PRIVACY PROTECTION FOR MOBILE HEALTH (MHEALTH) IN NIGERIA: A CONSIDERATION OF THE EU REGIME FOR DATA PROTECTION AS A CONCEPTUAL MODEL FOR REFORMING NIGERIA'S PRIVACY LEGISLATION

by

Olufunke Olawumi Salami

Submitted in partial fulfilment of the requirements

for the degree of Master of Laws

at

Dalhousie University

Halifax, Nova Scotia

April 2015

For Oluwatimilehin, 'mummy's special special'. I love you son!

Table of Contents

Abstract ……..vii

Acknowledgements ……..viii

Chapter One: Introduction ……1

1.1 Background……1
1.2 Thesis Objective …….. 6
1.3 Why the European Union Privacy Regime?……...……6
1.4 Structure and Arrangement …….. 7

Chapter Two: Introducing mHealth: A Subset of EHealth…….11

2.1 Introduction ……. 11
2.2 What is EHealth? ……. 12
2.3 Mobile Health (mHealth) ……..16
2.4 Defining Privacy ……. 20
2.4.1 Privacy as Control ……. 21
2.4.2 Privacy as Limited Access ……. 22
2.4.3 Privacy as Intimacy ……. 23
2.5 Assessment of Theories on Privacy ……. 23
2.6 Justifying the Need for Privacy……. 25
2.6.1 Privacy Protects Personal Autonomy ……. 26
2.6.2 Privacy Promotes the Dignity and Worth of the Individual……. 26
2.6.3 Privacy as Necessary for Developing Interpersonal Relationships……....27
2.7 Privacy in the Health Information Context…….28
2.8 Conclusion ……...34

Chapter Three: mHealth in Nigeria: Context and History ……..35

3.1 Introduction ……...35

3.2 Mobile Health (mHealth) in Nigeria ……...39

3.2.1 Background to the Mobile Market in Nigeria……39

3.2.2 mHealth in Nigeria: Overview and Privacy Risks ……...41

3.3 Socio-Cultural Context of Privacy in Nigeria ……...49

3.3.1 Culture as a Factor …….....50

3.3.2 Poverty and Illiteracy as Factors ……...57

3.4 Conclusion …….. 59

Chapter Four: mHealth Privacy in Nigeria: The Legal Framework ……...60

4.1 Introduction …….. 60

4.2 The Nigerian *Constitution* and the Judicial Interpretation of the Right to Privacy…….....61

4.3 The *Code of Medical Ethics* ……... 63

4.3.1 The *Code* on Health Information Generally……...64

4.3.2 The *Code* on Health Information via Computer and Telecommunication Technologies ……... 64

4.4 The *Consumer Code of Practice Regulations* ……... 67

4.5 Identified Shortcomings of the Legal framework for mHealth Privacy in Nigeria……..... 71

4.5.1 The *Constitution* ……71

4.5.1.1 Determining the Scope of the Right to Privacy ……71

4.5.1.2 Cost of Enforcing Fundamental Rights Actions ……72

4.5.2 The *Code of Medical Ethics* ……73

4.5.2.1 Silence on Patient's Decisional Control over Their Health Information……73

4.5.2.2 Construction of 'Consent' Limited to Medical Procedures ……...74

4.5.2.3 Silence on other Principles for Fair Processing of Personal Information …76

4.5.3 The *Consumer Code of Practice Regulations*……...76

4.5.3.1 Rules for Protection of Personal Information are Determined by Industry Players ……76

4.5.3.2 No Special Rules Apply to Health Information ……78

4.5.3.3 Silence on Protection for Cross Border Transfers ……...79

4.6 Conclusion…… 80

Chapter Five: mHealth and Privacy Models: *The European Union Directive* and the *E-Privacy Directive* ……..…….. 81

5.1 Introduction ……..81

5.2 The *European Union Directive* ……84

5.2.1 Background and Scope ……...84

5.2.2 Processing Personal Information Generally
(i.e Non-health Specific Information) ……..85
5.2.2.1 Purpose Specification …… 85

5.2.2.2 Transparency ……..86

5.2.2.3 Right of Access, Rectification and Cancellation ……..87

5.2.2.4 Security …… 87

5.2.2.5 Restrictions on Transfer of Personal Information …… 88

5.2.2.6 Enforcement of the Provisions of the Directive …… 91

5.2.2.7 Summary of the General Principles on Processing of Personal Information
…… 91
5.2.3 Processing of Health Information …… 92

5.3 The *E-Privacy Directive* ……..93

5.3.1 Conditions for Processing of Location Data …… 95

5.3.2 Use of Location Data for Unsolicited Communications …… 96

5.4 The Europe-wide Privacy Models: Analysis and Assessment …… 97

5.4.1 The *Directive* …… 97

5.4.1.1 Specific Application to Health Information …… 97

5.4.1.2 Individual Control of Processing of Their Personal Information……..98

5.4.1.3 Reference to mHealth Captured under Rubric of ‘automatic Processing’.99

5.4.1.4 Exclusion of ‘anonymous Data’ from the Scope of its Application…….101

5.4.1.5 Absence of Any Reference to Location Data ……104

5.4.2 The *E-Privacy Directive* ……....105

5.5 Conclusion ……107

Chapter Six: Reforming Nigerian Privacy Legislation ……... 109

6.1 Introduction ……... 109

6.2 Prospects of Adopting the European wide Legislation as a Conceptual Framework ……111

6.2.1 Opportunity to Participate in a Globalized Regime for Privacy Protection……111

6.2.2 Protection for Cross Border Transfer of Personal Information ……115

6.3 Potential Challenges or Problems to the Adoption of the European Framework……....117

6.3.1 Culture and the Place of the Individual in Society ……117

6.4 Through the Eye of Ubuntu: The Replication of the *Directive* in South Africa's *Protection of Personal Information Act* ……121

6.5 Cultural Views on Respect for Elders and Gender Stereotyping ……....127

6.6 The European Model in a Corrupt Legal System…….. 129

6.7 Illiteracy and Poverty ……... 131

6.8 Feasibility of Adoption for Nigeria ……... 133

6.9 Conclusion ……... 134

Chapter Seven: Conclusion ……... 136

Bibliography ……141

Abstract

The use of mobile technologies to provide and deliver healthcare is known as Mobile Health. Nigeria is one of the countries witnessing a profound use of these technologies. While discussions have focused on the potentials of this technologies to address the challenges in the health system, nothing is said about the risks from unauthorized disclosure or misuse of health information provided by users. This becomes worse when Nigeria's laws do not offer adequate protection.

As Mobile Health is a novelty to Nigeria, this thesis looks to relevant international standards on privacy protection. It does this by examining the European regime for protection of personal information. To prescribe this regime for Nigeria however, the differences in the socio-economic and cultural realities between Nigeria and Europe are presented and examined. This thesis argues that notwithstanding, Nigeria can draw on the European regime to reform its privacy framework.

Acknowledgements

I am profoundly grateful for the financial support provided to me during the course of my master's programme by the Canadian Institutes of Health Research (CIHR) and the Dalhousie Law School through the endowment by Sir Seymour Schulich.

This dissertation would not have been possible without the direction of my thesis supervisor, Professor Elaine Gibson. Prof Gibson guided my thinking, provided support and offered valuable comments which helped me in articulating my thoughts for this thesis. Prof Gibson constantly nudged me to open my mind in my research and was patient with me throughout the course of this research. I am extremely thankful, prof.

I also thank Professor Jon Penney for his comments; for carefully reviewing drafts of this thesis and for his guidance and direction when required. I appreciate the time he spent reading through my thesis and offering his remarks and valuable suggestions.

To David Dzidzornu, I owe a deep sense of gratitude. Mr. Dzidzornu carefully read through each page and provided incisive and candid comments which contributed to the production of this thesis. The conversations we had shaped the direction of this work.

I thank other people-friends and family that have contributed in diverse ways to this project. First my husband, Olumide Salami, whose love, support, encouragement and belief in my abilities helped towards the completion of this thesis. Thank you love, I appreciate you so much. At those times I thought it was impossible to continue, you helped me to keep things in perspective.

I thank Treasure Daniels whose kindness to my son and I helped in many times of difficulty. Treasure was an answer to a prayer for strangers like us in Canada. I would never forget you.

My heartfelt gratitude to my mom, Mrs. Omodunbi Adeniran whose constant prayers, support and encouragement were always available. I love you Mom. I am also grateful to my parents-in law for their support, especially my amazing father-in-law, even though they were thousands of miles away.

And to my son, Oluwatimilehin, this is for you, always. You made it all worthwhile. You were there all the way. I can only hope to bring you as much joy as you have given me.

Finally, I am forever grateful to my maker and savior; the One who was there in my darkest hours; for answered prayers and for bringing me through each and every one of my doubts.

Chapter One

Introduction

1.1 Background

Mobile technologies and applications have spread across the world at a more rapid pace than most other technological innovations.[1]According to statistics from the International Telecommunications Union (ITU), there are over 7 billion mobile cellular subscriptions all over the world, with a forecast that by the end of 2014, there would be 90% penetration in the developing countries. As at the end of 2014, Africa was one of the regions with the strongest in terms of mobile cellular growth.[2] In Nigeria, the mobile phone market also thrived with more than 130 million active mobile subscribers as at December 2014.[3] This represents a significant increase from December 2000 when the number of mobile cellular lines was approximately 35 000 subscribers.[4]

At the same time, Nigeria, like other countries in Africa, faces a major challenge in its health sector. Nigeria has one of the poorest health indicators in the world[5]: a low life expectancy, high maternal and child mortality rate, among others. A major factor hampering the healthcare delivery system in the country is accessibility to care, resulting from inadequate health facilities

[1] Saradhi Motamarri et al, "mHealth, a better alternative for healthcare in developing countries" (Paper delivered at the Pacific Asia Conference on Information Systems (PACIS), Vietnam, July 2012), [Unpublished].

[2]"The World in 2014, ICT Facts and Figures", online:ICThttp://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf>.

[3]Nigerian Communications Commission, "Subscriber Statistics", online: Nigerian Communications Commission < http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125&Itemid=73>.

[4] Ernest Ndukwe,"Country Experience in Telecom Market Reforms-Nigeria", online: Nigerian Communications Commission<http://www.ncc.gov.ng/archive/speeches_presentations/EVC's%20Presentation/Country%20Experience%20with%20Market%20Reforms%20in%20Telecoms%20%20-%20060705..pdf>.

