduct may thus exist side by side with the Convention and act to reinforce the practical, industry specific application of the Convention. Codes of conduct are useful, in that they not only reflect existing industry approaches, but also set out goals towards which the industry might strive in future.

V CONCLUSION

The contribution of this chapter is twofold: firstly, it recommends the adoption of multiple layers of data protection regulatory measures; secondly, it proposes that significant strides in data protection can be made by the use of a formal regional regulatory legal instrument. I questioned the completeness of the Malabo Convention and sought to identify those areas of data protection within the Malabo Convention, where the content and substance require amendment. Following this, finally, I addressed what form such amendments should take.

[161] 'Code of conduct for mHealth privacy sent to WP29' (2016) 3 (6) *Ehealth law and policy* at 1.

CHAPTER 9: POSITION GOING FORWARD

The issue of privacy is not for us simply as a matter of business practice. It's just fundamental to human dignity.

Gerald Levin

I INTRODUCTION

This thesis presents a constructive perspective, a conceptual understanding and a pragmatic critique of the questions that lie at the intersection of the following: an individual's right to privacy and data protection, the cultural disparity when defining privacy, the sensitivity of health related data, the individual's right to health care, where lack of resources and accessibility are often commonplace, the introduction of networked technologies and development within the health care system as solutions, the borderless and largely unregulated nature of the digital environment, and the emergence of more stringent data protection norms internationally.

II POSITION GOING FORWARD

The solution to safeguarding data privacy in eHealth within the African region is proposed. It is suggested that there is a need to reaffirm human rights values particularly the right to privacy. The future position in South Africa is discussed, as is the way forward for Africa.

(1) How to resolve the paradox

Against the backdrop of emerging regulatory policies and practices, I have examined the complexity of challenges in the context of eHealth development in Africa, with particular attention being paid to the right to privacy and protection of the processing of personal data. While eHealth service delivery and the widespread reach of the data generated are revolutionary, the concomitant threat to privacy is inevitable. An appeal is made for a more systematic and critical review of the regulation of data protection and data exchanges, and for a simplification of the regulatory environment by unifying the governance of data privacy protection within Africa.

In answering the various challenges, I argue that the adoption of an accepted social imperative protected by a powerful triumvirate of ethical constraints, effective legal provisions and regulations, and operational necessities, is possible. I therefore support the adoption of multiple layers of protection and the establishment of a consolidated regional instrument, which provides a regulatory baseline comprising clearly defined, non-negotiable, yet contextually and culturally sensitive

data protection standards and principles that are relevant specifically to health care delivery in an eHealth environment in a developing world. Such an instrument should still accept and incorporate internationally agreed upon human rights norms and those standards and concepts, which are contextually feasible.

(2) The need to reaffirm human rights values

We are at a difficult juncture in the protection of privacy in the digital environment. The contribution of this thesis is to embark on a vigorous reaffirmation of privacy in a contextually sensitive manner. The challenge is to apply principles that have been endorsed internationally and regionally to domestic legislation and practice.

Human rights exist to protect people. Rights place a limitation on states and people, and they impose obligations on how states and people are to act. With the increase in technological change, the growing global economy, and steady inequality between the developed and developing worlds, a degree of alienation of the values underpinning human rights is being witnessed. Protecting rights, including the right to privacy, is essential for people to live with dignity. The reaffirmation – and defence – of human rights is a moral imperative.[1] The full observance of privacy rights should be the norm, with limitations being only the exception.[2] As new technologies have empowered individuals, I argue that rights are now more important than ever. Finally, I agree with the Human Rights Watch report of 2017, which argues that how states protect human rights in the digital age will determine whether the internet is a force that 'liberates or enchains us'.[3]

(3) The South African position

Taking into consideration the virtues of their cultural heritage, their social and historical legacy and the values inherent in African civilisations, inspiration may be drawn from validating African peoples' particular concept of privacy. The position in

---

[1] K Roth 'The dangerous Rise of Populism' (2017) *Human Rights Watch*.

[2] D PoKempner 'The Internet is Not the Enemy: As Rights Move Online, Human Rights Standards Move with Them' World Report (2017) *Human Rights Watch* at 44.

[3] Ibid at 39.

South Africa is thus presented to as an illustration of an approach and its challenges that may be mirrored throughout Africa.

In South Africa, privacy is protected by virtue of the law of delict, by means of a protected right of privacy enshrined in the Constitution, and by provisions in general or specific privacy and/or data protection legislation. These means of protection run concurrently within the legal system and, rather than existing independently, their convergence and mutual interaction can serve to strengthen any consequential privacy protection.

Traditional theories of liability based on delict, although well established in common law privacy protection, may prove deficient when applied to uses of computer technology in eHealth. Reformation and the development of privacy and data protection laws by means of statutory protection that is specifically tailored to safeguard data generated by eHealth endeavours appears to be the most viable solution. Notwithstanding the advancements made by the enactment of the POPI Act, specific privacy protection provisions safeguarding eHealth in South Africa are still described as incomplete, contentious and inadequate. Little accommodation is made with regard to the unique circumstances found in developing countries in drafting such provisions. Neither is any discernable contribution or influence attributed to the wealth of traditional African laws in South Africa, nor is any obvious attempt made to include aspects of African philosophy and ideology.

As the influence of various international law measures has played a role in the drafting of various legislations hinging on human rights, most notably the POPI Act, the measures will most likely be evident in the development of future South African legislative and jurisprudential efforts. As the role of international law has been instrumental in the development of socio-economic jurisprudence since 1994, there should be little reason why it should not be present as a factor in the evolution of further specific human rights jurisprudence, as contained in the Bill of Rights, for instance, with regard to the right to privacy.[4]

---

[4] Confirmation that international law is included among the 'tools of interpretation', which the Court may consider, is Chaskalson J's reference in *S v Makwanyane* at para 35. See further *Government of South Africa and Others v Grootboom and Others,* amongst others, which demonstrate that the provisions of 'soft' international law influenced the guarantees of these rights under the Constitution. Also, see *Residents of Joe Slovo Community, Western Cape v Thubelisha Homes and others*, where the relevance of provisions contained in the ICESCR and in General Comment 7 of the United Nations CESCR is apparent.

The reality is that privacy protection in health care in South Africa is typically fragmented, with inconsistencies found in the various legislations, policies and guidelines. No comprehensive or cohesive national legislative or regulatory standard exists, governing exclusively privacy interests within the eHealth environment or issues arising therefrom, for instance, the practice of eHealth across national jurisdictions. To comply with the requirements in the POPI Act with regard to trans-border data exchanges, companies typically conclude a data transfer agreement, which stipulate the foreign transferee's obligations and any data restrictions.

Organisations, such as the HPCSA, while perfectly positioned to embrace the challenges imposed by new health care technology and proactively provide insightful solutions in its guidelines, have not done so. Currently, the regulatory position has moved from vague, unclearly defined provisions and guidelines, to a bank of drafted guidelines with the sole purpose of specifically governing eHealth and telemedicine initiative. Sadly, guidelines and codes of conduct cannot provide a complete solution, as their authority to regulate and penalise is limited to medical data protection and privacy issues within a small and confined eHealth sector.

Additionally, privacy and data protection, where enacted, is not specific to the health care sector, but is rather part of a general omnibus privacy and data protection legislative regime.[5] Moreover, it is common for a blurring of the boundaries to occur between the different regulations and legislative positions that may apply to eHealth data protection and privacy within a single country or region. In South Africa, for instance, the POPI Act, the National Health Act, the ECT Act and several guidelines all have provisions dealing with particular aspects of medical data protection to various degrees.

Despite data protection legislation being enacted or being in the process of enactment, not all data protection legislation is comparable. While considerable international Human Rights instruments, comprehensive data protection literature and authoritative sets of data protection principles are available to which countries can refer, regrettably, certain data protection measures may be described as narrow and inadequate versions of the full range of data protection principles that are ideally

[5] S Avancha, A Baxi and D Kotz 'Privacy in mobile technology for personal healthcare' (2012) 45 (1) 3 *ACM Computing Surveys* at 3.9.

required. Nevertheless, attempts to address the issues are positive and encouraging and may be an indicator of what is to come.

(4) In summation: The way forward for Africa

There have been considerable research efforts in recent years to create a common repository of reusable eHealth system designs, documents, tools and codes focusing primarily on the standards related to the technical interoperability of health care systems. This has allowed health information systems currently in operation to function as a viable whole. Despite this, little has been done to create a common cohesive repository of international eHealth best practice, regulatory or ethical guidelines, protocols and/or legislations, which could be useful in the governance of data protection, particularly within the field of eHealth in developing regions.

Data protection within eHealth is a challenge that cannot be ignored. The undertaking is to demonstrate how we are to protect the interest in privacy and personal data, where the following factors are present: the emergence of a constantly evolving online and technological environment, the nature of eHealth and its ability to span jurisdictions, and the barriers confronted in a developing world.

The intensification of these factors gives rise to a deeply troubled and compromised data protection position. The starting point for a solution is, firstly, the use of a multi-layered approach, using the best aspects of the many models of data protection already in place. Secondly, a solution is to be found in the adoption of a coherent, regional, African cross-jurisdictional instrument that informs the adoption of an Afro-centric approach in respect of, particularly, issues of consent, data storage and exchange, and regional enforcement. At the centre of such reconstruction, I suggest, exists a range of possibilities, and the provision of exclusively one specific and limited solution is ambitious.

What is needed is a sense of confirmation of, and adoption of, the various helpful aspects already developed in the legislation, and we need to draw on those attractive elements that are of value. Where concepts and measures are inappropriate or where a range of choices exists, it is not necessary to tumble all the way down to the bottom position but rather to find a comfortable, appropriate position somewhere in the middle. Expectations of performance and standards need not be ‘lower’ but may just be ‘different’, depending on the context.

Finally, for our purposes, it is wise to acknowledge that any attempt at data protection integration in Africa will be futile, where there is an unwillingness on the part of African member states to translate their commitments in terms of the provisions of such regional treaty or agreement into clear substantive amendments to their domestic policies, legislation, rules and regulations. Disparities in culture and legal traditions may impede consensus on the details of legal international or regional provisions. Moreover, the passive adherence to inappropriate and imprecise regulations implemented in other parts of the world should not automatically be indicated for Africa. Any recommendation ought to be subjected to constant scrutiny, debate, evolution and re-evaluation.

Where substantial investment into eHealth development has been made, the indication appears to be that the legal frameworks providing concomitant data protection are simultaneously being accelerated. However, this has been largely on a fragmented and reactionary basis.[6] Noteworthy too, is that where privacy legislation is adopted, it is often generic and superficial, with limited provisions addressing the more nuanced data protection requirements that are needed to safeguard the user's privacy rights within a health care environment.[7]

What is required is for African member states to subordinate any immediate national political interests in their commitment to achieve long-term regional data protection objectives and thus to cede elements of sovereignty to a regional institution, such as the AU. This circumventing of the parliamentary function of states in policy creation is not always well received. While initial cooperation may be forthcoming, a danger exists that states may leave policies to atrophy.

Thus, as a general point, multinational international agreements, by their very nature, have limitations. International treaty making is constrained, firstly, by what is politically possible, secondly, by the value of subsidiarity, and lastly, by the need to integrate international laws with diverse domestic legal approaches.

Accordingly, Africa cannot afford to take an isolationist approach. However, the requirements, issues and priorities of the developed world sometimes differ from

---

[6] WHO 'Global Observatory for eHealth' (2006) at 6.

[7] Ibid. See M Wugmeister, K Retzer and C Rich 'Code of Conduct for cross-border data transfers: making the case for corporate privacy rules' (2007) 38 *Georgetown Journal of International Law* at 449.

those pertinent to developing countries. Regulations suitable for the developed world may be incompatible with those relevant in the developing world. The problem in formulating 'international best practices' for the developing world is that it may lead to a further deepening of the 'digital divide' between the developed and the developing world.

III CONCLUSION

To conclude, there are many things to be hopeful about and Africa has made a very promising start in the field of privacy protection in eHealth. In attempting to find a solution, my goal is modest. Achieving an optimal balance between too little and too much protection of privacy is a complex process. The necessary balance implicit in any regulatory framework should take into consideration not only a claim to privacy, but also the desire to provide health care delivery on a vast scale to those most in need, by encouraging innovative methods of eHealth technological development.

What this is alerting us to is that eHealth data protection regulation is in a fragile state of development and that the basic principles of modern health privacy law are not easily determined, nor do they have a particularly strong foundation. Nonetheless, the concession is made that the relationship between the transformation of the eHealth regulatory landscape in safeguarding privacy and data protection and the existing well-established, albeit dated, legal regime is not easily resolved, nor straightforward. The process is not static and requires careful deliberation and debate.

BIBLIOGRAPHY

Primary Sources

Table of Cases

South Africa

Bernstein v Bester (CCT23/95) [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (27 March 1996)

Bhe and others v Khayelitsha Magistrates and others B 2005 (1) SA 580 (CC)

C v Minister of Correctional Services 1996 (4) SA 292 (T)

Financial Mail (Pty) Ltd vs Sage Holdings Ltd 1993 2 SA 453 (SA)

Fose v Minister of Safety and Security 1997 3 SA 786 (CC)

Gosschalk v Rossouw 1966 (2) SA 476 (C)

Government of South Africa and Others v Grootboom and Others (CCT11/00) [2000] ZACC 19; 2001 (1) SA 46; 2000 (11) BCLR 1169

Hoffmann v South African Airways 2001 SA 1 (CC)

Huey Extreme Club v MacDonald t/a Sport Helicopters 2005 (1) SA 485 (C)

Janit v Motor Industry Fund Administrators (Pty) Ltd 1995 (4) SA 293 (A)

Jansen van Vuuren v Kruger 1993 4 SA 842 (A)

Khumalo and Others v Holomisa (CCT53/01) [2002] ZACC 12; 2002 (5) SA 401; 2002 (8) BCLR 771

Mayelane v Ngwenyama and another 2013 (4) SA 415 (CC)

MEC for Education: KwaZulu-Natal and Others v Pillay CCT 51/06 [2007] ZACC 21

MEC for Health, Mpumalanga v M-Net 2002 (6) SA 714 (T)

Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127(CC); 1998 (7) BCLR 880 (CC)

National Media Ltd v Jooste 1996 3 SA 262 (A)

NM and Others v Smith (Freedom of Expression Institute as amicus curiae) 2007 5 SA 250 (CC)

O'Keeffe v Argus Printing and Publishing Co Ltd and Another 1954 (3) SA 224 (C)

Pharmaceutical Manufacturers Association of South Africa ao: In re Ex parte

President of the Republic of South Africa and Others (CCT31/99) [2000] ZACC 1; 2000 (2) SA 674; 2000 (3) BCLR 241 (25 February 2000)
Pretoria Portland Cement Co Ltd v Competition Commission 2003 (2) SA 385 (SCA)
Port Elizabeth Municipality v Various Occupiers (CCT 53/03) [2004] ZACC 7; 2005 (1) SA 217 (CC); 2004 (12) BCLR 1268 (CC)
Reid-Daly v Hickman 1981 (2) SA 315 (ZA) 323
Residents of Joe Slovo Community, Western Cape v Thubelisha Homes and others (CCT 22/08) [2009] ZACC 16; 2009 (9) BCLR 847 (CC); 2010 (3) SA 454 (CC)
S v A 1971 2 SA 293 (T)
S v Makwanyane and another CCT3/94) [1995] ZACC 3; 1995 (6) BCLR 665; 1995 (3) SA 391; [1996] 2 CHRLD 164; 1995 (2) SACR 1
S v Mamabolo (CCT 44/00) [2001] ZACC 17; 2001 (3) SA 409 (CC); 2001 (5) BCLR 449 (CC) (11 April 2001)
S v Orrie 2004 (3) SA 584 (T)
S v Zuma 1995 (2) SALR 642 [15] (CC)
Swanepoel v Minister en Sekuriteit 1999 4 SA 549 (T)
Tshabalala-Msimang v Makhanya 2007-08-30 case no 18656/07 (W)
Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk 1977 (4) SA 376 T; 1979 (1) SA 441 (A).

International

Bavarian Lager v Commission [2007] ECR II-3201 and C-92/09 and C-93/09
Chester v Afshar [2004] UKHL 41
Entick v Carrington 1558-1774 All ER Report 45
Olmstead v United States 277 US 438, 478 (1928)
Mackenzie v Soden Mineral Springs Co 27 Abb N Cas 402 18 NYS 240 (Sup Ct 1891)
Manola v Stevens (NY Sup Ct 1890)
Marks v Jaffa 6 Misc 290 26 NYS 908 (super ct NY City 1893;
Maximillian Schrems v Data Protection Commissioner and Digital Rights Ireland Limited (Case C-362/14)
Roberson v Rochester Folding Cox Co 171 NY 538 64 NE 442 (1902)
Roe v Wade 410 U.S. 113 (1973)
Schuyler v Curtis 147 NY 434 42 NE 22 (1895)

Volker und Markus Schecke and Hartmut Eifert [*2010] ECR I-11063*

South African Statutes

Constitution of the Republic of South Africa, 1996
Electronic Communications and Transactions Act No. 25 of 2002
Health Professions Act No. 56 of 1974
National Health Act No. 61 of 2003
Promotion of Access to Information Act No.2 of 2000
Protection of Personal Information Act No. 4 of 2013

International treaties and declarations

African Charter on Human and People's Rights (1981) *Organisation of African Unity* Doc Cab/Leg/67/3 rev.5 21 I.L.M. 58 (1982).

African Charter on the Rights and Welfare of the Child (1990) *Organisation of African Unity*.

Arab Charter on Human Rights (2004) *League of Arab States*.

Convention on Cyber Security and Personal Data Protection (2014) *African Union*.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 23.11 (1995) 31-50.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178 (2000) 1-16.

Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare OJ L 88 4.4 (2011) 45-65.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201 31.7 (2002) 37-47.

Guidelines on the Protection of Privacy and Transborder of Personal Data (1980) *OECD*. Available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (accessed 23 January 2017).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119 4.5 (2016) 1-88.

Universal Declaration on Bioethics and Human Rights (2005) *UN General Assembly*.

Universal Declaration of Human Rights (1948) *UN General Assembly*.

United Nations International Covenant on Civil and Political Rights (1976).

United Nations International Covenant on Economic, Social and Cultural Rights. (1976).

Policy documents / reports and internet sources

'A Telemedicine Strategy for South Africa 2010 - 2015 Extending Better Health care' (2010) Version 3 *National e-Health Steering Committee*.

'Accelerating the Development of the eHealth Market in Europe' (2007) *European Union eHealth Taskforce Report* 1.

'Africa: The Impact of Mobile Phones' (2005) *Vodafone Policy Paper Series Number 2* 1.

'An online Magna Carta: Berners-Lee calls for bill of rights for web' (2014) *The Guardian.* Available at https://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web (accessed on 18 February 2017).

Article 29 Data Protection Working Party Opinion 8/2014 on the Recent Developments on the Internet of Things (2014).

'Barriers prevent Indonesian women from achieving reproductive health' (2010) *Amnesty International.* Available at https://www.amnesty.org/en/press-releases/2010/11/19361/ (accessed 24 February 2017).

'Chinese Supreme People's Court Issues Interpretations Regarding the Publication of Personal Information on the Internet' (2014) *Privacy and Information Security Law Blog.* Available at https://www.huntonprivacyblog.com/2014/10/articles/chinese-supreme-peoples-court-issues-interpretations-regarding-publication-personal-information-Internet/ (accessed 24 October 2016).

'Cloud infrastructure providers unveil ground-breaking data protection Code of Conduct' (2016) *CISPE press release*.

'Code of Conduct on privacy for mHealth apps has been finalised' (2016). Available at https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised (accessed 21 February 2017).

'Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy' (2012) *The White House*.

‘Communication from the Commission to the European Parliament on telemedicine for the benefit of patients, health care systems and society’ (2008) *Commission of the European Communities*. Available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0689:FIN:EN:PDF (accessed 30 January 2017).

'Criminal Laws on Homosexuality in African Nations' (2014) *Global Legal Research Directorate Law Library of Congress.* Available at https://www.loc.gov/law/help/criminal-laws-on-homosexuality/homosexuality-laws-in-african-nations.pdf (accessed 20 February 2017).

‘Cyberchondriacs on the Rise?’ (2012) *Harris Interactive*. Available at http://www.harrisinteractive.com/vault/HI-Harris-Poll-Cyberchrondriacs-2010-08-04.pdf (accessed 30 January 2017).

'Data Protection Code of Conduct for Cloud Service Providers' (2015) *EU Digital Single Market*.

Diabetes SA. Available at www.diabetessa.co.za (accessed 12 December 2016).

‘East African Legislative Assembly Report of the Committee on communications, trade and investments on the on-spot assessment of regional cooperation in ICT’ (2013) *East African Community*.

'ECJ rules that the EU-US Safe Harbor arrangement is invalid' (2015) *Practical Law*. Available at http://uk.practicallaw.com/5-619-2986#null (accessed 21 February 2017).

'Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations' (2010) *Policy Engagement Network for the International Development Research Centre* 15.

‘EU-US Privacy Shield’ (2016). Available at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf (accessed 20 February 2017).

‘EU-US Privacy Shield draft adequacy decision’ (2016) *European Data Protection Supervisor Opinion*. Available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf (accessed 17 February 2017).

European Data Protection Supervisor Press Release EDPS/2016/11 (2016). Available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf (accessed 21 February 2017).

‘Final Version of NIST Cloud Computing Definition Published’ (2011). Available at http://www.nist.gov/itl/csd/cloud-102511.cfm (accessed 21 February 2017).

'Green Paper on mHealth' (2014) *European Commission* 1. Available at https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth (accessed 24 February 2017).

Guidelines - core standards for telemedicine operations (2007) American Telemedicine Association. Available at www.ict-ageing.eu/?page_id=1291 (accessed 18 February 2017).

'Health Fact Sheet' *Pew Research Center’s Internet & American Life Project*. Available at http://www.pewinternet.org/fact-sheets/health-fact-sheet/ (accessed 13 January 2017).

Heart Foundation SA. Available at http://www.heartfoundation.co.za (accessed 24 February 2017).

HPCSA 'HPCSA condemns unethical telemedicine practice' (2011).

HPCSA *Confidentiality: protecting and providing Information* 2nd ed. Booklet 11 (2007).

HPCSA *General Ethical Guidelines for the Health care professions* Booklet 1 May (2008).

HPSCA *Draft document of the Human Rights, Ethics and Professional Practice Committee of the Health Professions Council of South Africa* (2008).

'Human Rights in Danger: What is happening to Human Rights in the World' (2017) *Human Rights Watch* at 1. Available at https://www.hrw.org/sites/default/files/supporting_resources/hrw_world_report_etr_final_0.pdf (accessed 27 January 2017).

'Leveraging Mobile Health Technology for Patient Recruitment: an emerging opportunity' (2012) *Blue Chip Patient Recruitment* 1.

'Maternal messaging & mHealth programmes: Empowering and enabling decision makers to include mHealth services into their budgets' (2014) *Deloitte*/*GSMA*. Available at http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/12/GSMA-mHealth-Programme-high-resolution.pdf (accessed 18 January 2017).

'Mobile Health: Reconciling technological innovation with Data Protection' (2015) *European Data Protection Supervisor Opinion 1/2015*. Available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-05-21_Mhealth_EN.pdf (accessed 21 February 2017).

'Mobile Technology: text messages for better reproductive health' (2012) *Family Health International*.

'Mobile trends in Sub-Saharan Africa' *GSMA Intelligence.*

'Model Contract clauses - International transfers of personal data' (2012) *Information Commissioners Office*.

'New Global eHealth Ambassador Appointed' (2014) *eHealth News South Africa*. Available at http://ehealthnews.co.za/news/new-global-ehealth-ambassador-appointed/ (accessed 21 January 2017).

'Nokia unveils two handsets that offer a range of useful features and colours aimed at consumers in emerging markets' (2008). Available at http://company.nokia.com/en/news/press-releases/2008/01/22/nokia-unveils-two-handsets-that-offer-a-range-of-useful-features-and-colours-aimed-at-consumers-in-emerging-markets (accessed 3 January 2017).

'Patient Privacy in a Mobile World A framework to address privacy law issues in mobile health' (2013) *mHealth Alliance*. Available at www.mhealthalliance.org/images/content/trustlaw_connect_report.pdf (accessed 22 January 2017).

'Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)' (1998) *European Commission Opinion 1/98*. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp11_en.pdf (accessed 10 December 2016).

'Power to the patient: How mobile technology is transforming healthcare' (2015) *The Economist Intelligence Unit Limited* 1. Available at http://www.economistinsights.com/sites/default/files/HowMobileisTransformingHealthcare.pdf (accessed 22 February 2017).

'Progress on EU data protection reform now irreversible following European Parliament vote' (2014) *European Commission Memo*. Available at http://europa.eu/rapid/press-release_MEMO-14-186_en.htm (accessed on 20 February 2017).

'Proposal for a Regulation 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' (2012) *European Commission*. Available at http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf (accessed 21 February 2017).

'Proposed International Guidelines for Biomedical Research Involving Human Subjects' (1982) *Council for International Organizations of Medical Sciences and the World Health Organization*.

'Redesigning health in Europe for 2020' (2012) *European Union eHealth Taskforce Report* 1.

'Reforming healthcare in South Africa' Report 18 (2011) *Centre for Development and Enterprise* 1. Available at http://www.cde.org.za/reforming-healthcare-in-south-africa-what-role-for-the-private-sector/ (accessed 10 October 2016).