[5]Dr Sipporah Kpamor, " Nigeria's Health Statistics and Trends" (Presentation delivered at the Woodrow Wilson International Center for Scholars Environmental Change and Security Program Global Health Initiative,25 April, 2012).

and extreme shortage of health professionals. Years of chronic under-funding of the health sector by the government has led to a rapidly mobile health workforce that is willing to emigrate to seek better opportunities elsewhere.

Related to this is the fact there is a concentration of health professionals in the urban areas, and a shortage of health workers in the rural areas where more than 70% of Nigeria's population live.[6] Many people in remote and rural areas have lost their lives due to the long distances they have to travel between their homes or communities and the nearest health centre. The mortality risk increases with increasing distance from health facilities. Indeed, many pregnant women lose their lives and even the lives of their unborn children as a result of such spatial challenges.[7]

The vast expansion of mobile communication technology and its potential to facilitate access to care for underserved populations and communities, especially in developing countries, has led to the emergence of Mobile Health or mHealth. According to the Global Observatory for eHealth, Mobile Health is a "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices."[8] mHealth leverages the voice and short messaging service capabilities of these mobile devices to send and receive information in real time to support health services or provide health information.[9] Mobile Health (mHealth) technologies thus offer easily accessible healthcare and

---

[6] Olufunke Ebuehi & Princess Campbell, "Attraction and retention of qualified health workers to rural areas in Nigeria: a case study of four LGAs in Ogun State, Nigeria", online :(2011)11:1 Rural and Remote Health 1515 < http://www.rrh.org.au/articles/subviewafro.asp?ArticleID=1515>.

[7] Okechukwu Ajaegbu, "Perceived Challenges of Using Maternal Healthcare Services in Nigeria" (23 May 2013), online: Aston Journals < http://astonjournals.com/manuscripts/Vol2013/ASSJ-65_Vol2013.pdf>.

[8] World Health Organization, "mHealth: New Horizons for health through mobile technologies", online: World Health Organization< http://www.who.int/goe/publications/goe_mHealth_web.pdf>.

[9]"First Report of the Working Group on mHealth: m-Powering Development Initiative" (31 March 2014),online: International Telecommunication Union <http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Documents/mHealth_Report_of_the_Working_Group.pdf>.

health information to hard-to reach populations. These technologies have also increased health workers' ability to diagnose and track diseases[10] and facilitated medical education for health workers. As a matter of fact, mHealth is being extolled as a defining tool to address challenges in the health sector in Africa.[11]

Nigeria is one of the African countries leading the way in using mHealth solutions for health service[12] delivery through private and government-led initiatives to exploit the potentials of mHealth. Recently, the mHealth community of practice in Nigeria was launched under the Saving One Million Lives Initiative by the Federal Government of Nigeria.[13] Its aim is to reduce maternal and infant mortality in the rural areas by providing valuable health information and support services to pregnant and nursing mothers.

As with most technological innovations and the risks attached to their use, mHealth depends on the collection of health data via these platforms. This raises serious privacy concerns, including the potential for discriminatory profiling[14], surveillance[15] and unauthorized mining of health data.[16] A typical mHealth initiative involves: collection of data; transmission of such data and

---

[10] The Earth Institute Colombia University, "Barriers and Gaps Affecting mHealth in Low and Middle Income Countries: A Policy White Paper" (May 2010), online: mHealth Alliance < http://mHealthalliance.org/media-a-resources/publications>.

[11] *Ibid.*

[12] Jeanine Lemaire, "Scaling up Mobile Health: Elements for the successful Scale-Up of mHealth in Developing Countries", online: K4Health <https://www.k4health.org/sites/default/files/ADA_mHealth%20White%20Paper.pdf>.

[13] "New Public- Private Initiative Leverages Mobile Technologies to Save One Million Lives in Nigeria" (3 December 2012),online:UN Foundation <http://www.unfoundation.org/news-and-media/press-releases/2012/new-public-prive-partnership-mHealthalliance.html>.

[14] Alessandro Acquisti et al, eds, *Digital Privacy: Theory, Technologies and Practices,* (New York; Auerbach Publications, 2008) at ix.

[15] *Ibid*

[16] "Green Paper on Mobile Health ("mHealth")" (10 April 2014), online: European Commission<http://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mHealth>.

storage of the data, for example, to monitor the health of a patient in a remote area.[17] Doing this raises questions about how the data may be used, or to whom it is disclosed, and for what purpose.

Nigeria's 1999 Constitution (as amended), expressly recognizes the individual's right to privacy as sacrosanct,[18]subject to lawful limitation in appropriate circumstances.[19] As well, the *Code of Medical Ethics*[20] places the physician in a fiduciary position to ensure that all communications with a patient are treated in strict confidence. There is also the *Consumer Code of Practice Regulations* made pursuant to the *Nigerian Communications Commission Act* [21] which provides some protection for subscriber data collected by telecommunication companies. Essentially, these are broad and very limited efforts to protect the privacy of Nigerians.

In essence, there is no dedicated legal framework on data privacy protection generally or more specifically one on data privacy for mHealth purposes. Moreover, the existing protections do not reflect emerging principles on the regulation of coverage for data subjects, access and control of the use of data, consent requirements, or the conditions for cross border uses of data. These and other explicit data protection principles apply under the European Union legal regime, comprised

[17] Ademola O Adesina et al, "Ensuring the security and privacy of information in mobile health-care communication systems" (2011) 107 South African Journal of Science 1 at 9.
[18] *Constitution of the Federal Republic of Nigeria (Promulgation)* 1999 No. 24, s 37 [*Constitution*].
[19] According to Section 45 of the Constitution, fundamental rights may be limited in the interest of defence, public safety, public order, public morality or public health.
[20] *Medical and Dental Practitioners Act [cap M8] Laws of the Federal Republic of Nigeria 2004, Code of Medical Ethics* [*Code*].
[21] *The Nigerian Communications Commission Act, 2003* [Act].

of the *European Union Data Protection Directive 95/46/EC*[22]and the *Directive on privacy and electronic communications, 2002/58/EC.*[23]

Nigeria's socio-economic and cultural realities are issues of concern in the consideration of a legal framework in the mould of the European regime. Socio-economic realities derived from factors such as poverty and illiteracy affect the population's awareness of its human rights including the right to the protection of their health information. Further, in a country plagued by inadequate health services and high poverty levels, mHealth serves a useful alternative and the fact that it is available and cheap may make patients vulnerable in the use of their health information as it may be the only health service they are promised.

The impact of Nigeria's cultural realities on the construction of consent as is depicted under the European regime on personal health information protection may also present some difficulty. The cultural system in Nigeria is based on a pervading philosophy of collectivism that gives precedence to group solidarity and roles, relative to the individual's existence and/or identity. For many women especially in the rural areas, for instance, the assignment of roles tends to affect their capacity to consent in the privacy context, while social expectations and familial influence can weigh on their freedom to give consent in other circumstances.

Nevertheless, this thesis considers the feasibility of adapting the European privacy regime for Nigeria. It argues that though the contextual matrixes differ, Nigeria's cultural norms do not prescribe any rules on how the individual private sphere may be protected. Moreover, the socio-

[22] *EC,Commission 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 information and the free movement of such data*, [1995] OJL 281/31 [Directive].

[23] EC, *Commission Directive 2002/58/EC of 31 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, [2002] OJ, L 201 [E-Privacy Directive].

economic realities do not operate as a bar to adopting an effective legal framework to protect privacy rights.

1.2 Thesis Objective

This thesis seeks to consider data protection privacy and the use of mobile health in Nigeria. It does this by examining the inadequacies of the present framework relevant to mHealth privacy protection in Nigeria. The examination inquires whether the existing privacy framework protects mHealth users in terms of collection, use and transfer of their health information. The analysis shows that although a privacy protection framework exists, its provisions on processing health information are not clearly defined. As a prescriptive solution, this thesis considers the prospect of adapting the European regime for privacy protection to regulate for mHealth privacy in Nigeria. It finds that although, the contextual differences between Nigeria and Europe in terms of culture and socio-economic factors may present problems to its adoption and implementation, these problems are not unassailable.

The discussion draws on the experience of South Africa, which is similar to Nigeria in terms of socio-economic and cultural realities, and which recently passed a law replicating the European Directive as its data privacy legislation. The argument is that if legislation based on this European model could work in South Africa, its potential for Nigeria must, at least, be explored.

The rationale for selecting the European Union regime for consideration is set out next.

1.3 Why the European Union Privacy Regime?

Under the framework referred to as the European Union regime, two pieces of legislation are considered: the *Directive* and the *E-Privacy Directive*.

The *Directive* is considered because it is widely applicable and has been transposed into the local laws of all member states of the EU. Moreover, many countries outside of Europe are reworking their national privacy regimes to comply with the requirements of the *Directive* by replicating its provisions in their privacy statutes. Nigeria could do the same. The *E-Privacy Directive*, which complements the *Directive*, is considered because it covers the incidence of data processing brought on by digital technology which this thesis speaks to through the discussion on mHealth.

1.4 Structure and Arrangement

The discussion of the EU regime for data protection as a conceptual framework on which to build mHealth privacy protection in Nigeria is considered over the next five substantive chapters.

Chapter 2 examines the subject of mHealth. It explores the argument that mHealth is a subset of eHealth, or derivable from it. eHealth is broadly defined to encompass the use of information and communication technologies in health. The chapter also examines the privacy risks attached to the growing use of mHealth. The background to this part of the chapter is the philosophical views or conceptions of privacy, their connection to information privacy, and judicial interpretation of the notion of privacy in the context of health.

Chapter 3 explores the context for mHealth in Nigeria. First, it looks at the challenges of healthcare in Nigeria, in terms of access and service delivery. These challenges have necessitated the consideration of mHealth as a suitable, alternative arrangement to conventional medical care, given the ubiquity of mobile phones, even in remote communities. But the chapter acknowledges that there are privacy risks attached to the use of mHealth for Nigeria. This is accentuated by the country's general socio-economic and cultural problems. The analysis of these factors is done in

terms of their relevance to the consideration of how a privacy protection framework may be effective if adopted in Nigeria.

Chapter 4 explores the current law on privacy in Nigeria. It begins by examining the provisions of the *Constitution* which guarantee a fundamental right to privacy for Nigerians. It finds that although a constitutional right to privacy exists for Nigerians, there has been little or no development through judicial interpretation to determine the scope of this right. The effect is that its application to health information or mHealth for that matter is uncertain. Also, substantial costs associated with initiating fundamental right actions is a flaw to this constitutional provision. The chapter also analyses two pieces of subsidiary legislation, the *Code of Medical Ethics*[24] and the *Consumer Code of Practice Regulation* made pursuant to the *Nigerian Communications Commission Act.*[25] For the *Code of Medical Ethics*, it finds that although it places a duty on physicians to keep their patients' confidences in the medical context, patients cannot exercise any control over their health information. The *Code* fails to delimit what control, if any, patients have over their health information. Moreover, while it may appear to have acknowledged the advances of the digital age and its incursion into the practice of medicine through information and communications technology, it only places a cursory obligation of security on physicians and nothing more. Its provision as to consent applies strictly to only medical procedures and not to health information. The analysis also shows that the *Consumer Code of Practice Regulation*, which at first blush, set out the basic principles for the "protection of individual consumer information"[26] is functionally inadequate. This is because it leaves compliance with these principles to the discretion of industry players. The chapter's overall

[24] The *Code, supra* note 20.
[25] The *Act, supra* note 21.
[26] The *Act*, s 106 (2).

conclusion is that given the weakness of the present legal architecture on health information protection in Nigeria, whatever protection there is for mHealth is deeply inadequate.

Chapter 5 examines the European model for privacy via the *Directive* and the *E-Privacy Directive*. The analysis explores the principles or requirements for privacy protection as enunciated in both pieces of legislation. The discussion shows that although both statutes are not specific to mHealth, they have implications for it. This comes, first, in the *Directive*'s specific requirements for processing health information and its application to personal information processed automatically. This implies that mHealth information falls within the purview of the *Directive* as information processed through automatic means. Second, the *E-Privacy Directive* is relevant to location data generated by electronic devices such as mobile devices. The analysis finds that though both the *Directive* and the *E-Privacy Directive* provide sufficient protection for mHealth privacy and may be prescribed for Nigeria, their replication in the latter's legislation must take cognizance of the socio-economic and cultural factors noted in chapter 3.

Chapter 6 examines the broad socio-economic and cultural factors noted in chapter 3 and the ways in which they could present constraints to the operation of the European regime in Nigeria if it is adopted. Using the South African example, the chapter argues that since South Africa which faces the same socio-economic and cultural challenges like Nigeria has adopted the European model, specifically the *Directive*, Nigeria can do the same.

In conclusion, Chapter 7 argues that given the inadequacies of the privacy framework in Nigeria, the European regime presents a useful alternative, not to protect the health information of mHealth users only but also to facilitate Nigeria's participation in a globalized regime on information protection. As such, though cultural notions and socio-economic privations exist, it

is necessary as part of ameliorating those harsh and negative realities, to adopt a robust regime to protect the privacy of Nigeria's mHealth users.

Chapter Two

Introducing mHealth: A Subset of EHealth

2.1 Introduction

Technological advances are shaping our everyday lives in diverse areas including communication, medicine, transportation, education, banking and entertainment.[27] Particularly, modern information technologies, like computers and mobile phones touch our lives in many different ways and have changed how individuals access and disseminate information, communicate with others, learn, exchange knowledge, and provide services.[28]

The integration of information technology into healthcare is changing the traditional perception of healthcare in many ways and with significant influence on how health services are accessed and delivered. The change resulting from this new technological paradigm is what Smith[29] periodizes as a move from 'industrial age medicine' to 'information age health care' where physicians are exposed to, and increasingly use or deploy information tools in their practice.

This chapter analyses the key trends in today's use of information and communications technology in healthcare, especially in terms of its impact on traditional health systems. The analysis places particular focus on the introduction of mobile devices into healthcare, and assesses their potential and current use in this field.

---

[27]Occupational Health and Safety Agency for Healthcare in British Columbia, "Technological Innovations in Occupational Health and Safety in the Healthcare Industry" online: Oregon Coalition for Healthcare Ergonomics <http://www.hcergo.org/136-id-technologicalinnovationsreport.pdf>.

[28]Kendall Ho, "Health in the Digital World: Transformational Trends" in Stefane M Kabene, ed, *Healthcare and the Effect of Technology: Developments, Challenges and Advancements* (Hershey: IGI Global, 2010) 1-3.

[29]Richard Smith," The future of medical education: speculation and possible implications", online: BMJ Talks<www.bmj.com/talks>.

In general eHealth is playing an increasing role in transforming health care systems and helping individuals to make informed choices about their health. As well, it is being utilized to improve healthcare delivery and access. At the same time, the capabilities of these technologies have brought to the fore, issues regarding privacy of health information of patients in eHealth systems. This is because health information stored or transferred via these technologies are for example, vulnerable to hacking by meddlesome individuals, thus, raising concerns about privacy.[30]

This chapter discusses these issues, with specific focus on privacy in the context of mHealth. The discussion examines the concept of eHealth in general, and mHealth more specifically. It then provides a foundation for examining the privacy issues emerging from mHealth by considering the philosophical concept of privacy. This discussion then provides the theoretical basis for an analysis regarding privacy of health information and the need to protect it.

2.2 What is EHealth?

As a concept, eHealth has many definitions. Some have limited their definition of eHealth to the use of the internet in healthcare.[31] In particular, the emergence of 'e-words' in the 1990s, such as e-commerce and e-business, to give an account of the new possibilities in marketing and business via the Internet, have prompted the association of the term eHealth solely with the use of the internet in healthcare.[32] This definition of eHealth views the concept from the purview of

[30] Robert Pear, "Tighter Medical Privacy Rules Sought"*The New York Times* (22 August 2010)online:The New York Times <http://www.nytimes.com/2010/08/23/health/policy/23privacy.html?_r=0>.

[31] JC Wyatt & JLY Liu, "Basic concepts in medical informatics", online: (2002) 56 Journal of Epidemiology and Community Health 11< http://jech.bmj.com/content/56/11/808.full>.

[32]G Eysenbach, "What is e-health?", online :(2001) Journal of Medical Internet Research<http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761894/>.

internet use by the public, health workers, and others to access health information, services and support.[33]

In this context, health professionals can access health related information and reference materials through the internet to help in clinical decisions. The internet becomes a professional information source for health professionals to educate themselves on clinical guidelines at the point of caring for their patients.[34] The connectivity offered by the internet also allows health professionals to directly interface with patients and share laboratory and other diagnostic test results, information resources relevant to the patients' conditions, responses to patient queries related to diagnosed conditions or prescribed treatments and appointment scheduling. On the patients' side, the internet provides an information source for them to obtain information to manage their health. As such, it is not surprising that the definition of eHealth by this school of thought from literature sees it as a "convergence between the Internet and the health care industry to provide … a wide variety of information relating to the health care field".[35]

Apart from the convergence between internet and healthcare, eHealth is also used in reference to health informatics. This deals with how technology aids the use, acquisition and storage of health information to improve individual healthcare or that of the public.[36] To this end, eHealth encompasses the use of information and communication technologies ICT to digitally collect

[33] Wyatt JC, *supra* note 31.

[34] Karl W Thomas, Charles S Dayton & Michael W Peterson, "Evaluation of Internet-Based Clinical Decision Support Systems", online:(1999)Journal of Medical Internet Research<http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761710/>.

[35]Medical Business News "What is eHealth?" cited in Hans Oh et al, "What Is eHealth (3): A Systematic Review of Published Definitions", Online: Journal of Medical Internet Research< https://tspace.library.utoronto.ca/html/1807/4733/jmir.html>.

[36]William Hersh, "A stimulus to define informatics and health information technology", online :(2009) BMC Medical Informatics and Decision Making <http://www.biomedcentral.com/1472-6947/9/24>.

health information about individual patients that can be accessed by health professionals in different locations involved in their care.

Additionally, the term 'eHealth' is used in relation to the use of information and communication tools in healthcare. In this context, eHealth is conceived as embracing the use of telecommunications and computer based technology in healthcare service delivery. Falling into this conception is, for instance, the use of satellite and video conferencing for synchronous exchange of clinical information through video, text, photographs and data[37] between health professionals involved in a patient's care, irrespective of geographic or time differences. It also includes the provision of some health services through mobile devices to "improve quality, safety and access to care".[38] It is in this vein that the World Health Organization defines eHealth as "the use of information and communication technologies for health…"[39] For the WHO, there are two measures for determining the meaning of this concept. First, it involves the information and communications technology delivery of healthcare.[40]In other words, information and communication technology types such as computers, mobile telephones and internet technologies used to facilitate the provision of healthcare become part of the conceptualization of 'eHealth'.

Second is the potential impact of these technologies to transform health. According to the WHO, the use of these technologies must have an impact on healthcare delivery by "making health services more efficient and improving access to care".[41] Because the capabilities of these

[37] American College of Physicians, *Ehealth and its impact on medical practice*, online: American College of Physicians http://www.acponline.org/advocacy/current_policy_papers/assets/ehealth.pdf>.
[38] See *World Health Organization,* WHA Res 58.28, WHO, 114th Sess, UN Doc A58/21 (2005) at 108.
[39] "Building Foundations for eHealth, Progress of Member States: Report of the Global Observatory for eHealth", online: World Health Organization <http://www.who.int/goe/publications/bf_FINAL.pdf>.
[40] Trevor Lewis *et al*, "E-health in low- and middle-income countries: findings from the Center for Health Market Innovations", online: World Health Organization <http://www.who.int/bulletin/volumes/90/5/11-099820/en/>.
[41] WHO, 58th Sess, UN Doc WHA58/2005/REC/1 (2005).

technologies extend beyond physical or geographical domains, physician and patient consultations, for example, can be conducted via a network or video link.[42] As well, health professionals can easily access patient data as opposed to delays associated with physical access to paper records. All these are considered to facilitate increased access by patients, and improvement in the overall efficiency of the health system.[43]

The foregoing views on the concept of eHealth seem to have provided diverging interpretations of the concept. In essence, there is no common understanding or general consensus on the meaning of the concept. As stated by Showell & Nohr, the lack of precision or consensus makes understanding of the concept susceptible to diverse measures for its evaluation.[44] Thus, it is not surprising, as seen above that, while one view sees the internet solely as vital to eHealth, the other conceives it as the use of ICT tools to collect and share information in a healthcare setting. The broader view adopted by the WHO conceives of the concept as the use of any form of information and communication technologies in ways that transform the delivery of healthcare.

This thesis adopts the conception of eHealth, as defined by the WHO, to mean the use of information and communication technologies to transform healthcare. This is appropriate because unlike other definitions, the definition adopted takes cognizance of technologies, such as mobile phones, computer technology, video conferencing, and internet platforms through which eHealth could be provided. This conception is not restrictive and thus, the discussion of what constitutes mHealth in this work is subsumed under it.

---

[42] Yunkap Kwankap, "eHealth in developing countries: contemporary issues, challenges and opportunities for hospitals", online: Africa Health <http://www.africa-health.com/articles/march_2011/13.%20Yunkap%20opinion.pdf>.