'Socio-economic impact of mHealth: An assessment report for the European Union' (2013) *PwC*. Available at http://www.gsma.com/connectedliving/wp-content/uploads/2013/06/Socio-economic_impact-of-mHealth_EU_14062013V2.pdf (accessed 12 December 2016).

South African Department of Health *Developed countries making huge savings through recruitment from Africa* (2008).

South African Department of Health *National e-Health Strategy South Africa 2012 - 2016* (2012). Available at http://www.hst.org.za/sites/default/files/eHealth_Strategy_South_Africa_2012-2016.pdf (accessed 26 January 2017).

South African Department of Health *e-Health Programme Plan Enabling Better Health care through Better Information* (2009).

South African Department of Health *National Tuberculosis Management Guidelines* (2008).

South African Law Reform Commission 'Privacy and Data Protection' Discussion paper 109 Project 124 (2005). Available at http://www.justice.gov.za/salrc/dpapers/dp109.pdf (accessed 22 February 2017).

South African Law Reform Commission 'Privacy and Data Protection Report' Project 124 (2009).

'Special Eurobarometer 359 - Attitudes on Data Protection and Electronic Identity in the European Union' (2011). Available at http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (accessed on 22 February 2017).

Statement of the Article 29 Working Party on the Opinion on the EU-US Privacy Shield (2013). Available at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf (accessed 22 February 2017).

Statistics South Africa, Key Results (2001).

'Sub-Saharan Africa Mobile Observatory' (2012) *GSMA/Deloitte*. Available at http://www.gsma.com/publicpolicy/wp-content/uploads/2013/01/gsma_ssamo_full_web_11_12-1.pdf (assessed 23 January 2017).

'Summary Report: Study on Regulatory Aspects of eHealth' (2013) *Greenfield Management Solutions*. Available at http://www.greenfield.org.za/downloads/eHSA%20Reg%20Study%20Summary%20Report.pdf (accessed on 17 January 2017).

'The Mobile Economy: Africa 2016' (2016) *GSMA* 1.

TRUSTe 2013 Great Britain - Consumer Confidence Privacy Report. Available at http://www.truste.com/great-britain-consumer-confidence-index-2013/ (accessed 11 November 2016).

UNAIDS ‘Global Aids Epidemic’ (2012).

UNCTAD ‘Harmonizing Cyberlaws and Regulations: The experience of the East African Community’ (2012).

UNESCO Division of Ethics of Science and Technology. Guide No. 3 *Educating Bioethics Committees* (2007).

UNICEF ‘African Mobile Observatory 2011: Driving Economic and Social Development through Mobile Services’ (2011).

World Bank 'Information and communications for development: maximizing mobile' (2012). Available at http://www.worldbank.org/ict/IC4D2012 (accessed 22 February 2017).

World Bank 'Infrastructure in Latin America: Recent Developments and Key Challenges' (2005) 1.

WHO ‘Ebola Situation Reports’ (2015). Available at http://www.who.int/csr/disease/ebola/situation-reports/en/ (accessed 22 February 2017).

WHO 'From innovation to implementation - eHealth in the WHO European Region' (2016). Available at http://www.thehealthwell.info/node/975721 (accessed on 22 February 2017).

WHO 'Global Observatory for e-health' (2006).

WHO ‘Legal framework for e-health' in *Global Observatory for eHealth Series* vol. 5 (2012). Available at

http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf/ (accessed 22 February 2017).

WHO 'mHealth: New horizons for health through mobile technologies' in the second *Global Observatory for eHealth Series* vol. 3 (2011). Available at http://www.who.int/goe/publications/goe_mhealth_web.pdf (accessed 18 January 2017).

WHO 'Safety and security on the Internet: challenges and advances in Member States' in *Global Observatory for eHealth Series* vol. 4 (2011). Available at http://www.who.int/goe/publications/ehealth_series_vol4/ (accessed 27 January 2017).

WHO 'Telemedicine - Opportunities and developments in Member States' (2010) 2 *Global Observatory for e-Health series*. Available at http://www.who.int/goe/publications/goe_telemedicine_2010.pdf (accessed 21 February 2017).

WHO 'The bigger picture for e-health' (2012) 90 (5) *Bulletin of the World Health Organization* 321-400.

WHO 'World Health Statistics 2012' (2012).

WHO ‘WHA58.28 e-health’ (2005).

WMA ‘Statement on the Professional and Ethical Use of Social Media’ (2011).

WMA 'Statement on Guiding Principles for the Use of Telehealth for the Provision of Health Care' (2009).

Secondary Sources

A

AS Adeniyi ‘The need for data protection law in Nigeria’ (2012) *Communications and IT Law* 1. Available at http://adeadeniyi.wordpress.com/2012/07/18/the-need-for-data-protection-law-in-nigeria-2/ (accessed 21 February 2017).

AO Adesina, KK Agbele, K Kehinde, R Februarie, AP Abidoye and HO Nyongesa 'Ensuring the security and privacy of information in mobile health-care communication systems' (2011) 107 (9-10) *South African Journal of Science* 1.

V Afshar 'How Google Glass will transform healthcare' (2015) *Huff Post Tech*. Available at http://www.huffingtonpost.com/vala-afshar/how-google-glass-will-tra_b_6003100.html (accessed 30 January 2017).

JC Aker and IM Mbiti 'Mobile Phones and Economic Development in Africa' (2010) 24 (3) *Journal of Economic Perspectives* 207-232.

AL Allen 'Privacy and Medicine' in EN Zalta (ed.) *The Stanford Encyclopedia of Philosophy* (2011). Available at http://plato.stanford.edu/archives/spr2011/entries/privacy-medicine/ (accessed 22 February 2017).

AL Allen 'Privacy in Health Care' in SG Post (ed.) *Encyclopedia of Bioethics* 3 ed. (2004).

M Alliot 'Un droit nouveau est-il en train de naitre en Afrique?' [Is a new law appearing in Africa?] in Kuyu (ed.) *Le Droit et le Service Public* 193.

AN Allott 'Towards the unification of laws in Africa' (1965) 14 (2) *The International and Comparative Law Quarterly* at 366.

AN Allott 'What is to be done with African customary Law?' (1984) 28 (1-2) *Journal of African Law* at 57.

I Altman ‘Privacy regulation: Culturally universal or culturally specific?’ (1977) 33 (3) *Journal of Social Issues* 66.

CT Andoh 'Bioethics and the challenges to its growth in Africa' (2011) 1 (2) *Open Journal of Philosophy* 67-75.

M Armbrust, A Fox, R Griffith, AD Joseph, R Katz, A Konwinski, G Lee, D Patterson, A Rabkin, I Stoica and M Zaharia 'A view of cloud computing' (2010) 53 (4) *Communications of the ACM* 50-58.

E Ashley, S Israni and L Minor 'Data science and the practice of modern medicine' (2014) 1 (9) *eHealthlaw&policy*. Available at http://www.e-comlaw.com/ehealth-law-and-policy/article_template.asp?ID=110 (accessed 18 October 2017).

S Avancha, A Baxi and D Kotz 'Privacy in mobile technology for personal healthcare' (2012) 45 (1) 3 *ACM Computing Surveys* at 3.1 and 3.8.

IM Azmi ‘E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill’ (2002) 16 (3) *International Review of Law, Computers & Technology* 317.

B

D Banisar 'Linking ICTs, the right to privacy, freedom of expression and access to information' (2010) 16 (1) *East African Journal of peace and human rights* 124-154.

D Banisar and S Davies 'Global Trends in Privacy Protection: An international survey of privacy, data protection, and surveillance laws and development' (2012) 18 (1) *John Marshall Journal of Computer & Information Law.*

D Banisar and S Davies 'Privacy and Human Rights: An International Survey of Privacy Laws and Practice' *Global Internet Liberty Campaign*. Available at http://gilc.org/privacy/survey/intro.html (accessed 10 December 2016).

A Banjo 'The ECOWAS Court and the Politics of Access to Justice in West Africa' (2007) 32 (1) *CODESRIA Africa Development*.

AT Baptist, M Thompson, KS Grossman, L Mohammed, A Sy and GM Sanders 'Social Media, Text Messaging and Email preferences of Asthma patients between 12 and 40 years old' (2011) Oct 48 (8) *J Asthma* 824.

E Barclay 'Text messages could hasten tuberculosis drug compliance' (2009) 373 *The Lancet* 15-16.

SB Barnes 'A privacy paradox: Social networking in the United States' (2006) 11 (9) *First Monday*.

M Barry 'Ethical considerations of human investigation in developing countries: the AIDS dilemma' (1988) 319 *The New England Journal of Medicine* 1083-1086.

S Basu 'Policy-Making Technology and Privacy in India' (2010) 6 *The Indian Journal of Law and Technology* 65-88.

C Bateman 'Cutting-edge telemedicine venture freezes as official bodies frown' (2011) 10 (6) *SAMJ* 368.

TL Beauchamp & JF Childress *Principles of Biomedical Ethics* 6 ed. (2008).

KG Behrens 'Towards an indigenous African bioethics' (2013) 6 (1) *S Afr J BL* 32-35.

F Bélanger and RE Crossler 'Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems' (2011) 35 (4) *MIS Quarterly* at 1017-1041.

S Bellman, EJ Johnson, SJ Kobrin and GL Lohse 'International differences in information privacy concerns: a global survey of consumers' (2004) 20 (5) *Information Society* 313-324.

S Benetar, AS Daar & P Singer 'Global health ethics: the rationale for mutual caring' in S Benatar & G Brock (eds.) *Global health and global health ethics* (2011) 129-140.

S Benhabib *Another Cosmopolitanism* (2008).

CJ Bennett *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (1992).

CJ Bennett 'What Government Should Know about Privacy: A Foundation Paper' (2001) Paper prepared for the Information Technology Executive Leadership Council's Privacy Conference.

C Bennett & C Raab *The Governance of Privacy: Policy instruments in Global perspective* (2006).

TW Bennett & J Strug *Introduction to International Law* (2013).

B Berendt, O Gunther, and S Spiekermann 'Privacy in e-commerce: stated preferences vs. actual behavior' (2005) 48 (4) *Communications of the ACM* 101-106.

KP Berger 'The Law Merchant and the New Market Place: 21st Century view of transnational commercial law' (2000) *International Arbitration Law Review*.

PS Berman 'The New Legal Pluralism' (2009) 5 *Annual Review of Law and Social Science* 225-242.

PA Bernal 'Web 2.5: The Symbiotic Web' (2010) 24 (1) *International Review of Law Computers & Technology*.

R Berry and M Reisman 'Policy challenges of cross-border cloud computing' (2012) 4 (2) *Journal of International Commerce and Economics* 1-38.

JM Berry *The Interest Group Society* (1989).

N Bhagwandin 'Health Technology for equitable access to quality health services' (2011) 8 *SAHR* 96.

N Biggar 'Why religion deserves a place in secular medicine' (2015) 41 *J Med Ethics* 229-233.

S Biko *I Write What I Like* (2004).

MD Birnhack 'The EU Data Protection Directive: An engine of a global regime' (2008) 24 *Computer Law and Security Report*.

MD Birnhack and N Elkin-Koren 'Does Law Matter Online? Empirical Evidence on Privacy Law Compliance' (2011) *Mich. Telecomm Tech Law Rev*iew at 337.

JA Blaya, HSF Fraser and B Holt 'EHealth technologies show promise in developing countries' (2010) 29 (2) *Health Affairs* 244-251.

JD Blum 'The role of law in Global e-health: A tool for development and equity in a digitally divided world' (2002) *Saint Louis University Law Journal*.

F Boehm 'Regulatory Capture Revisited - Lessons from Economics of Corruption' Working paper (2007).

GT Bosslet 'Commentary: The Good, the Bad, and the Ugly of Social Media' (2011) 18 *Academic Emergency Medicine* 1221.

GT Bosslet, AM Torke, SE Hickman, CL Terry and PR Helft 'The patient-doctor relationship and online social networks: results of a national survey' (2011) 26 *J Gen Intern Med* 168.

ME Boulding 'Perspective: Self-Regulation: Who Needs It?' (2000) 19 (6) *Health Affairs* 133-139.

CA Bradley 'Breard, Our Dualist Constitution and the Internationalist Conception' (1999) 51 *Stanford Law Review*.

D Brin *The Transparent Society: will technology force us to choose between privacy and freedom?* (1998).

I Brown 'Comparative study on the different approaches to new privacy challenges in particular in the light of technological developments' (2010) *European Commission Directorate General Justice, Freedom and Security.* Available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf (accessed 22 February 2017).

A Brysk *From tribal village to global village: Indian rights and international relations in Latin America* (2000).

J Burchell 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' (2009) 13 (1) *Electronic Journal of Comparative Law* 1.

SE Burke *The doctor-patient relationship: An exploration of trainee doctors' views'* (PhD Thesis University of Birmingham) (2008) 1.