[43] *Ibid.*

[44] Chris Showell & Christian Nohr, *How Should We Define eHealth, and Does the Definition Matter: Proceedings of the European Medical Informatics Conference, Pisa, 2012* (IOS Press, 2012).

Further, this definition of eHealth acknowledges the capabilities of ICT to transform health service delivery. Thus, whether it is through mobile technologies or computer systems and network, it is suggested that eHealth improves current practice by providing solutions to some of the challenges in the healthcare system. For example, using mobile technologies or video conferencing, patients can set up appointments to consult with their physicians. This allows for patient access to healthcare, no matter how geographically remote they may be and limits the number of hospital visits.

Overall, the broad description of eHealth acknowledges that a wide range of ICT tools, including mobile technologies, are useful in transforming and creating efficiency in healthcare systems.

2.3 Mobile Health (mHealth)

The Global Observatory for eHealth, a World Health Organization, an initiative dedicated to the study of eHealth, defines mHealth "as medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices**".**[45] This practice is meant to "enhance access to health information, improve distribution of routine and emergency health services, or provide diagnostic services".[46]

These devices have advanced features for voice calls or text messaging;[47] high quality cameras to capture photographs and high-definition videos; global positioning systems (GPS) for location

---

[45] "mHealth: New Horizons for Health through mobile technologies", online: World Health Organization <http://www.who.int/goe/publications/goe_mHealth_web.pdf>.

[46] Alain Labrique, "Opportunities and Challenges for mHealth Strategies in Resource-Limited Settings*"*(4 September 2012) (Youtube) online: Johns Hopkins University < http://www.jhumHealth.org/content/alain-labrique-director-gmi-and-assistant-professor-jhsph-discusses-opportunities-and >.

[47]See The World Bank, "2012 Information and Communications Development: Maximizing Mobile",online:The WorldBank<http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/IC4D-2012-Report.pdf.>. This Report by the World Bank indicated that one of the reasons for this

tracking and advanced capabilities to download applications or 'apps'. Apps are software programs run on a mobile or computing platform, for example, a mobile phone, a tablet or some other device, to perform some function.[48] In the context of mHealth, these apps enable mobile devices to deliver healthcare, or to support some health-related service.

Clinicians and health care providers use text messaging, voice-calling or Apps to provide or support patient care.[49] For example, there are a broad range of Apps that assist physicians in prescribing drugs for patients because they provide quick reference information about a medication.[50] Also with the camera functionality of mobile phones, clinicians can capture and share images with other physicians involved in the care of a patient and store such images to form part of the electronic health record of the patient.[51]

For patients, mHealth offers wider possibilities through Apps or text messaging. There are a wide range of Apps that support patient wellness by allowing users to track calories burnt, weight loss, and generally monitor their body fitness.[52] Some Apps even assume the function of a medical device, like an electrocardiography machine, by monitoring abnormal heart rhythms to

---

decline is because people now make voice calls over the internet such Skype which is usually through Wi-Fi as opposed to than the cellular network.

[48] See Centre for Devices and Radiological Health, *Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff,* (9 February 2015) online: U.S. Department of Health and Human Services Food and Drug Administration<http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf> Throughout this paper, "Apps" would be used inclusively to mean mobile health applications and mobile applications. This term is retained because of its popularity and ease of recognition.

[49] Canada Health Infoway, "Mobile Health Computing between Clinicians and Patients", online: Canada Health <https://www.infoway-inforoute.ca/index.php/resources/technical-documents/emerging-technologynfoway>.

[50] See Epocrates, online: Epocrates < http://www.epocrates.com/products>.

[51] See for example, Clinicam referred to in "Adam Landman et al, "A mobile app for securely capturing and transferring clinical images to the electronic health record: description and preliminary usability study",online:JMIR Publications < http://mHealth.jmir.org/2015/1/e1/>.

[52]Aditi Pai, "23 health and wellness apps that connect to Apple's Health Kit",online:Mobi Health News <http://mobihealthnews.com/36870/23-health-and-wellness-apps-that-connect-to-apples-healthkit/ >

detect if a patient is experiencing a heart attack.[53] The information collected can then be simultaneously available to the patient's healthcare providers or first responders.

Text messaging or SMS also perform health related functions for patient benefits as does Apps. With SMS, patients can be reminded of their appointment with their medical providers,[54]informed of the result of their laboratory test, provided some health related information or to consult with health professionals via SMS, for example, to monitor their adherence to the use of their drugs.[55] The difference is that unlike Apps which require internet access for their download or use, SMS or text-based mHealth services do not. This makes text messaging an attractive fixture where internet access is unavailable; where the cost of access makes it unaffordable, or where social factors such as high level of illiteracy makes internet use unappealing. [56]

Studies on mHealth use, especially in resource constrained settings in developing countries, show that because text messaging is less expensive and messaging can be done in local languages, patterns of use of mHealth tend to revolve around SMS or text messaging.[57]

---

[53] See for example iStethoscope Pro marketed by iPhone. This App records readings of the heartbeat; in addition the reading can be sent through the phone via email available at "iTunes Preview", online: Apple Itunes <http://itunes.apple.com/us/app/istethoscopepro/id322110006?mt=8# >.

[54] Krishnan Narasimhan, "Text Message Appointment Reminders"(2013) 88 American Family Physician at 20.

[55] Richard T Lester et al, "Effects of a mobile phone short message service on antiretroviral treatment adherence in Kenya (WelTel Kenya1): a randomized trial", online: (2010) The Lancet <http://www.pepfar.gov/documents/organization/161268.pdf>.

[56] Carole De´glisen et al, "SMS for disease control in developing countries: a systematic review of mobile health applications" online: Academia. Edu < http://www.academia.edu/2311064/SMS_for_disease_control_in_developing_countries_a_systematic_review_of_mobile_health_applications >.

[57] See Gabriel Otieno et al., "The feasibility, patterns of use and acceptability of using mobile phone text messaging to improve treatment adherence and post-treatment review of children with uncomplicated malaria in western Kenya"(2014) 13:44 Malaria Journal < http://www.malariajournal.com/content/pdf/1475-2875-13-44.pdf>; Francisco Diez-Canseco et al, "Design and Multi-Country Validation of Text Messages for an mHealth Intervention for Primary Prevention of Progression to Hypertension in Latin America", online: (2015) 3:1 JMIR mHealth

We see that the use of mHealth is available in two contexts- viz -health care provider use and patient centred use. It is in the context of patient centred use of mHealth via text messaging that the discussion in this thesis focuses. This use of mHealth offers significant benefits to patients. One of its benefits is that it improves access to healthcare and healthcare related information.[58] This is particularly imperative in developing countries where clinics and hospitals are few and inadequately equipped to cater to the needs of the public. Nigeria, for example, accounts for 13% of the global maternal mortality rate with an estimated 36,000 women dying in pregnancy or at child birth each year.[59] It is significant that most of these deaths occur in the rural areas where there are no health services, and the travel distance to the nearest hospital is long. Through text messaging, organizations like UNICEF are able to provide crucial information on maternal and early-childhood health to pregnant and nursing women in remote parts of that country.[60]

Whether mHealth is via SMS or Apps, it is apparent that patients provide their health information, or such information is collected to provide some health service to them. This information is provided within a technological context, meaning that controlling who has access or whom it is shared with, is not as easily determinable as health information provided physically in a physician-patient context.

---

uHealth 19 < http://mHealth.jmir.org/article/viewFile/mHealth_v3i1e19/2>; James G Kahn, Joshua S Yang & James S Kahn, "Mobile' Health Needs And Opportunities In Developing Countries", online: (2010)29:2 Health Affairs < https://www.k4health.org/sites/default/files/Kahn,%20Yang,%20Kahn%20Mobile%20Health%20Needs%20and%20Opportunities%20in%20Developing%20Countries.pdf>.

[58] The Earth Institute, *supra* note 10.

[59] See Damilola Oyedele, "Nigeria Accounts for 13% Global Maternal Mortality Rates", *This Day* (12 July 2014) online: This Day <http://www.thisdaylive.com/articles/nigeria-accounts-for-13-global-maternal-mortality-rates/183394/>.

[60] Blessing Ejiofor, "A message for maternal and child health", online: UNICEF <http://www.unicef.org/nigeria/media_8457.html>.

In order to provide an appropriate background on control of access or sharing of health information in mHealth, the next section examines the concept of privacy, but with particular emphasis on its relevance to health information protection. This discussion surveys various theories that have attempted to provide a coherent description of privacy to consider how these theories have become highlighted in the concept of privacy.

2.4 Defining Privacy

Privacy is considered the fundamental right of every individual.[61] It is asserted in commentaries[62] that this right traverses three zones,[63] to wit, protecting bodily integrity from physical invasion by others;[64] territorial privacy, which concerns setting limits on intrusion into physical spaces where personal, and sometimes, intimate activities take place;[65]and the notion of individuals being able to control what information about them is available to others, that is, informational privacy.[66] For the purpose of this thesis, emphasis is given to informational privacy above the first two categories.

Because the concept of privacy is sweepingly connected to control over one's body, non-intrusion into one's physical space, and control over one's personal information, it is difficult to

---

[61] *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403.

[62] See Electronic Privacy Information Centre and Privacy International (PI), "Overview of Privacy" in Privacy and Human Rights Report, online: WORLDLII < http://www.worldlii.org/int/journals/EPICPrivHR/2006/>.; Jane Bailey, "Framed by Section 8: Constitutional Protection of Privacy in Canada"(2008) 50 Canadian Journal of Criminology and Criminal Justice 279 at 282-83.

[63] Please note that the right to privacy is also noted to extend to the thought zone. In other words, the right to privacy allows an individual to exercise their thoughts through writings without self-censoring from fear of surveillance. See Madeleine Thien, "Freedom Of Thought Requires Privacy, Not State Scrutiny", *Huffington Post* (23 December 2013)online: Huffington Post <http://www.huffingtonpost.ca/madeleine-thien/freedom-of-thought-requires-privacy_b_4495244.html>.

[64] *R v Dyment*, [1988] 2 SCR 417 [*Dyment*].

[65] *R v Tessling* [2004] 3 SCR 432 [*Tessling*].

[66] See *Dyment*, *supra* note 64 at para 22.

define.[67] According to William Beaney, "… there are serious problems [in] defining the essence and scope of this right".[68] This is because the interests protected are distinct and unrelated one to the other.[69] Thus given that the concept has been attached to different interests, so also have theories that have sought to define and delineate its scope.

According to Alan Westin, a person has privacy when they are able to control the availability of information about themselves to others.[70] For Mill, there is privacy when access to information about the individual is limited or restricted. In his view, "there is a circle around every individual human being, which no government… ought to be permitted to overstep…"[71] Similarly, David O'Brien defines it as "a state or condition of limited access to a person."[72] For Julie Inness, privacy is intimacy, as it relates to protection of those aspects of individuals' personal lives that are intimate or sensitive.[73]Each of these is explored in more detail below.

2.4.1 Privacy as Control

Control is the ability of the individual to regulate the circulation of information about themselves.[74] For a person to be in control, it means they are able to exercise power either to

---

[67] Daniel J Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2008) at 1.
[68] William M Beaney, "The Right to Privacy and American Law" (1966) 31 Law and Contemporary Problems. 253 at 255.
[69] William L Prosser, "Privacy [A Legal Analysis]" in Ferdinand David Schoeman, ed, *Philosophical Dimensions of Privacy* (Cambridge: Cambridge University Press, 1984)104 at 107. Here, Prosser stated that the law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common. See also Ken Gormley, "One Hundred Years of Privacy" (1992) Wisconsin Law Review 1335 at 1339.
[70] Alan Westin, *Privacy and Freedom,* Ist ed (New York: Atheneum Press, 1967) at 7.
[71] John Stuart Mill, *Principles of Political Economy with Some of their Applications to Social Philosophy* (Toronto: University of Toronto Press, 1965) at 938.
[72] David O' Brien, *Privacy, Law, and Public Policy* (New York: Praeger Publishers, 1979) at 16.
[73] Julie C Inness, *Privacy, Intimacy and Isolation* (New York: Oxford University Press, 1992) at 140.
[74] Arthur R Miller, *The Assault on Privacy*: *Computers, Databank and Dossiers* (Ann Arbor: University of Michigan Press, 1971) at 25.

deny or grant others access to information about themselves. In *R v Dyment,*[75]it was held that the idea of privacy as control emanated "from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit".[76] The implication is that, with privacy as control, a person has exclusive claim over their information and every other person cannot interfere with their claim except they yield their control right by giving consent.[77]

2.4.2 Privacy as Limited Access

In *Privacy and the Limits of Law,* Ruth Gavison conceptualizes privacy as 'limited access' to the self.[78] According to her

> Our interest in privacy... is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention.[79]

Gavison explains that an individual enjoys privacy in terms of limitation of access to others when no one is able to obtain information about the individual; no one pays attention to them or has physical access to the individual.[80] With regards to information privacy, Gavison contends that secrecy is an important element to limiting access to the self.[81] This is done by withholding or concealing the disclosure of one's personal information from others.

---

[75] *Dyment, supra* note 64.
[76] *Ibid* at para 22.
[77] Adam Moore, "Defining Privacy" (2008) 39 Journal of Social Philosophy 411 at 415.
[78] Ruth Gavison, "Privacy and the Limits of Law" (1980) 89 Yale LJ 421.
[79] *Ibid* at 423
[80] *Ibid* at 428.
[81] Gavison, *supra* note 76 at 429.

Consistent with this notion of privacy as secrecy from disclosure of one's personal information, the United States Supreme Court in *Whalen v Roe,*[82] acknowledged that privacy encompassed the individual interest in avoiding disclosure of personal matters.

2.4.3 Privacy as Intimacy

The thrust of this conception of privacy is that privacy only concerns areas of the individuals' personal life that are intimate or sensitive.[83] In other words, there is loss of privacy where 'intimate' or 'sensitive' information, personal to the individual, are revealed. Julie Inness, one of the intimacy theorists postulates that privacy is "the state of possessing control over a realm of intimate decisions, which includes decisions about intimate access, intimate information, and intimate actions".[84] These theorists think that privacy is only concerned with the protection of information that possesses an intimate essence, and nothing more. Thus, information of an intimate and sensitive nature, such as a person's sexual preference, would qualify as private and, thus, is worthy of protection.[85]

2.5 Assessment of Theories on Privacy

Evident in the notions of privacy as control, limited access and intimacy is the idea that privacy operates as a limit to the use of one's personal information. This implies that with privacy, individuals can control access to information about themselves. It also implies that individuals may control aspects of their personal lives that are intimate and sensitive.

---

[82] *Whalen v Roe*, 429 US 589 (1977).
[83] Lee Bygrave, "The Place of Privacy in Data Protection Law" (2001) 24 UNSWLJ 277 at 280.
[84] Inness*, supra* note 71 at 140.
[85] Raymond Wacks, *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1989) at 26.

Privacy as control means individuals can deny or limit access to information about themselves.[86] The idea of control may suggest that an individual can unlimitedly contain the flow of their personal information, though it is questionable whether this is possible in all circumstances. For example, while shopping at an 'adult store' in broad daylight, can an individual control being seen by a colleague? In other words, can the idea of control apply in all circumstances? According to Tavani, control in this sense does not implicate absolute control over all aspects of one's self, including, in this case, information that the individual would wish to remain personal, but which is public in nature.[87] This suggests that the individual can choose what realm is private, or they can similarly decide to forego their privacy by consent.

With choice, a person can choose situations that provide the level of privacy desired. Using the example above, a person who desires privacy may choose to patronize the 'adult store' at night, or employ means of protecting their identity when doing so. In other words, individuals can, by their own choice, decide what is private. In *Katz* v *United States*, the United States Supreme Court alluded to this choice stating that that there is no reasonable expectation of privacy in things exposed to the public,[88] pointing out that "…what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[89]

Consent is also an element of control. Literally construed, consent as agreement or approval, in the privacy context, becomes the mechanism that determines whether individuals have relinquished control of their privacy to another. In other words, to provide consent is to frame an

---

[86] Herman Tavani, "Privacy and the Internet" in Madeleine Plascenscia & Paul Finkelman, eds., *Privacy and the Constitution* (New York: Routledge, 1999) at 261.
[87] Herman Tavani, "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy" (2007)38 Metaphilosophy at 11.
[88] *Katz v United States*, 389 US 347 (1967) at 351.
[89] *Ibid.*

exception to a claim for privacy by allowing for collection, use or disclosure of one's personal information in a particular way.[90] For example, the collection, use and disclosure of certain categories of personal information which deal with health, sexual orientation or race, are prohibited by data protection laws and privacy legislation.[91] The rationale for this is that the misuse of information relating to these categories could have the severe consequence of exposing their owner to discrimination or social stigma.[92]With consent, individuals can limit or control the flow of information about themselves and, thus, the potential risks they may face from doing so.

The discussion in this thesis draws on the ideas expressed in these foregoing conceptions of privacy. In sum, the view adopted is that privacy of information provides individuals control over their personal information. Control enables them to determine the realms they construe as private. Even so, individuals can provide their consent to the use of their information in ways that may otherwise constitute infringement of their privacy. The question this thesis examines, therefore, is whether this idea of control arises in regard to the particular sphere of health information. A preceding point, considered next, is the importance of privacy to personal information.

2.6 Justifying the Need for Privacy

The discussion of the theories, above, emphasizes that privacy is an essential value to the individual. The logical inquiry, therefore, is what benefit privacy holds for the individual.

---

[90] "Consent: A separate privacy principle dealing with consent?" online: Australian Law Reform Commission <http://www.alrc.gov.au/publications/19.%20Consent/separate-privacy-principle-dealing-consent>.

[91] See Article 6, Council of Europe, CA, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*; *EC, Commission 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 information and the free movement of such data*, [1995] OJL 281/31, Article 8.

[92] Article 29 Working Party, "Advice paper on special categories of data ("sensitive data"),online: European Commission<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf>.

Various ethical justifications[93] have been provided to rationalize the need for privacy, and consequently, its protection by the law. I examine three interrelated ones.

2.6.1 Privacy Protects Personal Autonomy

According to Alan Westin, one of the functions of privacy is its protection of the personal autonomy of the individual.[94] He describes personal autonomy in terms of "the uniqueness of the individual, [their] basic dignity and worth as a human being" which demands that they maintain their autonomy and "… avoid being manipulated or dominated wholly by others"[95] To be autonomous means a person has the capacity to make their own decisions and act on them.[96] By allowing individuals control over their lives and their personal information, privacy enhances personal autonomy by allowing individuals to determine or choose what aspects of their lives may be known to others. For example, in the illustration above, an individual may wish to keep knowledge of their sexual orientation away from their work colleagues, and the ability to keep this information from others fosters a feeling that they can make decisions about living their lives independently of what others may think even where the decisions may depart from social norms of behaviour or be contrary to social expectations.

2.6.2 Privacy Promotes the Dignity and Worth of the Individual

It is also contended that privacy promotes respect and individual privacy. James Rachels justifies privacy because it is important to keep some aspect of one's life or behaviour to oneself "simply

---

[93] See Robert Post, "Three Concepts of Privacy" (2001) 89 Geo LJ 2087; Alan F Westin, "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy" (1966) 66 Colum L Rev 1003; Daniel J Solove, "A Taxonomy of Privacy" (2006) 154 U Pa L Rev 477.
[94] Westin, *Ibid* at 1022.
[95] *Ibid*.
[96] Tom L Beauchamp & James F Childress, *Principles of Biomedical Ethics,* 4th ed (New York: Oxford University Press, 1994) at 126.

because it would be embarrassing for other people to know about it".[97] While autonomy, as examined above, refers to the ability of persons to create their own identity from domination by others, dignity, by contrast, refers to "our sense of ourselves as commanding respect."[98] It is the value human beings have in themselves as humans that deserves respect. This sense of dignity derives from social norms regarding accepted standards of behaviour which individuals imbibe, albeit unconsciously, from living with others in society.[99] In other words, dignity protects one's status in relation to others in society.

For instance, norms of behaviour regarding sexual orientation vary from society to society. Gendered norms of appropriate sexual behaviour for men and women exist from society to society.[100] For an individual whose orientation and habits run contrary to the social standard or signification, being private protects them from scrutiny that may result in social humiliation or embarrassment and adversely affect their sense of respect and status in society.