M Bury 'Researching patient-professional interactions' (2004) 9 (Suppl. 1) *Journal of Health Services Research and Policy* 48.

LA Bygrave *Data protection law: approaching its rationale, logic and limits* (2002).

LA Bygrave 'Data Protection pursuant to the right to privacy in human rights treaties' (1998) 6 (3) *International Journal of Law and Information Technology*.

LA Bygrave ‘Minding the machine: Article 15 of the EC data protection directive and automated profiling’ (2001) 17 *Computer Law & Security Report*.

LA Bygrave ‘Privacy and Data Protection in an International Perspective’ (2010) *Stockholm Institute for Scandinavian Law* 165.

LA Bygrave ‘The place of privacy in data protection law’ (2001) 24 (1) *UNSW Law Journal*.

C

S Callens and K Cierkens 'Legal aspects of eHealth' (2008) 141 *Stud Health Technol Inform* 47-56.

GP Calliess 'Reflexive Transnational Law: The privatization of civil law and the Civilisation of private law (2002) 23 *Zeitschrift fur Rechtssoziologie* 185-216.

WJPM Calis and PHM Mulder ‘Dokter.nl Digital Consultation’ (2006) *Med-e-Tel* 85.

S Cameron 'Q&A: The US big data report and fully utilising big data within healthcare' *eHealth Law & Policy* Available at http://www.e-comlaw.com/ehealth-law-and-policy/ (accessed 3 December 2016).

JA Cannataci ‘Privacy, Technology Law and Religions across Cultures’ (2009) 1 *Journal of Information, Law & Technology*.

MM Carauna and JA Cannataci ‘European Union Privacy and Data Protection Principles: Compatibility with Culture and Legal Frameworks in Islamic States’ (2007) 16 (2) *Information & Communications Technology Law* 99-124.

BM Carson 'Legally speaking - Warren, Brandeis and the creation of the legal concept of privacy' (2008) 20 (2) *Against the Grain*.

E Carolan ‘The continuing problems with online consent under the EU’s emerging data protection principles’ (2013) 32 *Computer Law & Security Review* 462-473.

FH Cate 'The EU Data Protection Directive, Information Privacy, and the Public Interest' (1994-95) 80 *Iowa Law Review* 431.

M Chanock ‘Human Rights and Cultural Branding: Who Speaks and How?’ in A An-Naim *Cultural Transformation and Human Rights in Africa* (2002).

M Chaskalson, J Kentridge, J Klaaren, G Marcus, D Spitz & S Woolman *Constitutional Law of South Africa* (2002).

FS Chilapowski ‘The Constitutional Protection of Informational Privacy’ (1991) 71 *Boston University Law Review* 133.

JF Childress and M Siegler 'Metaphors and Models of Doctor-Patient Relationships. Their Implications for Autonomy' (1984) 5 *Theoretical Med and Bioethics* 22.

N Chomsky *Profit Over People: Neoliberalism and Global Order* (2011).

S Choudhury, JR Fishman, ML McGowan and ET Juengst 'Big data, open science and the brain: Lessons learned from genomics' (2014) 8 *Frontiers in Human Neuroscience* 1.

T Chowles 'IBM launches Ebola eHealth solutions' (2014) *eHealth News.* Available at http://ehealthnews.co.za/news/ibm-ebola/ (accessed 28 January 2017).

NA Christakis 'The ethical design of and AIDS vaccine trial in Africa' (1988) *The Hastings Center Report* 31.

RH Christie *The Law of Contract* (2001).

L Cilliers and SV Flowerday ‘Health information systems to improve health care: A telemedicine case study’ (2013) 15 (1) *SA Journal of Information Management* 1-5.

E Clark and G Cho ‘Privacy in an e-business world: A question of balance’ (2001) 11 (1) *Journal of law, information and science* 7.

R Clarke ‘Internet privacy concerns confirm the case for intervention’ (1999) 42 (2) *Communication of the ACM* 64.

RJW Cline and KM Haynes ‘Consumer health information seeking on the Internet: the state of the art’ (2001) 16 (6) *Health Educ Research* 671.

S Cockcroft, N Sandhu and A Norris 'How does national culture affect citizens’ rights of access to personal health information and informed consent?' (2009) 15 (3) *Health Informatics Journal* 229-243.

D Collier ‘Email and SMS contracts’ (2008) 16 (1) *Juta’s Business Law* 20.

G Collste ‘Global ICT-ethics: the case of privacy’ (2008) 6 (1) *Journal of Information, Communication & Ethics in Society* 79.

J Comaroff & S Roberts *Rules and Processes: The Cultural Logic of Dispute in an African Context* (1981).

K Congdon 'The rise of mHealth' (2013) *Health IT Outcomes.*

H Coovadia, R Jewkes, P Barron, D Sanders and D McIntyre 'The health and health system of South Africa: historical roots of current public health challenges' (2009) 374 (9692) *The Lancet* 817-834. Available at http://dx.doi.org/10.1016/S0140-6736(09)60951-X (accessed 28 January 2017).

D Cornell 'A call for a nuanced constitutional jurisprudence: Ubuntu, dignity and reconciliation' (2004) 19 *SA Public Law: Public law in transformation : Special Edition III* 666-675.

SR Cotten and SS Gupta ‘Characteristics of online and offline health information seekers and factors that discriminate between them’ (2004) 59 *Social Science & Medicine* 1795.

A Coulter ‘Paternalism or partnership? Patients have grown up and there’s no going back’ (1999) 319 *BMJ* 719.

RM Cover 'The Folktales of Justice: Tales of Jurisdiction' (1985) *Yale Law School Legal Scholarship Repository*: *Faculty Scholarship Series Paper 2706* at 181. Available at http://digitalcommons.law.yale.edu/fss_papers/2706 (accessed 22 February 2017).

C Cuijpers 'A private law approach to privacy; mandatory law obliged?’ (2007) 4 (4) *SCRIPT-ed* 304.

L Curren and J Kaye 'Revoking consent: A blind spot in data protection law?' (2010) 26 *Computer Law & Security Review* 273-283.

D

DN Dagbanja 'Privacy in Context: The right to privacy, and freedom and independence of the media under the constitution of Ghana' (2014) 22 (1) *African Journal of International and Comparative Law* 40-62.

C Dario, A Dunbar, F Feliciani, M Garcia-Barbero, S Giovannetti, G Graschew, P Mancini, MTJ Mohr, P Ortiz García, S Pedersen, JM Pérez-Sastre and A Rey ‘Opportunities and Challenges of Ehealth and Telemedicine via Satellite’ (2004) *Eur J Med Res Supplement*. Available at http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.469.3233 (accessed 24 February 2017).

SG Davies 'Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity' in Agre & Rotenberg (eds.) *Technology and Privacy : the new landscape* (1997) 143.

DM Davis ‘Constitutional borrowing: The influence of legal culture and local history in the reconstitution of comparative influence: The South African experience’ (2003) 1 (2) *Oxford University Press and the New York University School of Law* 181.

J DeCew ‘Privacy’ in EN Zalta (ed.) *The Stanford Encyclopedia of Philosophy* (2013). Available at http://plato.stanford.edu/archives/fall2013/entries/privacy/ (accessed 20 February 2017).

P de Hert and V Papakonstantinou ‘The new General Data Protection Regulation: Still a sound system for the protection of individuals?’ (2016) 32 *Computer Law & Security Review* 179-194.

P de Hert and V Papakonstantinou 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?' (2013) 9 (2) *I/S: A Journal of Law and Policy for the Information Society* 272.

E Del Bo 'Regulatory capture: A review' (2006) 22 (2) *Oxford Review of Economic Policy* 203.

GE Devenish ‘The Limitation Clause Revisited - The Limitation of Rights in the 1996 Constitution’ (1998) *Obiter* 256.

B de Sousa Santos & CA Rodriguez-Garavito *Law and Globalization from Below: Towards a Cosmopolitan Legality* (2005).

J De Waal, I Currie & G Erasmus *The Bill of Rights Handbook* (2000).

J Dugard *International Law: A South African Perspective* (2011).

J Dwyer 'Global health and justice' (2005) 19 (5-6) *Bioethics* 460-475.

E

JB Earp, AI Anton, L Aiman-Smith and WH Stufflebeam 'Examining internet privacy policies within the context of user privacy values' (2005) 52 (2) *IEEE Transactions on Engineering Management* 227-237.

FH Easterbrook ‘Cyberspace and the Law of the Horse’ (1996) *University of Chicago Law Forum* 207.

C Eberhard 'Towards an Intercultural legal theory: The dialogical challenge' (2001) 10 *Social and Legal Studies* 171.

WA Edmundson 'Privacy' in Golding & Edmundson (eds.) *The Blackwell Guide to the Philosophy of Law and Legal Theory* (2005) 271.

SM Edworthy 'Telemedicine in developing countries' (2001) 323 (7312) *BMJ* 524-525.

KE Edison, DA Fleming H and Pak ‘Telehealth ethics’ (2009) 15 (8) *Telemedicine and e-health* 797.

E Edouard and L Edouard 'Application of information and communication technology for scaling up youth sexual and reproductive health' (2012) 16 (2) *African Journal of Reproductive Health* 197.

L Edwards 'Consumer Privacy, On-Line Business and the Internet: Looking for Privacy in all the Wrong Places' (2003) 11 (3) I*nternational Journal of Law and Information Technology* 226-250.

L Edwards 'Privacy and Data Protection Online: The Laws Don't Work?' in *Law and the Internet* L Edwards & C Waelde (eds.) 3rd ed. (2009) 443-488.

E Ehrlich *Principles of the Sociology* (1936).

EO Ekunwe and R Kessel 'Informed consent in the developing world' (1984) 14 (3) *Hastings Cent Rep* 22-24.

R Elangovan and S Arulchelvan 'A Study on the Role of Mobile Phone Communication in Tuberculosis DOTS Treatment' (2013) 38 (4) *Indian J Community Med* 229-233.

D Elbourne, C Snowdon and J Garcia 'Informed consent. Subjects may not understand concept of clinical trials' (1997) 315 (7102) *British Medical Journal* 248-249.

C Erwell 'Telemedicine: overcoming obstacles on the road to global health care' (2003) *International Trade Law Journal* 68.

SE Estroff and RL Walker 'Confidentiality: concealing "things shameful to be spoken about"' (2012) 14 (9) *Virtual Mentor* 733-737.

SD Esposti 'When big data meets dataveillance: the hidden side of analytics' (2014) 12 (2) *Surveillance and Society* 209.

G Eysenbach 'Towards ethical guidelines for dealing with unsolicited patient emails and giving teleadvice in the absence of a pre-existing patient-physician relationship systematic review and expert survey' (2000) Feb 24 *J Med Internet Res*. Available at http://www.jmir.org/2000/1/e1/ (accessed 22 February2017) .

G Eysenbach 'What is e-health?' (2001) 3 (2) *Journal of Medical Internet Research* e20.

G Eysenbach and C Köhler 'Health-related searches on the Internet' (2004) 291 (24) *J Am Med Assoc* 2946.

G Eysenbach and C Kohler 'How do consumers search for and appraise health information on the World Wide Web? Qualitative study using focus groups, usability tests, and in-depth interviews' (2002) 324 (7337) *BMJ* 573.

G Eysenbach, E Ryoung Sa and TL Diepgen ‘Shopping around the internet today and tomorrow: towards the millennium of cybermedicine’ (1999) 319 (7220) *BMJ* 1294.

F

F Fanon *Black Skins, White Masks* (1967).

F Fanon *Wretched of the Earth* (1961).

N Ferraud-Ciandet 'Privacy and data protection in eHealth: A comparative approach between South African and French legal systems' (2010) *IST-Africa* 1-10.

JJ Flinn 'Personalizing Informed Consent: The Challenge of Health Literacy' (2008) *Louis UJ Health Law and Policy* 379.

L Floridi 'Big data and their epistemological challenge' (2012) 25 (4) *Philosophy & Technology* 435-437.

L Floridi *Protection of Information and the Right to Privacy - A New Equilibrium?* (2014) 89.

R Friedberg ‘Is Telemedicine a Fundamentally Different Way of Practicing Medicine?’ (2012). Available at http://www.techhealthperspectives.com/2012/06/06/is-telemedicine-a-fundamentally-different-way-of-practicing-medicine/ (accessed 21 February 2017).

N Friederici, C Hullin & M Yamamichi 'Chapter 3: mHealth' in T Kelly (ed.*) Information and Communications for Development 2012 - Maximizing Mobile* (2012). Available at http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/IC4D-2012-Chapter-3.pdf (accessed 24 January 2017).

AM Froomkin 'Empire strikes back' (1997-1998) 73 *Chicago-Kent Law Review* 1101.

AM Froomkin 'The Death of Privacy?' (2000) 52 (5) *Stanford Law Review* 1461-1543.

AM Froomkin 'The Internet as a source of Regulatory Arbitrage' in *Borders in Cyberspace* B Kahin & C Nesson (eds.) (1997) 129.