2.6.3 Privacy as Necessary for Developing Interpersonal Relationships

Another privacy value is that privacy protects social interaction.[101] According to Charles Fried, it is important for individuals to have a private sphere that allows them to control information they disclose to others.[102] This opinion argues that being able to control access to one's information

---

[97] James Rachels, "Why Privacy is Important" (1975) 4 Philosophy and Public Affairs at 323.
[98] Post, *supra* note 93 at 2092.
[99] See Robert C Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort" (1989) 77 Cal L Rev 957 at 984.
[100] Sive Mxokoheli,"Controversies of gender and sexuality, heteronormativity and homosexuality in African contexts", online: Academia.edu<http://www.academia.edu/8753580/Controversies_of_gender_and_sexuality_heteronormativity_and_homosexuality_in_African_contexts>.
[101] Beate Roessler & Dorota Mokrosinska, "Privacy and social interaction" (2013) 39 Philosophy and Social Criticism 771 at 774-84.
[102] Charles Fried, "Privacy" (1968) 77 Yale LJ 475 at 482-83.

serves to define the ability to create and maintain social relationships with different people.[103] This is because patterns of social relationship differ from one person to the other depending on the person or people being interacted with.[104] Rachel sums it up as follows:

> a man may be playful and affectionate with his children .. business like with his employees, and respectful and polite with his mother in law. And to his close friends he may show a side of his personality that others never see-perhaps he is secretly a poet, and rather shy about it, and shows his verse only to his best friends.[105]

For relationships that are intimate, such as with close family members, it is possible to share confidences or intimate information and be "real",[106] as opposed to non-intimate personal relationships where the individual can role-play to sustain the requirements of such relationships.

The value of privacy, given that we pursue differentiated relationships with people, is that the degree of personal information that an individual discloses to, and conceal from others, allows them to determine their privacy and, thus, control the character of their different social relationships.

In the light of the foregoing, what does the concept of privacy mean for the particular sphere of health information? This matter is taken up next.

2.7 Privacy in the Health Information Context

In the health sector, the value in privacy protection has long been recognized.[107] As a matter of medical ethics, the value of health information protection is cognizable under the duty of

---

[103] Rachels, *supra* note 97 at 326.
[104] *Ibid.*
[105] *Ibid*.
[106] *Ibid.*
[107] Sharyl J Nass, Laura A Levitt & Lawrence O Gostin, eds, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* (Washington DC: National Academies Press, 2009) at 75.

confidentiality placed on medical practitioners. This duty was presaged by the Hippocratic Oath, an ethical code for physicians which provides

> Whatever I may see or hear in treatment, or even without treatment, in the life of human beings — things that should not ever be blurted out outside—I will remain silent, holding such things to be unutterable [sacred], not to be divulged.[108]

From the Hippocratic Oath to the Declaration of Geneva, which provides that "I will respect the secrets which are confided in me even after the patient had died",[109] it is recognized that physicians owe a duty to ensure that all information generated in the course of a medical relationship is confidential.

Discussions on the concept of confidentiality adopt the utilitarian position that patients are likely to speak freely about their conditions to their physicians where their confidence is guaranteed. According to Beauchamp and Childress, "[a]ssurance of confidence is of paramount importance because it allows people to seek help without the stigma that would result from public knowledge: It encourages full disclosure essential for effective treatment, and it is necessary for the maintenance of trust."[110] Conversely, a patient who has no assurance that the information shared with their physician would be kept confidential is likely to refrain from providing the needed information that could lead to "non-presentation, misdiagnosis, or failure of treatment, and ultimately cause more harm than maintaining confidentiality."[111]

The rationale for confidentiality is that there is a fiduciary relationship of trust between physicians and their patients. This is necessary for the patient to provide the information required

---

[108] Steven H Miles, *The Hippocratic Oath and the Ethics of Medicine* (Oxford: Oxford University Press, 2005) at 49.
[109]World Medical Association, "Declaration of Geneva" online: World Medical Association <http://www.wma.net/en/30publications/10policies/g1/index.html>.
[110] Beauchamp & Childress, s*upra* note 96 at 230.
[111] Chris Jones, "The utilitarian argument for medical confidentiality: a pilot study of patients' views" (2003) 29 Journal of Medical Ethics at 348.

for their diagnosis. While the patient provides their information for the purpose of treatment, the physician holds such information in a manner akin to a trust for the benefit of the patient, that is, their treatment.[112]

Because 'privacy' and 'confidentiality' in the medical context both concern the protection of health information, the tendency has been to use both concepts interchangeably.[113] This is done also because, according to Raymond Wacks, both concepts refer to information that is out of the public domain.[114] Others, however, think that privacy encompasses confidentiality, and both mean the same thing.[115]

For the purpose of this thesis, it is not necessary to determine the difference except to point out that unlike privacy, confidentiality requires one person, the patient to provide their health information in the context of a trust relationship to their physician in the expectation that the information would be kept confidential. The English case of *Attorney General v Guardian*,[116] speaks to the relations that determine the existence of this duty. In that case, the court noted that certain relationships, such as that between a physician and a patient implicate this duty.[117] In other words, confidentiality is relational, and it is based on the context of a relationship which implicates a professional duty on one person to protect the information provided by another.

---

[112] See *McInerney* v *Macdonald* [1992] 2 SCR 138 [*McInerney*].
[113] John C Moskop et al, "From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine-Part:1 Conceptual, Moral, and Legal Foundations" (2005) 45 Annals of Emergency Medicine 53 at 54.
[114] Raymond Wacks, ed, *Privacy*, 1st ed (New York: New York University Press) at xi.
[115] Joy L Pritts," The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research" online: Institute of Medicine <http://www.iom.edu/~/media/Files/Activity%20Files/Research/HIPAAandResearch/PrittsPrivacyFinalDraftweb.pdf>.
[116] *Attorney General v Guardian Newspapers Ltd* (1988) [1990] 1 AC 109 [*Guardian*].
[117] *Guardian,supra* note 116.

The question is whether an obligation of confidentiality alone would suffice in the evolving health context where developments in technology have led to a shift in how care is provided and, thus, in the traditional role of the physician in healthcare. The significant changes brought on by new technologies on health systems is provided by a report on the health sector of the province of British Columbia, Canada.[118] According to the report, the health sector is being transformed by developments in digital technologies.[119] Some of these changes include the way health information can be digitized and readily shared with health care providers across various points of services in the health sector.[120] It also notes that mobile health technologies have changed the traditional pattern from physician case notes to digitized means of accessing patients' health information.[121]

The changes, as noted earlier, have improved efficiency in the management of patient care. For example, using the technologies cuts medical errors of working with paper records and also allows patient records to flow seamlessly within different services in the health sector.[122]Of course, within this technology context, patients still provide their health information in the expectation that they would be protected on the same ethical standards of confidentiality that have always been practised in the health profession.[123]Even so, the difference today is that health

[118] "Special Report: A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector" (30 April 2014), online: Office of the Information and Privacy Commissioner for British Columbia <https://www.oipc.bc.ca/special-reports/1634>.
[119] *Ibid.*
[120]*Ibid*.
[121] *Ibid*.
[122] Kellie Leitch et al, "Leveraging Information Technologies To Transform and Sustain British Columbia's Health Care Sector", online: Centre for Health Innovation and Leadership <http://sites.ivey.ca/healthinnovation/files/2010/10/BC-White-Paper-Final.pdf>.
[123] Special Report, *supra* note 118.

information serves a range of purposes not limited to diagnosis and treatment of diseases.[124] Information provided by patients could serve for medical research to learn about new diseases; to direct the focus of government policy; or shared with state Medicare services to justify payment of services rendered by physicians.[125] Also unlike paper files available to only one user at a time, and which are usually under the control and care of the physician attending to a patient,[126] with technology, health information becomes available to many users of the documentation. The downside is that there may be breaches where information is stolen or accessed in an unauthorized manner by persons without the requisite privilege,[127] to be used for purposes, other than for the care of the patient.[128]

In *McInerney* v. *MacDonald*, [129] the Supreme Court of Canada articulated the 'personal 'nature of health information in relation to individuals and also defined the patient's right to its control. In that case, the patient, Mrs MacDonald, had asked her physician, the Appellant in this case, to provide her with copies of the content of her entire medical file. The doctor complied in part, delivering copies of her own notes, but refusing to provide copies of documents that originated

[124] Ajit Appari & M Eric Johnson , "Information Security and Privacy in Healthcare: Current State of Research", online: Institute for Security Technology Studies <http://www.ists.dartmouth.edu/library/416.pdf>.
[125] *Ibid*.
[126] Laurinda B Harman, Cathy A Flite & Kesa Bond, "Electronic Health Records: Privacy, Confidentiality, and Security" (2012) 14 American Medical Association Journal of Ethics 712.
[127] Jeff Goldman, "Stolen Computers, Mobile Phones Expose Thousands of Patients' Medical Data"(3 February 2015),online:eSecurityPlanet<http://www.esecurityplanet.com/network-security/stolen-computers-mobile-phones-expose-thousands-of-patients-medical-data.html>.
[128] See "Vitalité Health refers doctor privacy breach to RCMP" *CBCNews* (23 September 2014)online: CBCNews <http://www.cbc.ca/news/canada/new-brunswick/vitalit%C3%A9-health-refers-doctor-privacy-breach-to-rcmp-1.2775290>, where in New Brunswick, Canada, a radiation oncologist, accessed the personal health information of several females between the ages of 13 and 39 without authorization. He did not access the records for the purpose of treating the patients and neither was he authorized to do so; "Colleen Stamp found guilty of illegally accessing patient records" *CBCNews* (30 September 2014)online: CBCNews<http://www.cbc.ca/news/canada/newfoundland-labrador/colleen-stamp-found-guilty-of-illegally-accessing-patient-records-1.2782794> where a nurse illegally accessed the electronic records of patients.
[129] *McInerney, supra* note 112.

from other physicians. On appeal to determine the question of her access to the records, the Court characterized health information contained in a patient's medical records as follows:

> ...medical records contain information about the patient revealed by the patient, and information that is acquired and recorded on behalf of the patient. Of primary significance is the fact that the records consist of information that is highly private and personal to the individual.[130]

Having determined that such information is highly private and personal to the individual, the Court said that such information "…goes to the personal integrity and autonomy of the patient"[131] as they relate to "…sensitive aspects of an [individual's] life."[132]

The need to regard health information as sensitive is borne out of the implications of an inappropriate disclosure or misuse. Inappropriate disclosure of information about the sexual orientation, mental health or reproductive choices of a person could expose individuals to discrimination and, in some extreme case, harm. Misuse or abuse could also result when health records of patients are accessed in an unauthorized manner, sometimes with no defined intent to cause harm, but to meddle in the affairs of the individual.[133] According to the Court in the *McInerney* case, because of the personal nature of health information, it is important that individuals have a "continuing interest in what happens to this information and in controlling access to it".[134] Having continuing interest in this sense means that patients are able to determine how many people have access to their health information, and their authorization is sought where other persons seek access. It also means that patients' information are only used for the purpose

---

[130] *Ibid* at para 22.

[131] *McInerney, supra* note 112 at para 22.

[132] *Ibid* at para 18.