S Fox and M Duggan 'Information Triage' (2013) *Pew Research Center's Internet & American Life Project.*

S Fox and L Rainie 'The online health care revolution' *Pew Internet & American Life Project: Online Report* (2000).

B Futter 'The naked patient' (2012) 79 (9) *South African Pharmaceutical Journal* 64.

G

D Gatherer 'The 2014 Ebola virus disease outbreak in West Africa' (2014) 95 *Journal of General Virology* 1619.

T Gerber, V Olazabal, K Brown and A Pablos-Mendez 'An Agenda For Action On Global E-Health' (2010) 29 (2) *Health Affairs* 233.

A Geissbuhler, C Safran, I Buchan, R Bellazzi, S Labkoff, K Eilenberg, A Leese, C Richardson, J Mantas, P Murray and G De Moor 'Trustworthy reuse of health data: A transnational perspective' (2013) 82 (1) *International Journal of Medical Informatics* 1-9.

T Gidron 'Publication of private information: an examination of the right to privacy from a comparative perspective (part 2)' (2010) 2 *Tydskryf vir die Suid-Afrikaanse Reg* 270-287.

R Gittleman 'The African Charter on Human and Peoples' Rights: A legal Analysis' (1982) 22 (4) *Virginia Journal of International Law* 667.

I Goldberg, A Hill and A Shostack 'Trust, Ethics and Privacy' (2001) 81 *Boston University Law Review* 101-116.

J Goldman "Health at the Heart of Files?" Brandeis Lecture delivered at the Massachusettes Health Data Consortium's Annual Meeting and made available at the 23rd International Conference of Data Protection Commissioners in Paris in 24-26 September 2001.

J Goldman and Z Hudson 'Virtually exposed: Privacy and e-Health' (2000) 19 (6) *Health Affairs* 140.

MM Goldstein 'Health Information Technology and the Idea of Informed Consent' (2010) 38 *Journal of Law, Medicine and Ethics* 27-35.

G González Fuster *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (2014) 56.

C Gowar and CJ Visser 'Distinguishing between Dignity, Identity and Privacy: Is it Really Necessary? Kumalo V Cycle Lab (Pty) Ltd (31871/2008) [2011] ZAGPJHC 56' (2012) 75 *Journal of Contemporary Roman-Dutch Law* 154.

C Grady 'Enduring and Emerging Challenges of Informed Consent' (2015) 372 *New Engl J Med* 855-862.

DA Grandinetti 'Doctors and the Web: help your patients surf the Net safely' (2000) 4 *Medical Economics* 28. Available at http://www.ncbi.nlm.nih.gov/pubmed/10848409 (accessed 25 January 2017).

E Grant 'Human rights, cultural diversity and customary law in South Africa' (2006) 50 *Journal of African* 2-23.

A Gray and Y Vawda 'Health Policy and Legislation' in *South Africa Health Review 2013/2014* Padarath & English (eds.) (2014) *Health Systems Trust*. Available at

www.hst.ortg.za/publications/south=africa-health-review-2-13/14 (accessed 25 January 2015).

A Gray, Y Vawda and C Jack 'Health policy and legislation: legislation and financing' (2012/2013) *South Africa Health Review* 3-19.

A Greenberg 'The privacy paradox' (2008) *Forbes*.

G Greenleaf '120 national data privacy laws now include Indonesia and Turkey' (2017) Privacy Laws and Business International Report No. 145 10-26.

G Greenleaf 'An endnote on Regulating cyberspace: code vs law?' (1998) *University of New South Wales Law Journal* 1.

G Greenleaf 'Global data privacy laws: 89 countries, and accelerating' (2012) Queen Mary University of London, School of Law Legal Studies Research Paper No. 98/2012.

G Greenleaf 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (2013) *Journal of Law, Information & Science*.

G Greenleaf 'The UN Special Rapporteur: Advancing a Global Privacy Treaty?' (2015) 136 *Privacy Laws & Business International Report* 7-9. Available at http://ssrn.com/abstract=2672549 (accessed 27 November 2016).

G Greenleaf and M Georges 'The African Union's data privacy Convention: A major step toward global consistency?' (2014) 131 *Privacy Laws and Business International Report* 18-21.

SR Greysen, T Kind KC and Chretien 'Online professionalism and the mirror of social media' (2010) 25 (11) *J Gen Intern Med* 1227.

J Griffiths 'What is Legal Pluralism?' (1986) 24 *Journal of Legal Pluralism and Unofficial Law* 1.

S Gritzalis 'Enhancing Privacy and Data Protection in Electronic Medical Environments' (2004) 28 (6) *Journal of Medical systems* 535-547.

H Gross 'The Concept of Privacy' (1967) 42 *New York University Law Review* 34.

R Gross and A Acquistiti 'Information revelation and privacy in online social networks (the Facebook case)' Proceedings of the 2005 Workshop on Privacy in the Electronic Society (2005) *ACM*.

G Gunasekara 'Paddling in unison or just paddling? International trends in reforming information privacy law' (2014) 22 (2) *International Journal of Law and Information Technology* 141.

S Gutwirth *Privacy and the Information age* (2002).

A Gwagwa 'Internet Governance lessons Africa can learn from Brazil's success story'. Available at http://www.opennetafrica.org/?wpfb_dl=29 (accessed 26 November 2016).

A Gwagwa 'To what extent are Africa's regional and national cybersecurity regulatory frameworks keeping up with the emerging international norms on the protection of privacy and civil liberties in the cyberspace?'. Available at https://www.academia.edu/12045652/To_what_extent_are_Africa_s_regional_and_national_cybersecurity_regulatory_frameworks_keeping_up_with_the_emerging_international_norms_on_the_protection_of_privacy_and_civil_liberties_in_the_cyberspace (accessed 22 February 2017).

H

MA Hall 'Law, Medicine, and Trust' (2002) 55 *Stanford Law Review* 463.

OH Hans, C Rizo, M Enkin and A Jadad 'What is eHealth (3): A Systematic Review of Published Definitions' (2005) 7 (1) *Journal of Medical Internet Research* e1.

BE Harrell-Bond & EAB van Rouveroy van Nieuwaal *Disparity Between Law and Social Reality in Africa* (1975).

C Hawn 'Take Two Aspirin and Tweet Me In The Morning: How Twitter, Facebook, And Other Social Media Are Reshaping Health care' (2009) 28 (2) *Health Affairs* 361.

L Haynes, D Legge, L London, D McCoy, D Sanders and C Schuftan 'Will the struggle for health equity and social justice be best served by a Framework Convention on Global Health? (2013) 15 (1) *Health and Human Rights The President and Fellows of Harvard College* at 111-116. Available at http://www.jstor.org/stable/healhumarigh.15.1.111 (accessed 22 February 2017).

D Helly 'Africa, the EU and R2P: Towards Pragmatic International Subsidiarity? (2009) *Journal for International Relations and Global Trends* 45-58.

P Hernon 'Discussion Forum: National Information Policy' (1989) 6 (3) *Government Information Quarterly* 229.

P Hernon & HC Relyea 'Information policy' in A Kent & H Lacour (eds.) *Encyclopedia of Library and Information Science: vol. 48 Supplement II* (1968).

C Heyns and F Viljoen 'An Overview of International Human Rights Protection in Africa' (1999) 15 *South African Journal on Human Rights* 421-445.

A Higgins and A Azhar 'China begins to erect second Great Wall in Cyberspace' (1996) *The Guardian.*

H Hijmans 'Recent developments in data protection at European Union level' (2010) 11 *ERA Forum* 219.

Z Hill, C Tawiah-Agyemang, S Odel-Danso and B Kirkwood 'Informed consent in Ghana: what do participants really understand?' (2008) 34 *J Med Ethics* 48-53.

L Hoffmann 'The Universality of Human Rights' (2009) *Judicial Studies Board Annual Lecture* Available at https://www.judiciary.gov.uk/announcements/speech-by-lord-hoffmann-the-universality-of-human-rights/ (accessed 19 January 2016).

J Hohmann and S Benzschawel 'Data protection in eHealth platforms' in RG Beran (ed.) *Legal and Forensic Medicine* (2013) 1633.

FW Hondius *Emerging Data Protection in Europe* (1975).

G Hosein 'Privacy and Developing Countries' (2011) *Privacy Research Paper, Office of the Privacy Commissioner of Canada*.

M Househ 'Communicating Ebola through social media and electronic news media outlets: A cross-sectional study' (2015) *Health Informatics Journal.* Available at http://jhi.sagepub.com.ezproxy.uct.ac.za/content/early/2015/02/03/1460458214568037.full.pdf+html (accessed 22 February 2017).

M Househ 'The role of short messaging service in supporting the delivery of healthcare: An umbrella systematic review' (2014) *Health Informatics Journal.* Available at http://jhi.sagepub.com.ezproxy.uct.ac.za/content/early/2014/07/16/1460458214540908.full.pdf+html (accessed 22 February 2017).

I

CB IJsselmuiden and RR Faden 'Research and Informed Consent in Africa — Another Look' (1992) 326 *The New England Journal of Medicine* 830-834.

JC Inness *Privacy, Intimacy and Isolation* (1992) *Oxford University Press.*

EC Ip 'Globalization and the future of the law of the sovereign state' (2010) 8 (3) *Oxford University Press and New York University School of Law* 636-655. Available at http://icon.oxfordjournals.org/ (accessed 22 February 2017).

K Iserson ‘Telemedicine: A proposal for an ethical code’ (2000) 9 *Cambridge Quarterly Healthcare Ethics* 404.

J

C Jack, Y Singh, B Hlombe and M Mars 'Language, cultural brokerage and informed consent - will technological terms impeded telemedicine use?' (2014) 7 (1) *South African J BL* 14-18.

C Jack and M Mars 'Telemedicine a need for ethical and legal guidelines in South Africa' (2008) 50 (2) *South African Family Practice* 60, 60a-60c.

C Jack and M Mars 'Informed consent for telemedicine in South Africa: A survey of consent practices among healthcare professionals in Durban, KwaZulu-Natal' (2013) 6 (2) *S Afr J BL* 55-59.

JM Janzen *The Quest for Therapy in Lower Zaire* (1978).

PA Jennett, L Affleck Hall, D Hailey, A Ohinmaa, C Anderson, R Thomas, B Young, D Lorenzetti and RE Scott 'The socio-economic impact of telehealth: a systematic review' 2003 *Journal of Telemedicine and Telecare* 311.

B Johnson 'Privacy no longer a social norm, says Facebook founder' *The Guardian* 11 January 2010. Available at http://www.theguardian.com/technology/2010/jan/11/facebook-privacy (accessed 11 November 2016).

J Jonas 'Interview: Data protection challenge of the future: Big Data'. Available at http://www.e-comlaw.com/data-protection-law-and-policy/ (accessed 3 December 2016).

G Joubert, H Steinberg, E van der Ryst and P Chikobvu 'Consent for Participation in the Bloemfontein Vitamin A Trial: How Informed and Voluntary?' (2003) 93 (4) *American Journal of Public Health* 582-584.

K

BM Kalema and MR Kgasi 'Leveraging E-health for Future-oriented Healthcare Systems in Developing Countries' (2014) 65 (8) *The Electronic Journal of Information Systems in Developing Countries* 1-11.

N Kamwangamalu 'Ubuntu in South Africa: a sociolinguistic perspective to a pan-African concept' (1999) 13 (2) *Critical Arts: South-North Cultural and Media Studies* 24.

J Kang 'Informational Privacy in Cyberspace Transactions' (1998) 50 *Stanford Law Review* 1193.

RE Kapindu 'From the global to the local The role of international law in the enforcement of socio-economic rights in South Africa' (2009) at viii and ix.

WA Kaplan 'Can the ubiquitous power of mobile phones be used to improve health outcomes in developing countries?' (2006) 2 *Globalization and Health*. Available on http://www.globalizationandhealth.com/content/2/1/9 (accessed 21 January 2017).

R Kapuściński *The Shadow of the Sun* (2007).

SK Karanja 'Schengen Information System and Border Control Co-Operation: A Transparency and Proportionality Evaluation' PhD Thesis *Faculty of Law University of Oslo* (2006).

V Karavas and G Teubner 'http://www.CompanyNameSucks.com: The horizontal effect of fundamental rights on 'private parties' within autonomous internet law' (2003) 4 (12) *European & International Law* 1335-1358.

S Kauffman *The origins of Order: Self-organization and Selection in Evolution* (1993).

J Kaye, EA Whitley, D Lund, M Morrison, H Teare and K Melham 'Dynamic consent: a patient interface for twenty-first century research networks' (2015) 23 *European Journal of Human Genetics* 141-146.

JM Kearney 'Telemedicine: Ringing in a New Era of Health Care Delivery' (1997) 5 *CommLaw Conspectus* 289-303.

P Keckley and M Hoffmann 'Social Networks in Health Care: communication, collaboration and insights' (2010) *Deloitte Centre for Health Solutions*.