[133] See the case of *Jones v Tsige* 2012 ONCA 32. In this case, the plaintiff's privacy had been invaded by the defendant, an employee of a Canadian bank who improperly accessed the banking records of her common law partner's ex-wife, for personal reasons, without authorization. Although this case did not occur within the healthcare context, the tort of 'inclusion upon seclusion' recognized by the Ontario Court of Appeal in this case has been relied upon in cases of unauthorized and wrongful access of patient records by hospital staff.

[134] *McInerney, supra* note 112.

of their care. In other words, patients must be able to exercise control over uses other than for the purposes of their care.

2.8 Conclusion

This chapter started by showing that mHealth is a subset of eHealth. For its purposes, eHealth, is defined as the use of information and communication technologies in healthcare, including mobile technologies making mHealth a subset of eHealth.

The chapter also established that privacy is an important issue in mHealth. Conceptually, it was argued that privacy connotes notions of control by the individual, and that this finds expression in the 'choice' and 'consent' provisions in information protection legislation. The benefits of privacy and the value it provides for the individual, are in terms of promoting personal autonomy, protecting dignity, and allowing intimate personal relationships to develop along with a spectrum of other social relationships. Finally, the chapter argued that privacy discourse within the particular realm of health information may not be the same as the ethical duty of confidentiality in the medical context, although they are similar.

The next chapter uses the background provided in this chapter as the framework to examine mHealth in Nigerian. Of special attention is how privacy and its benefits in terms of individual autonomy and dignity carry into the Nigerian social context in the light of its socio-cultural realities founded in communal living and communal interest in an individual's personal matters.

Chapter Three

mHealth in Nigeria: Context and History

3.1 Introduction

Nigeria is Africa's most populous country with an estimated population of one hundred and seventy million people.[135]The country accounts for half of the population of the West African region and around 20% of the population of Sub-Saharan Africa.[136] It lies within the tropical zone, occupying about 923 773 km2 (about 3% of Africa's land area).[137]

It is an oil rich country, with oil revenue from the Niger-Delta region accounting for 80% of its national income.[138] It is the largest oil exporting country in Africa, providing 10% of all U.S. oil imports, and ranks as the fifth-largest source for oil imports in the U.S.[139] Apart from its oil resources, agricultural and forest resources are a driving force for its economy. Plentiful rain and arable soil for farming makes Nigeria one of the top producers of cash crops like cocoa, oil palm and rubber.

With its population and wealth, Nigeria is a "regional hegemon"[140] asserting its influence in peacekeeping operations in major conflicts in Africa. Furthermore, it has committed its resources

---

[135]World Health Organization, "Nigeria: Country Profile", online: World Health Organization <http://www.who.int/countries/nga/en/>.

[136]KPMG Services, "Nigeria: Country Profile", online: KPMG Services <http://www.kpmg.com/Africa/en/KPMG-in-Africa/Documents/NIgeria.pdf>.

[137] Worldmark Encyclopedia of Nations, "Nigeria", online: <http://www.encyclopedia.com/topic/Nigeria.aspx>.

[138] Jonah Rexler, "Beyond the Oil Curse: Shell, State Power, and Environmental Regulation in the Niger Delta" (2010) 12 Stanford Journal of International Relations 26 at 27.

[139] http://en.wikipedia.org/wiki/Petroleum_industry_in_Nigeria

[140] Peter Joseph Singhatey, *Peacekeeping in Africa: The Vital Role of a Regional Hegemon* (M A Thesis, Dublin City University, 2008) [Unpublished].

to programmes that help promote development in poorer African countries as well as greater economic cooperation among African countries.[141]

On the flip side, Nigeria is faced with a myriad of problems including political instability, crime and terrorism, poverty, unemployment and corruption. However, chief among these problems is corruption. Everyone seems to agree that the country has "a culture of corruption".[142] From public officers who abuse their public offices for personal gain to citizens who offer gratification to change the standards to suit their purpose, it is a fact that corruption has permeated all facets of Nigeria's national life.[143]

The effects of corruption are myriad.[144] It negatively impacts economic growth as government expenditure for the provision of basic social services such as health, education and infrastructure for its citizens[145] is diverted into private pockets. In the health sector in Nigeria, the effects are 'corrosive'.[146] Monies meant for the health sector are diverted by corrupt public officials and misappropriated to serve individual interests.[147] This comes with consequences. In many places in Nigeria, hospitals have become dilapidated structures with no health supplies. In some tertiary health centres, water supply is not available and patients' relatives resort to buying water in jerry

---

[141] *Ibid* at 20.

[142] Daniel Jordan Smith, *A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria* (Princeton: Princeton University Press, 2008); Farida Waziri, *Corruption and Governance Challenges in Nigeria* (Lagos: Cleen Foundation, 2010).

[143] Usman Mohammed, "Corruption in Nigeria: A challenge to sustainable development" (2013) 9 European Scientific Journal 118 at 123-31.

[144]Victor Dike, "Corruption in Nigeria: A New Paradigm for Effective Control", online: African Economic Analysis< http://www.africaeconomicanalysis.org/articles/gen/corruptiondikehtm.html>.

[145] Asaju Kayode, Sunday Onah Adagba & Silas Felix Anyio, "Corruption and service delivery: the case of Nigerian public service", online :(2013) 1 Wudpecker Journal of Public Administration< http://www.wudpeckerresearchjournals.org/WJPA/pdf/2013/July/Kayode%20et%20al.pdf> .

[146] Idris Akinbajo, "The Massive MDG Fraud: How the Health Ministry Steals From The Sick and Dying",*SaharaReporters*(20 July 2012) online: Sahara Reporters <http://sahrareporters.com/2012/07/20/massive-mdg-fraud-how-health-ministry-steals-sick-and-dying-premium-times >.

[147] *Ibid* .

cans, while in some instances, health workers have to wait endlessly for minor supplies, such as disposable gloves.[148]

As a result of this poor state of the health system, a sizeable portion of Nigerian medical practitioners migrate to the US and UK each year[149] to seek better economic standards and conditions for the practice of their trade. Many of the few medical practitioners left in the country prefer to practise their trade in the commercial centres of Lagos, Abuja and Port-Harcourt, with the rural areas being underserved in terms of healthcare provision and access.[150]

The effects on the country's health profile are disturbing. The average life expectancy in Nigeria is fifty-two years,[151] which makes it the seventeenth lowest in the world. Apart from this, there is a high prevalence of infectious and communicable diseases in Nigeria. With three hundred thousand deaths annually, Nigeria carries the world's largest burden of malaria,[152] and communicable diseases like tuberculosis, measles, and chicken pox are leading causes of mortality and morbidity in Nigeria. Unfortunately, access to health services is very poor, [153]and coupled with ill-equipped health centres, the people, especially the rural poor die from diseases that could have been cured if the health centres were well-equipped.

---

[148] Benjamin Ogbebulu, "The Sorry State Of Nigeria's Health Sector and the Agitation For A 21st Century Comprehensive Health Care Delivery System In Nigeria", online: Gamji<http://www.gamji.com/article6000/NEWS7105.htm>.

[149] According to the President of the Nigerian Medical Association, out of the 71, 740 medical practitioners listed on the register of the Medical and Dental Council of Nigeria, only 27,000 are currently in Nigeria with about 40,000 of that number reportedly practicing in the United States of America. See generally "Brain Drain: Read How Nigeria Turned a Manufacture[r] for Medical Doctors Production", (17 November 2013) online: Informed Minds Blog< http://www.naij.com/47348.html>.

[150] "Human Resources for Health: Country Profile", online: United Nations Population Fund<http://www.unfpa.org/sowmy/resources/docs/library/R050_AHWO_2008_Nigeria_HRHProfile.pdf>.

[151]World Health Organization, *supra* note 133.

[152] "Key Malaria Facts", online: Roll Back Malaria<http://www.rbm.who.int/keyfacts.html>.

[153] Adewale Stephen Bakare, "The crowding-out effects of corruption in Nigeria: An empirical study" (2011)2 Journal of Business Management and Economics 59 at 60.

To address the multiple health challenges, the government of Nigeria, like other countries in Africa, is exploring new approaches to reform the country's health sector with a view to expanding access to healthcare services and eradicating treatable diseases.[154]In the European context, the Economist Intelligence Unit, identified one of these approaches in the growing reliance on technology solutions to improve access and service delivery.[155]Video conferencing for cross-border consultations with specialists and mobile phone technology are leading examples of this technology use in healthcare. For the purpose of this chapter however and in line with the theme of this thesis, the discussion is limited to the use of mobile technology in healthcare.

This chapter describes the context in which the use of mobile technology in healthcare occurs. mHealth offers promise in reducing the disease burden in Nigeria. The ubiquity of mobile phones can also help improve access to health care in remote communities. However, beyond its benefits, there are privacy concerns in mHealth. Health information contains some of the most sensitive pieces of information and, within an African context such as Nigeria, the risk of misuse could open an individual to persecution or discrimination.

To ultimately seek to provide a privacy framework for mHealth in Nigeria, this chapter identifies those socio-cultural factors in Nigeria that may present as problems to the consideration of the framework.

---

[154]"The future of healthcare in Europe" *The Economist*, online: The Economist<http://www.economistinsights.com/sites/default/files/downloads/EIUJanssen_HealthcareAfrica_Report_Web.pdf >.

[155] *The Economist*, *supra* note 154.. It is pertinent to note that this report highlighted five approaches for reforming the healthcare or shaping the direction of the healthcare in Europe in the next two decades. The report noted that the future of healthcare would be shaped by technology use in healthcare delivery, the emergence of a pan-European healthcare system, a shift in government focus from funding treatments to promoting wellness of its citizens, reduction in health inequalities and privatization of the healthcare systems across Europe, However, in keeping with the theme of this thesis, one of them, the impact of technology use on healthcare, is highlighted here.

3.2 Mobile Health (mHealth) in Nigeria

3.2.1 Background to the Mobile Market in Nigeria

As discussed in chapter two, the Global Observatory on eHealth defines mHealth as "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices".[156] However, as will be seen, mHealth in Nigeria is basically driven by mobile phones as opposed to other categories of mobile devices.

At the basic level, mobile phones serve as a means to connect people irrespective of geographical divide or location. This means of communication is being harnessed in support of many development initiatives especially in the developing countries, in areas such as agriculture, banking, health, and as tools for improving governance systems in different parts of the world.[157] In the literature analysing the use of mobile phones based services as a tool for economic development, the World Bank identified key areas in which mobile telephony is leading economic, social and political developments in the developing countries[158] by its ability to connect individuals to individuals, information, markets and services.[159]

In Nigeria, the use of mobile phones as a tool for economic and social development is driven by an increased penetration of mobile networks into most parts of the country.[160]Figures from the Nigerian Communications Commission, the regulatory body for the telecommunications industry

---

[156] mHealth: New Horizons,*supra* note 45.