M Kekana, B Mkhize and P Noe 'The practice of telemedicine and challenges to the regulatory authorities' (2010) 3(1) *South African Journal of Bioethics and Law*.

M Kekana, P Noe and B Mkhize 'The practice of telemedicine and challenges to the regulatory authorities' (2010) 3 *S Afr J Bioethics Law*.

J Kenny 'African culture and medical ethics' (2015) *Traditional African Clinic* 56-57.

A Khrebtukova 'A call to freedom: Towards a philosophy of international law in an era of fragmentation' (2008) 4 (1) *Journal of International Law and International Relations* 51-103.

ED Kinney and BA Clark 'Provisions for health and health care in the constitutions of the countries of the world' (2004) 37 *Cornell International Law Journal* 285.

JM Kirigia, A Seddoh, D Gatwiri, LHK Muthuri and J Seddoh 'E-health: Determinants, opportunities, challenges and the way forward for countries in the WHO African Region' (2005) 5 *BMC Public Health* 137.

S Kleinert and R Horton 'South Africa's health: departing for a better future?' (2009) 374 (9692) *The Lancet* 759-760.

D Knapp van Bogaert and GA Ogunbanjo 'Confidentiality and Privacy: What is the difference?' (2009) 51 (3) *SA Family Practice* 194-195.

D Knapp van Bogaert and GA Ogunbanjo 'Ethics in Health care: confidentiality and information technologies' (2014) 56 (1) Supp. 1 *SA Family Practice* S3-S5.

BM Knoppers, JR Harris, AM Tassé, I Budin-Ljøsne, J Kaye, M Deschênes 'Towards a data sharing Code of Conduct for international genomic research' (2011) 3 *Genomic Med* 46.

M Koskenniemi 'Global Governance and Public International Law' (2004) 37 *Kritische Justiz* 241.

A Kreitman 'Reach 90% of Internet Users Worldwide (And 10 more reasons to buy traffic from Google AdWords)' (2014) 1.

C Kukathas 'Explaining moral variety' (1994) 11 (1) *Social Philosophy and policy* 20.

JK Kumekawa 'An overview of domestic and international telehealth standards organizations: how far have we come and where are we going?' (2003) 9 *Telemedicine Journal and e-Health* S34.

JK Kumekawa 'National initiative for telehealth guidelines: technology environmental scan' (2003) 9 *Telemedicine Journal and e-Health* S34.

M Kunene 'The Essence of being Human: An African Perspective' Inaugural lecture (1996) Durban.

C Kuner 'An International Legal Framework for Data Protection: Issues and Prospects' (2009) 25 *Computer Law & Security Review* 307.

C Kuner ‘Data Protection law and International jurisdiction on the Internet (part 1)’ (2010) 18 *International Journal of Law and Information Technology* 176.

A Kusamotu ‘Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by article 25 of European union directive 95/46’ (2007) 16 (2) *Information and Communications Technology Law* 149.

L

DB Lafky and TA Horan 'Personal health records: Consumer attitudes toward privacy and security of their personal health information' (2011) 17 (1) *Health Informatics Journal* 63-71.

P Langa ‘Transformative Constitutionalism’ (2006) 17 (3) *Stell Law Review* 351.

B Lange in *The New Oxford Companion to Law* P Cane & J Conaghan (eds.) (2008) 996.

P Le Goff 'Global law: A legal phenomenon emerging from the process of globalization' (2007) 14 *International Journal of Global Legal Studies* 119-126.

A Le Roux 'Telemedicine: A South African legal perspective' (2008) 1 *TSAR* 99.

A Le Roux-Kemp 'A legal perspective on the power imbalances in the doctor-patient relationship' unpublished thesis (2010) *Stellenbosch University* 1.

A Le Roux-Kemp 'HIV/AIDS, to disclose or not to disclose: That is the question' (2013) 16 (1) *PER: Potchefstroomse Elektroniese Regsblad*. Available at http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812013000100008&lng=en&tlng=en. (accessed 22 February 2017).

J Lear and E Mossialos ‘EU law and health policy in Europe’ (2008) 10 (3) *Euro Observer* 1.

K Lee & J Collin *Global change and health* (2005).

N Leon *et al.* 'Applying a framework for assessing the health system challenges to scaling up mhealth in South Africa' (2013) 12 *BMC Medical Informatics and decision making*. Abstract available at http://www.biomedicentral.com/1472-6947/12/123 (accessed 22 February 2017).

A Leonard *Your Profile, Please* (1997).

L Lessig *Code and Other Laws of Cyberspace* (1999).

L Lessig 'The law of the horse: What cyberlaw might teach' (1999) *Harvard Law Review* 501.

H Lévy-Bruhl 'Introduction à l'étude du droit coutumier Africain' [Introduction to the study of African customary law] (1956) 8 (1) *Revue Internationale de Droit Comparé* 67.

J Li 'Privacy policies for health social networking sites' (2013) 20 (4) *Journal of the American Medical Informatics Association* 704-707.

J Locke *The works of John Locke. To which is added the life of the author and a collection of several of his pieces* publ. by Mr. Desmaizeaux (1812).

J Locke *Two Treatise on Government* (1689).

DJ Loetz and C du Plessis 'Electroniese Koopkontrkte: 'n tegnologiese hemel of hel (deel-1)' (2004) 1 *De Jure* 1.

A Lollini 'The South African Constitutional Court Experience: Reasoning Patterns Based on Foreign Law' (2012) 8 2 *Utrecht Law Review* 55.

WW Lowrance *Privacy, Confidentiality and Health Research* (2012) 19.

C Lowry and U Schuklenk 'Two models in Global Health Ethics' (2009) 2 (3) *Public Health Ethics* 276-284.

N Lynoe, Z Hyder, M Chowdhury and L Ekstrom 'Obtaining informed consent in Bangladesh' (2001) 344 *New England J Med* 460.

O 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* 569-597.

M

O Maduka and O Odia 'Ethical challenges of containing Ebola: the Nigerian experience' (2015) *Journal of Medical Ethics* 41.

ABP Magalla and GE Kabuje 'The Law of Privacy in Tanzania: A discussion on the challenges affecting privacy in digital environment' (2015) 1.

AB Makulilo 'Data Protection Regimes in Africa: too far from the European 'adequacy' standard?' (2013) 3 (1) *International Data Privacy Law* 42-50.

AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law & Security Review* 78-89.

AB Makulilo '"One size fits all": Does Europe impose its data protection regime on Africa?' (2013) *Datenschutz und Datensicherheit-DuD* 447.

AB Makulilo 'Privacy and data protection in Africa: a state of the art' (2012) 2 (3) *International Data Privacy Law* 163-178.

P Malindi and MTE Kahn 'Letter to the Editor - Rural Telemedicine in Africa' (2005) 47(8) *South African Family Practice* 4.

T Maluwa 'The Constitutive Act of the African Union and Institution-Building in Postcolonial Africa' (2003) 16 (1) *Leiden Journal of International Law* 157-170.

S Mancuso 'African Law in Action' (2014) 58 (1) *Journal of Africa Law* 1.

S Mancuso 'Legal transplants and the economic development: Civil Law vs Common Law?' (2009) *Springer* 75.

S Mancuso 'The New African Law: Beyond the Difference Between Common Law and Civil Law' (2008) 14 (1) *Annual Survey of International & Comparative Law*. Available at http://digitalcommons.law.ggu.edu/annlsurvey/vol14/iss1/4 (accessed 22 February 2017).

SJ Mansfield, SG Morrison, HO Stephens, MA Bonning, SH Wang, AH Withers, RC Oliver, AW and Perry 'Social Media and the medical profession' (2011) 194 (12) *Med J Australia* 642.

NC Manson & O O'Neill 'Chapter 5: Informational privacy and data protection' in *Rethinking Informed Consent in Bioethics* (2007) 97-129.

B Markesinis, C O'Cinneide, J Fedtke and M Hunter-Henin 'Concerns and Ideas about the Developing English Law of Privacy (and How Knowledge of Foreign Law Might be of Help)' (2004) 52 (1) *American Journal of Comparative Law* 133.

M Mars 'Building the Capacity to Build Capacity in e-Health in Sub-Saharan Africa: The KwaZuluNatal Experience' (2012) 18 (1) *Telemedicine and e-Health* 32-37.

M Mars 'Telemedicine and Advances in Urban and Rural Healthcare Delivery in Africa' (2013) 56 *Progress in Cardiovascular Diseases* 326-335.

M Mars 'Telepsychiatry in Africa - A way forward?' (2012) 15 *African Journal of Psychiatry* 215.

M Mars and C Jack 'Informed Consent for Telemedicine in South Africa: Clinical Practice versus the Legislators' in *South African Telemedicine Conference* Cape Town (2010).

M Mars and C Jack 'Why is telemedicine a challenge to the regulators?' (2010) 3 (2) *SAJBL* 2010 55.

M Mars and RE Scott 'Global e-Health policy: A work in progress' (2010) 29 (2) *Health Affairs* 239.

M Mars and C Seebregts 'Country Case Study for eHealth: South Africa' (2008) *Rockefeller Foundation*.

CT Marsden '*Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace'* (2011) 242.

R Martin 'Japan is best prepared to capitalize on cloud computing' (2012).

RO Mason 'Four Ethical Issues of the Information Age' (1986) 10 (1) *MIS Quarterly* 5.

P Matshidze, and L Hanmer 'Health Information Systems in the Private Sector' (2007) *South African Health Review* 89

V Mayer-Schönberger 'Strands of Privacy: DNA databases and informational privacy and the OECD Guidelines' in *DNA and the Criminal Justice System: The Technology of Justice* (2004) 225-246.

J McGirk 'Religious leaders key in the Middle East's HIV/AIDS fight' (2008) 372 (9635) *The Lancet* 279-280.

D McGraw, JX Dempsey, L Harris and J Goldman 'Privacy as An Enabler, Not An Impediment: Building Trust Into Health Information Exchange' (2009) 28 (2) *Health Affairs* 416-427.

RB McKenzie & G Tullock *Modern Political Economy: An Introduction to Economics* (1978) 220.

J McGirk 'Religious leaders key in the Middle East's HIV/AIDS fight' (2008) 372 (9635) *The Lancet* 279.

D McQuoid-Mason 'Invasion of privacy: common law v constitutional delict - does it make a difference' (2000) *Acta Juridica* 227.

D McQuoid-Mason 'Privacy' in Woolman *et al.* (eds.) *Constitutional Law of South Africa* 2 ed. vol. 3 38.

D McQuoid-Mason *The Law of Privacy in South Africa* (1978).

PN Mechael, H Batavia, N Kaonga, S Searle, A Kwan, A Goldberger, L Fu and J Ossman 'Barriers and gaps affecting mHealth in low and middle income countries' (2010) *The Earth Institute Columbia University*.

F Megret 'Is There Ever a 'Right to One's Own Law'? An Exploration of Possible Rights Foundations for Legal Pluralism' *Israel law review* (2012) 45 (1).

SE Merry 'International law and socio-legal scholarship: toward a spatial global legal pluralism' (2008) 41 *Studies in Law, Politics and Society* 149-168.

T Metz '*Ubuntu* as a moral theory and human rights in South Africa' (2011) 11 (2) *African Human Rights Law Journal* 532-559.

R Michaels 'Global legal pluralism' (2009) 5 *Annual Review of Law & Social Science; Duke Law School Public Law & Legal Theory Research Paper No. 259.* Available at http://ssrn.com/abstract=1430395 (accessed 29 September 2014).

GM Miiro, OOM Oukem-Boyer, O Sarr, M Rahmani, F Ntoumi, K Dheda, A Pym, S Mboup and P Kaleebu 'EDCTP regional networks of excellence: initial merits for

planned clinical trials in Africa' (2013) 13 *BMC Public Health* at 258. Available at http://www.biomedcentral.com/1471-2458/13/258 (accessed 30 September 2016).

JS Mill *On Liberty* (1869).

PS Mistry 'Africa's Record of Regional Co-operation and Integration' (2000) 99 (397) *African Affairs* 553.

BM Mitnick *The Political Economy of Regulation: Creating, Designing, and Removing Regulatory Forms* (1980) 38.

BD Mittelstadt and L Floridi 'The Ethics of Big Data: current and foreseeable issues in Biomedical Contexts' (2015) *Sci Eng Ethics* 1.

BD Mittelstadt, NB Fairweather, M Shaw and N McBride 'The ethical implications of personal health monitoring' (2014) 5 (2) *International Journal of Technoethics* 37-60.

BD Mittelstadt, BC Stahl and NB Fairweather 'How to shape a better future? Epistemic difficulties for ethical assessment and anticipatory governance of emerging technologies' (2015) *Ethical Theory and Moral Practice* 1-21.

MA Mizani and N Baykal 'Policymaking to preserve privacy in disclosure of public health data: a suggested framework' (2015) 41 *J Med Ethics* 263-267.

JY Mokgoro '*Ubuntu* and the law in South Africa' (1998) 1 (1) *Potchefstroom Electronic Law Journal* 1.

CS Molyneux 'Trust and Informed Consent: Insights from Community Members on the Kenyan Coast' (2005) 61 (7) *Social Science & Medicine* 1463-1473.

CS Molyneux, N Pershu and K Marsh 'Understanding of informed consent in a low-income setting: three case studies from the Kenyan coast' (2004) 59 (12) *Social science and medicine* 2547-2559.

K Moodley, M Pather and L Myer 'Informed consent and participant perceptions of influenza vaccine trials in South Africa' (2005) 31 *J Med Ethics* 727-732.

B Moore 'Privacy Studies in social and Cultural History' (1984) *M.E. Sharpe Inc* 3-80.

N Moore 'The information policy agenda in East Asia' (1997) 23 (2) *Journal of Information Science* 139-147.

R Moshell 'And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend toward Comprehensive Data Protection' (2004-2005) 37 *Texas Tech Law Review* 357.

JC Moskop, CA Marco, GL Larkin, JM Geiderman and AR Derse 'From Hippocrates to HIPAA: Privacy and confidentiality in Emergency Medicine - Part II: Challenges in the emergency department' (2005) 45 (1) *Annals of Emergency Medicine* 60-67.

T Mayol 'A United Africa? Leaders revive a Dream' (2016) *The Daily Dos*e. Available at www.ozy.com/fast.forward/a-united-africa-leaders-revive-a-dream/70330 (accessed 4 December 2016).

M Mulumba, D Kabanda and V Nassuna 'Constitutional provisions for the right to health in east and southern Africa; EQUINET Discussion Paper *81' Centre for Health, Human Rights and Development, Regional Network for Equity in Health in East and Southern Africa (EQUINET)* (2010) Harare.

TB Murdoch and AS Detsky 'The inevitable application of Big Data to health care' (2013) 309 (13) *Journal of the American Medical Association* 1351.

C Muzaffar 'Human Rights, the State and the Secular Challenge' (1995) 26 (3) *Japan-Asia Quarterly Review* 47-53.

N

T Nagel *Concealment and Exposure and other essays* (2002) 28.

C Ncube 'A Comparative Analysis of Zimbabwean and South African Data Protection Systems' (2004) 2 *The Journal of Information, Law and Technology (JILT)*. Available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_2/ncube/ (accessed 24 February 2017).

J Neethling *Die reg op privaatheid* (LLD thesis UNISA 1976).

J Neethling 'Features of the Protection of Personal Information Bill, 2009 and the law of Delict' (2012) 75 *THRHR* 245.

J Neethling 'The Concept of Privacy in South African Law' (2005) 122 (1) *The South African Law Journal* 18.

J Neethling and J Potgieter 'Defamation of a Corporation: Aquilian Action for Patrimonial (Special) Damages and *Actio Iniuriarum* for Non-Patrimonial (General) Damages: *Media 24 Ltd v. SA Taxi Securitisation and Amici Curiae* 2011 5 SA 329 (SCA)' (2012) 75 *Journal of Contemporary Roman-Dutch Law* at 304-312.

J Neethling, JM Potgieter & PJ Visser *Law of Delict* (2010).

J Neethling, JM Potgieter & PJ Visser *Neethling's Law of Personality* (2005).

S Nel 'Defamation on the Internet and other Computer Networks' (1997) 30 *CILSA* 155.

L Neuhauser and GL Kreps 'Rethinking Communication in E-Health Era' (2003) 8 (1) *Journal of Health Psychology* 7.

H Nissenbaum 'Privacy as contextual integrity' (2004) 79 *Washington Law Review* 119-158.

S Nwaka *et al.* 'Analysis of pan-African centres of excellence in health innovation highlights opportunities and challenges for local innovation and financing in the

continent' (2012) 12 *BMC International Health and Human Rights* 11. Available at http://www.biomedcentral.com/1472-698X/12/11 (accessed 22 February 2017).

ES Nwauche *An Overview of Data Protection and Privacy Legislation in Africa* (2013).

O

D O'Brien 'The search for subsidiarity: The UN, African regional organizations and humanitarian action' (2000) 7 (3) *International Peacekeeping* 57-83.

J O'Brien and C Chantler 'Confidentiality and the duties of care' (2003) 29 *J Med Ethics* 36-40.

C O'Donoghue and K Brimsted 'Brazilian Data Protection Authority fines Internet Provider $1.59m'. Available at http://www.globalregulatoryenforcementlawblog.com/2014/08/articles/data-security/brazilian-data-protection-authority-fines-Internet-provider-159m/ (accessed 22 October 2016).

C Okpaluba 'Constitutional protection of the right to privacy: evaluating the contributions of Chief Justice Langa to the law of search and seizure' *Acta Juridica* (2015) 407.

HN Olinger, JJ Britz and MS Olivier 'Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007)) *International Information and Library Review* 31-43.

MS Olivier 'Database Privacy Balancing Confidentiality, integrity and availability' (2002) 4 (2) *SIGKDD Explorations Newsletter* 20.

S Olsen 'Nearly undetectable tracking device raises concern' (2000) *CNET News.* Available at http://news.cnet.com/ (accessed 6 February 2017).

GC Oosthuizen 'Africa's Social and Cultural Heritage in a New Era' (1987) 17 (2) *Africa Insight* 107-120.

H Oosthuizen and T Verschoor ‘Ethical principles becoming statutory requirements’ (2008) 50 (5) *SA Family Practice* 36.

UJ Orji *Cybersecurity Law and Regulation* (2012).

UJ Orji 'Examining Missing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection' (2014) (5) *CRi* 129.

JE Orlikoff and MK Totten 'Trustee workbook 3. E-health and the board: the brave new world of governance Part 1' (2000) 53 (7) *Trustee* 4.

E Orna 'Informational policies: yesterday, today, tomorrow' (2008) 34 (4) *Journal of Information Science* 547-565.

MFA Otlowski 'Tackling legal challenges posed by population biobanks: reconceptualising consent requirements' (2012) 20 *Med Law Rev* 191-226.

P

LM Pachter, J Sheehan and MM Cloutier 'Factor and subscale structure of a parental health locus of control instrument for use in a mainland United States Puerto Rican community' (2000) 50 (5) *Social Science and Medicine* 715-721.

S Papadopoulos 'Revisiting the Public Disclosure of Private facts in a Cyberworld’ (2009) 30 (1) *Obiter* 30-43.

SD Pattinson 'Consent and informational responsibility' (2009) 35 *J Med Ethics* 176-179.

PA Pavlou ‘State of the information privacy literature: Where are we now and where should we go?’ (2011) 35 (4) *MIS Quarterly* 977.

S Pearson, Y Shen and M Mowbray 'A privacy manager for cloud computing' in *Cloud Computing* MG Jaatun, G Zhao & C Rong (eds.) (2009) 90-106.

A Pentland, D Lazer, D Brewer and T Heibeck 'Improving Public Health and Medicine by the use of Reality Mining' A Whitepaper for the Robert Wood Johnson Foundation (2009) 2.

B Perinan ‘The origin of privacy as a legal value: a reflection on Roman and English Law’ (2012) 52 *American Journal of Legal History* 183.

HH Perritt 'The Internet is Changing International Law' (1998) 73 *Chicago-Kent Law Review* 997.

Y Pillay ‘The Impact ‘The Impact of South Africa's New Constitution on the Organization of Health Services in the Post-Apartheid Era’ (2001) 26 (4) *Journal of Health Politics, Policy and Law* 747-766.

C Piller 'Privacy in peril' (1993) 10 (7) *Macworld* 124-130. Available at http://search.proquest.com.ezproxy.uct.ac.za/docview/199348653/fulltext/149F50DFA87B43FFPQ/70?accountid=14500 (accessed 10 February 2017).

T Pistorius ‘Formation of Internet contracts: Contractual and security issues’ (1999) 11 *SA Mercantile Law Journal* 282.

T Pistorius 'Click-Wrap and Web-Wrap Agreements' (2004) 16 *SA Mercantile Law Journal* 568.

K Poe 'Telemedicine liability: Texas and other states delve into the uncertainties of health care delivery via advanced communications technology' (2001) 20 *The Review of Litigation* 681.

D PoKempner ‘The Internet is Not the Enemy: As Rights Move Online, Human Rights Standards Move with Them’ World Report (2017) *Human Rights Watch* at 39. Available at https://www.hrw.org/sites/default/files/world_report_download/wr2017-web.pdf (accessed 27 January 2017).

DG Post and DR Johnson 'Chaos Prevailing on Every Continent: Towards a New Theory of Decentralized Decision-Making in Complex Systems' (1998) 73 *Chicago-Kent Law Review* 1055.

J Prah Ruger 'Good medical ethics, justice and provincial globalism' (2015) 41 *Journal of Medical Ethics* 103-106.

MP Preziosi, A Yam, M Ndiaye, A Simaga, F Simondon and SGF Wassilak 'Practical experiences in obtaining informed consent for a vaccine trial in rural Africa' (1997) 336.5 *The New England Journal of Medicine* 370-373.

C Prins ‘When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?’ (2006) 3 (4) *SCRIPTed* 270.

WL Prosser 'Privacy' (1960) 48 (3) *California Law Review* 383.

NN Purtova ‘Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights’ (2010) 28 (2) *Netherlands Quarterly of Human Rights* 179-198.

Q

CZ Qiang, M Yamamichi, V Hausman and R Miller 'Mobile applications for the health sector' (2012). Available at http://documents.worldbank.org/curated/en/2012/04/16742613/mobile-applications-health-sector (accessed 24 January 2017).

R

CD Raab, CJ Bennett, RM Gellman and N Waters 'European Commission Tender No XV/97/18/D: Application of a Methodology Designed to Assess the Adequacy of the Level of Protection of Individuals with Regard to the Processing of Personal Data' (1998) *European Commission*. Available at http://ec.europa.eu/justice/data-protection/document/studies/files/19980901_adequacy_methodology_en.pdf (accessed 20 February 2017).

WW Rankin '*Ubuntu*: An African term meaning humaneness, inclusive community where all are respected' (2000) 15 (1) *Journal of Pediatric Nursing* 50.

L Rannefeld 'The doctor will e-mail you now: Physicians' use of telemedicine to treat patients over the Internet' (2004) 19 (1) *Journal of Law and Health* 75.

IM Rautenbach 'The conduct and interests protected by the right to privacy in section 14 of the Constitution' (2001) *Journal of South African Law* 115.

JR Reidenberg 'Lex Informatica: The Formulation of Information Policy Rules Through Technology' (1998) 76 (3) *Texas Law Review* 555.

X Rice 'Ugandan paper calls for gay people to be hanged' (2010). Available at http://www.theguardian.com/world/2010/oct/21/ugandan-paper-gay-people-hanged (accessed 2 February 2017).

C Rich 'Privacy Laws in Africa and the Middle East' (2014) 13 *Privacy and Security Law Report* 717.

SA Riesenfeld 'The Doctrine of Self-Executing Treaties and US v Postal: Win at Any Price' (1980) 74 *American Journal of International Law* 892.

H Rippen and A Risk 'e-Health Code of Ethics' (2000) 2 (2) *J Med Internet Res* e9.

M Rishmawi 'The Arab charter on Human Rights and the League of Arab States: An update' (2010) 10 (1) *Human Rights Law Review* 169-178.

RJ Rodrigues, P Wilson and SJ Schanz *The Regulation of Privacy and Data Protection in the Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-identifiable Health Databases* (2001).

A Roos 'Core principles of data protection law' (2006) 39 *CILSA* 102.

A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 *South African Law Journal* 400.

A Roos 'Personal data protection in New Zealand: Lessons for South Africa?' (2008) 4 *Potchefstroom Electronic Law Journal* 65.

A Roos 'Privacy in the Facebook era: a South African legal perspective' (2012) 129 *South African Law Journal* 375.

A Roos *The Law of Data (Privacy) Protection: A Comparative and Theoretical Study* LLD thesis *UNISA* (2003).

R Rose 'What is lesson-drawing' (1991) 11 *Journal of Public Policy* 3-30.

K Roth 'The dangerous Rise of Populism' (2017) *Human Rights Watch*.

I Rowlands 'Understanding information policy: concepts, frameworks and research tools' (1996) 22 (1) *Journal of Information Science* 13-25.

IS Rubenstein 'Regulating Privacy by Design' (2011) 26 *Berkeley Tech LJ at* 1409.

ML Rustad and TH Koenig 'Harmonizing Cybertort Law for Europe and America' (2005) 13 (5) *J High Tech Law* 13.

S

T Sahama, L Simpson and B Lane 'Security and Privacy in eHealth: Is it possible?' (2013) *e-Health Networking, Applications & Services (Healthcom)*. Available at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6720676&isnumber=6720623 (accessed 5 January 2017).

P Samuelson 'A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy' (1999) 87 *Calif Law Rev*iew 751.

P Samuelson 'Five Challenges for Regulating the Global Information Society'. Available at http://ssrn.com/abstract=234743 or http://dx.doi.org/10.2139/ssrn.234743 (accessed 30 January 2017).

J Sarasohn-Kahn 'Health citizens in emerging countries seek health information online even more than their peers in developed economies' (2011) *Health Populi*, Available at http://www.healthpopuli.com/2011/01/06/health-citizens-in-emerging-countries-seek-health-information-online-even-more-than-their-peers-in-developed-economies (accessed 18 January 2017).

C Schmierer 'Better late than never: How the online advertising industry's response to proposed privacy legislation eliminates the need for regulation' (2011) 13 *Richmond Journal of Law & Technology.*

C Schmierer 'Better late than never: How the online advertising industry's response to proposed privacy legislation eliminates the need for regulation' (2011) 13 *Richmond Journal of Law & Technology* at 6.

L Schoeman 'Embracing e-government: in search of accountable and efficient governance objectives that improve service delivery in the South African health sector' (2007) 42 (5) *Journal of Public Administration* 183.

RE Scott 'Glocal e-Health - A Conceptual Policy Development Framework'.

RE Scott, PA Jennett and M Yeo 'Access and authorisation in a glocal e-health policy context' (2004) 73 (3) *Int J Med Inform* 259.

RE Scott, M Mars and M Hebert ‘How Global is “e-health” and “knowledge translation”?’ (2012) *Technology Enabled Knowledge translation for e-health* 339.

JJM Seddon and WL Currie 'Cloud computing and trans-border health data: Unpacking U.S. and EU healthcare regulation and compliance' (2013) 2 (4) *Health Policy and Technology* 229-241.

A Sen 'Human rights and Asian values' (1997) *Carnegie Council on Ethics and International Affairs* 9-31.

A Sen 'Universal truths' (1998) 20 (3) *Harvard International Review* 40.

A Seppala, P Nykanen and P Ruotsalainen 'Privacy-Related Context Information for Ubiquitous Health' (2014) 2 (1) *JMIR Mhealth and Uhealth* e12.

J Sharmin, M Hoque Chowdhury 'mHealth: A Sustainable Healthcare Model for Developing World' (2014) 2 (3) *American Journal of Modeling and Optimization*.

GB Shaw 'The doctor's dilemma' (2003) 32 (6) *International Journal of Epidemiology* 910-915.

IG Shivji 'Constructing a New Rights Regime: Promises, Problems and Prospects ' (1999) 8 (2) *Social Legal Studies* 253-276.

IG Shivji *The concept of human rights in Africa* (1989).

G Siegal 'Enabling Globalization of Health Care in the Information Technology Era: Telemedicine and the Medical World Wide Web' (2012) 17 (1) *Virginia Journal of law and technology* 1.

MF Sihlongonyane 'The Invisible Hand of the Family in the Underdevelopment of Africa Societies: An African Perspective' Scholarly Papers Series: AFRICA - 1.

JA Singh, M Govender and EJ Mills 'Do human rights matter to health?' (2007) 370 *Lancet* at 521-527.

R Sivaswamy and J Kumar ‘Doctors on the Internet - Legal and Practical Implications’ (200) 12 *Eubios Journal of Asian and International Bioethics* 185.

D Sloss 'Non-Self-Executing Treaties: Exposing a Constitutional Fallacy' (2002) 36 (1) *UC Davis Law Review* 7.

KR Smith 'Religion, secular medicine and utilitarianism: a response to Biggar' (2015) 41 *J Med Ethics.*

S Snail and S Papadopoulos 'Chapter 13 - Privacy and data protection' in S Papadopoulos & S Snail (eds.) *Cyberlaw@SA* 3 ed. (2012) 275-313.

S Snail ‘Electronic contracting in South Africa (e-contracts)’ in S Papadopoulos & S Snail (eds.) *Cyberlaw@SA* 3 ed. (2012) 41-61.

S Snail ‘Electronic Contracts in South Africa - A Comparative Analysis’ (2008) 2 *JILT* 1.

K Sørensen, B Schuh, G Stapleton and P Schröder-Bäck 'Exploring the ethical scope of: a critical literature review' (2013) 2 *Albanian Med Journal* 71-83.

DJ Solove ‘Conceptualizing privacy’ (2002) 90 (4) *California Law Review* 1090.

B Stanberry 'Legal ethical and risk issues in telemedicine' (2001) 64 (3) *Computer methods and Programs in Biomedicine* 225-233.

B Stanberry ‘Telemedicine: Barriers and opportunities in the 21st century’ (2000) 247 *Journal of Internal Med* 615.

G Stapleton, P Schroder-Back, U Laaser, A Meershoek and D Popa 'Global health ethics: an introduction to prominent theories and relevant topics' (2014) 13 (7) *Global Health Action*.

Z Stapić, Z Vrček and G Hajdin 'Legislative Framework for Telemedicine' University of Zagreb Croatia.

C Stephanou 'Regulatory Convergence in the Wider Europe Region: Goals and Means' (2003) *Associazione Universitaria di Studi Europei ECSA Italy*.

GJ Stigler 'The Theory of Economic Regulation' (1971) 2 (1) *Bell Journal of Economics and Management Science* 3.

D Svantesson 'Legal liability for internet based cross-border provision of medical advice, information and products' (2003) *9th Greek-Australian Legal and Medicine Conference.*

PP Swire 'Of Elephants, Mice, And Privacy: International Choice of Law and the Internet' (1998) 32 (4) *The International Lawyer* 991.

T

S Tachakra, STH Mullet, R Freij and A Sivakumar 'Confidentiality and the ethics in telemedicine' (1996) 2 suppl. 1 *J Telemed Telecare* 68-71.

J Tamin 'Can informed consent apply to information disclosure? Moral and practical implications' (2014) 9 (1) *Clinical Ethics* 1-9.

AL Taylor 'Governing the globalization of public health' (2004) 32 *Journal of Law, Medicine and Ethics* 500-508.

AL Taylor, T Alfven, D Hougendobler and K Buse 'Nonbinding Legal Instruments in Governance for Global Health: Lessons from the Global AIDS Reporting Mechanism' (2014) *Journal of Law, Medicine and Ethics* 72-87.

AL Taylor, T Alfven, D Hougendobler, S Tanaka and K Buse 'Leveraging non-binding instruments for global health governance: reflections from the Global AIDS Reporting Mechanism for WHO reform' (2014) 128 (2) *Public Health* 151-160.

O Tene and J Polonetsky 'Big data for all: Privacy and user control in the age of analytics' (2012-2013) 11 (5) *Northwestern Journal of Technology and Intellectual Property* 240.

NP Terry 'What's wrong with health privacy' (2009) 5 (1) *Journal of Health & Biomedical Law* 1-32.

G Teubner 'Global Bukowina: Legal pluralism in the world society' in G Teubner (ed.) *Global Law without a State* Brookfield: Dartmouth (1997) 3-28.

LA Thompson, E Black, WP Duff, N Paradise Black, H Saliba and K Dawson 'Protected health information on social networking sites: Ethical and legal considerations' (2011) 13 (1) *Journal of Medical Internet Research* e8.

JH Thrall 'Globalization of Health Care' (2008) 247 (1) *Radiology* 3-7.

L Timberlake *Africa in Crisis: the Causes, the Cures of Environmental Bankruptcy* (1985).

S Tobak 'You have no privacy - get over it' (2013) *FOXBusiness*. Available at http://www.foxbusiness.com/technology/2013/07/31/have-no-privacy-get-over-it/ (accessed on 22 February 2017).

M Tomlinson, MJ Rotheram-Borus, L Swartz and AC Tsai 'Scaling Up mHealth: Where Is the Evidence?' (2013) 10 (2) *PLOS Med.*

JL Traça and B Embry 'An overview of the legal regime for data protection in Cape Verde' (2011) 1 (4*) International Data Privacy Law* 249.

M Tremblay ‘Telemedicine: Legal Issues A policy overview paper’ (1997) *Rainmaker Publications* 8.

M Tugendhat & I Christie *The Law of Privacy and the Media* (2002).

D Tutu *No future without forgiveness* (1999).

U

NJ Udombana 'A Harmony or a Cacophony? The Music of Integration in the African Union Treaty and the New Partnership for Africa's Development' (2002) 13 (1) *Indiana International & Comparative Law Review* 185. Available at http://ssrn.com/abstract=1925455 (accessed 3 October 2016).

V

MZ Varul 'Talcott Parsons, the Sick Role and Chronic Illness' (2010) 16 *Body & Society* 72.

WMJ van Binsbergen 'Dutch anthropology of sub-Saharan African in the 1970's' (1982) 16 *African Studies Centre Leiden* 13-14.

J Vanderlinden 'Civil law and common law influences on the developing law of Ethiopia' (1966-67) 16 *Buffalo Law Review* 263-264.

D van der Merwe ‘A comparative overview of the (sometimes uneasy) relationship between digital information and certain legal fields in South Africa and Uganda (2014) 17 (1) *PER* 298.

D van der Merwe, A Roos, T Pistorius & S Eiselen 'Chapter 9 - Data protection' in *Information and Communications Technology Law* (2008) 313-397.

J-M van Gyseghem 'Model Law on Data Protection Support for Harmonization of ICT Policies in Sub-Sahara Africa' *International Telecommunications Union* (ITU) 06/02/2012.

B van der Sloot & F J Zuiderveen Borgesius 'Google and Personal Data Protection' in A Lopez-Tarruella (ed.) *Google and the Law: Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models. Series: Information Technology and Law Series* vol. 22 VIII (2012) 75-111.

M var der Veldan and K El Emam 'Not all my friends need to know: a qualitative study of teenage patients, privacy, and social media' (2013) 20 *J Am Med Inform Assoc* 16-24.

W Venters and E Whitley 'A critical review of cloud computing: researching desires and realities' (2012) 27 *Journal of Information Technology* 179-197.

F Viljoen *International Human Rights Law in Africa* (2012).

F von Benda-Beckmann 'Who's afraid of legal pluralism?' (2002) 34 (47) *The Journal of Legal Pluralism and unofficial law* 37-82.

W

H Wallace 'Politics and Policy in the European Union: the Challenge of Governance' in *Policy-Making in the European Union* H Wallace & W Wallace (1996) 16.

N Waters and G Greenleaf 'Australia's 2012 Privacy Act revisions: Weaker Principles, More Powers' (2012) 121 *Privacy Laws & Business International Report* 12.

SD Warren and LD Brandeis 'The right to privacy' (1890) 4 (5) *Harvard Law Review* 193.

R Weeks 'A technology perspective of health care services management' (2012) 12 *Acta Commercii* 173.

FW Weingarten 'Federal information policy development: the Congressional perspective' in C McClure, P Hernon & H Relyea (eds.) *United states Government Information Policies: Views and Perspectives* (1989).

EE Westberg and RA Miller 'The basis for using the Internet to support the information needs of primary care' (1999) 6 *JAMIA* 6.

A Westin *Privacy and Freedom* (1967).

H Westphal and E Towell 'Investigating the future of Internet regulation' (1998) 8 (1) *Internet Research* 26-31.

P Whitaker and C Lynch 'The General Data Protection Regulation : update on the latest developments' (2014) *Lexology*. Available at http://www.lexology.com/library/detail.aspx?g=49dc9633-e8d6-4cf9-abeb-348a6b59a464 (accessed 22 January 2017).

EA Whitley and N Kanellopoulou 'Privacy and Informed consent in online interactions: Evidence from Expert focus groups' (2010) *ICIS 2010 Proceedings Paper 126*.

W Wilson *The New Freedom: A Call For the Emancipation of the Generous Energies of a People* (1913) 201-202.

R Wootton, NG Patil, RE Scott and K Ho *Telehealth in the Developing World* (2009). Available at http://www.ghdonline.org/uploads/Telehealth_in_the_Developing_World_2012_1.pdf (accessed 10 February 2017).

M Wugmeister, K Retzer and C Rich ‘Code of Conduct for cross-border data transfers: making the case for corporate privacy rules’ (2007) 38 *Georgetown Journal of International Law* 449.

Y

KI Yankuzo 'Impact of globalization on the Traditional African Cultures' (2014) 4 *International Letters of Social and Humanistic Sciences* 1-8.

KM Yilma and A Birhanu 'Safeguards of Right to Privacy in Ethiopia: A Critique of Laws and Practices' (2013) 26 (1) *Journal of Ethiopian Law* 3.

Z

BB Zaidan and AA Zaidan 'Impact on Data Privacy and Confidentiality on Developing Telemedicine Applications: A review participates opinion and expert concerns' (2011) *International Journal of Pharmacology* 1.

P Zumbansen 'Piercing the legal veil: Commercial Arbitration and Transactional Law' (2002) 8 *European Law Journal* 400.