[157]Jenny C Aker & Isaac M Mbiti, "Mobile Phones and Economic Development in Africa", online :(2010) 24 Journal of Economic Perspectives 3< https://www.aeaweb.org/articles.php?doi=10.1257/jep.24.3.207 >.

[158] *Ibid.*

[159] *Ibid.*

[160]Pyramid Research, *The Impact of Mobile Services in Nigeria: How Mobile Technologies are Transforming Economic and Social Activities,* online: Pyramid Research <http://www.pyramidresearch.com/documents/IMPACTofMobileServicesInNIGERIA.pdf >.

in Nigeria, shows a subscription rate of one hundred and twenty six million active mobile subscribers for March 2014,[161] the highest penetration when compared to any other country in Africa.[162]

In part, the reason for this is the increasing affordability of basic or feature phones, with typically voice calling and text-messaging functionalities.[163] Before now, landline telephones were the 'exclusive preserve of the rich and mighty'; persons of lower income had no access to this means of communication. It was considered a status symbol rather than a necessity. However, the arrival of mobile technology and, consequently, cheap and basic phones means lower income individuals could own this hitherto expensive means of communication.

Another reason is the improved network of mobile coverage, especially in the remote and rural areas of Nigeria. In the past, telecommunications companies in Nigeria were reluctant to make in-roads into the rural areas and hinterland due to poor terrains and lack of electricity access to power their networks.[164] However, it was identified that there was a need to extend the telecom boom to the rural communities so as to encourage growth in these areas and to reduce the rate of rural-urban migration.[165]

---

[161]Nigerian Communications Commission, *Monthly Subscriber Day (May 2013-April 2014),* online: Nigerian CommunicationsCommissionhttp://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125&Itemid=73.

[162]Deloitte, *Sub-Saharan Africa Mobile Observatory 2012*, online: GSM Association <http://www.gsma.com/publicpolicy/wp-content/uploads/2013/01/gsma_ssamo_full_web_11_12-1.pdf>.

[163] See "An analysis of Mobile Technology in West Africa: The Case of Nigeria, Ghana and Cote D'Ivoire"online: research ihub < http://research.ihub.co.ke/uploads/2012/october/1351001605_819_249.pdf >.

[164] Andrew Onwuemele, "Impact of Mobile Phones on Rural Livelihoods Assets in Rural Nigeria: A Case study of Ovia North East Local Government Area "online :(2011)9:2 African Journals Online <http://www.transcampus.org/JORINDV9Dec2011/Jorind%20Vol9%20No2%20Dec%20Chapter30.pdf>.

[165] *Ibid.*

Consequently, there are many development initiatives in Nigeria that leverage on the connectivity provided by mobile phones to provide services in health, education, governance and in the financial services sector.[166]

An overview of the use of mobile phones for health services in Nigeria is provided next. The description provides a broad context for discussing the privacy implications of the use of mHealth in Nigeria.

3.2.2 mHealth in Nigeria: Overview and Privacy Risks

The challenges in Nigeria's health sector in terms of the quality of healthcare delivery and access led to innovative ways of achieving health through the cost-effective technology offered by mobile phones.

mHealth in Nigeria, as in most developing countries, is delivered via mobile phones as opposed to smart devices, such as patient monitoring devices and personal digital assistants. These smart devices rely on the latest mobile data infrastructure some of which are not available in these countries[167] to provide some mHealth service.[168] As such mHealth platforms in these countries utilize the less complex infrastructure of SMS or text messaging.

Text messaging or SMS is a most popular route for mHealth applications because of its ubiquity. Gold et al, note that text messaging is the technology of choice for mHealth. According to them:

> Text messages (SMS) are a highly promising method of health promotion for multiple reasons. They are widely available and accessible; in 2009 it was estimated that there were 3.6 billion global users of SMS,

[166] Pyramid Research, *supra* note 160.

[167] Kristel Teyras, "SMS innovation and dynamic mobile content drives mHealth initiatives in Africa",*Gemalto's Blog*(16July 2014)online:Gemalto.com<http://blog.gemalto.com/blog/2014/07/16/sms-innovation-and-dynamic-mobile-content-drives-mHealth-initiatives-in-africa/#sthash.ZfgwXzGp.dpuf>.

[168] Alex Krouse, "iPads, iPhones, Androids and Smartphones: FDA Regulation of Mobile Phone Applications as Medical Devices" (2012)9 Indiana Health Law Review 731 at 733-35.

> double the number of internet users. Most mobile users have their mobiles turned on, and in reach during waking hours. Messages can be sent to multiple recipients simultaneously and delivered immediately...and the cost of sending text messages is relatively low.[169]

The above is true for Nigeria. A 2014 GSMA Report on mHealth in Nigeria shows that out of forty-five clearly identified mHealth services in Nigeria, most are through text-messaging. A text-based mHealth service to support maternal nutrition and child health has been shown to reach as many as four million women in different parts of the country.[170] These text messages are distributed in the local Nigerian languages understood with ease by the local people.

In many mHealth services across the country, text messaging is being successfully used to disseminate health information.[171] For example, in 2012, an initiative known as *ICT for Saving One Million Lives (ICT4SOML)* was launched by the Federal Government of Nigeria in conjunction with organizations such as the UN Foundation and the GSM Association.[172] The aim of the initiative is to reduce infant and maternal mortality by providing relevant information to pregnant and nursing women using the mobile technology infrastructure already available in the country.[173] Thus, toll-free information about what to expect during and after pregnancy are provided via SMS to pregnant and new mothers. The initiative ambitiously intends to save the

---

[169]Judy Gold et al, "What's in a message? Delivering sexual health promotion to young people in Australia via text messaging", online :(2010)10:792 BMC Public Health <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3022861/>.

[170]GSMA Mobile for Development, "mHealth Country Feasibility Report: Nigeria", online: GSM Associationhttp://nigeria.gsmamHealthfeasibility.com/GSMA_Country_Feasibility_Report_Nigeria_2014.pdf >.

[171] Erin McCann, "WHO credits mHealth app with helping Nigeria get rid of Ebola", *mHealth News* (24 October, 2014) online: mHealth News < http://www.mHealthnews.com/news/who-credits-mHealth-app-helping-nigeria-get-rid-ebola>.

[172] See Clinton Foundation, News Release, "The Government of Nigeria Launches "Saving One Million Lives" with support from CHAI"(17 October 2012)online: Clinton Foundation https://www.clintonfoundation.org/main/clinton-foundation-blog.html/2012/10/17/the-government-of-nigeria-launches-saving-one-million-lives-with-support-from-chai>.

[173] "ICT4SOML: Leveraging ICTs to Save the Lives of One Million Women and Children in Nigeria"(11 February 2013),online: Health Level Seven <http://wiki.hl7.org/images/5/5c/SOML_Situational_Analysis_FINAL_20130909.pdf>.

lives one million such women considering the country's high burden of maternal and child mortality.[174]

Some others use text messaging as a tool for two-way communication between mHealth users and healthcare providers or health workers. For example, *Learning about Living* uses its *My Question* service to provide information via SMS to educate young people about their reproductive and sexual health.[175] Through this platform, young people can ask questions and receive individualized responses about sexual health based on the information provided.[176]

It is instructive that a 2013 study by Joseph Isabona to measure the use of mobile phone technology in healthcare services in two local government areas of Ekpoma in Esan West and Irrua in Esan Central respectively of Edo State in Midwest Nigeria showed diverse uses of mobile phones. Majority of participants confirmed using their mobile phones to receive text messages on public health alerts; to text nurses, doctors and community health workers as well as to receive medical reminders.[177]

Similarly, community health workers can track and record data using information provided via text messages. For example, research by the United States Agency for International Development (USAID) to review the quality of support provided through mobile technology for community health extension workers involved in ante-natal care services found that a significant number of

[174] United Nations Foundation, "Assessing the Enabling Environment for ICTs for Health in Nigeria: A Landscape and Inventory", online: UN Foundation < http://www.unfoundation.org/assets/pdf/nigeria-landscape-report.pdf>.
[175] One World, "Learning about Living – Using cross-media technology to empower young people with reproductive health and life skills"online:OneWorld < http://oneworld.org/2014/08/21/learning-about-living-using-cross-media-technology-to-empower-young-people-with-reproductive-health-and-life-skills/>.
[176] Ann K Blanc et al, "Myths and misinformation: An analysis of text messages sent to a sexual and reproductive health Q&A service in Nigeria", online: Population Association of America < http://paa2014.princeton.edu/papers/141862>.
[177] Joseph Isabona, "Harnessing Telecommunications Revolution in Nigeria: A Case Study" (2013) 1 Wireless and Mobile Technologies 20 at 21-22.

community health extension workers used the mobile health platform, COMMCARE, to track and record data provided by their ante-natal care clients. The information are recorded via 'mid-range phones' and then submitted to the server of COMMCARE and "accessible to supervisors and program managers around the world".[178]

Although the above studies have limited their scope to assessing the potential of mHealth in Nigeria, some things are apparent: health information is provided by mHealth users for particular purposes and this information may become available to a number of parties such as the mHealth provider, the telecommunications company, international funding bodies and agencies or even the government in regard to mHealth services established by the government.[179]

In spite of its potential, there is, as yet, no best practice to inform public policy or law in this area. The implication is that mHealth in Nigeria is an unregulated sphere.[180]

For example, there is a high concentration of foreign sponsors and international funding agencies. Organizations such as UK Aid, the Norwegian Agency for Development Cooperation (NORAD),[181] the United States Agency for International Development (USAID) and non-profits such as the Bill and Melinda Gates Foundation, provide funding and support for mHealth services in Nigeria as in many countries in Africa. Telecommunication companies in Nigeria are also involved with mHealth in Nigeria. They either provide a direct mHealth service or provide the platform or connectivity for the delivery of an mHealth service.

---

[178]USAID, *A DIV-funded start-up becomes a leading solution for mobile health,* online: USAIDhttp://www.usaid.gov/div/commcare>.

[179]Ayo Bamgboye, "Ondo State use Mobile phones to Improve Maternal and Child Health", *Africa Health IT News* (11 July 2012) online: Africa Health IT News <http://africahealthitnews.com/blogs/2012/07/ondo-state-use-mobile-phones-to-improve-in-maternal-and-child-health/>.

[180] Paul Adepoju, "Doctors warn against uncertified health tips", *Health News NG* (22 January 2014) online: Health News NG<http://www.healthnewsng.com/2014/01/nigerian-doctors-warn-against.html>.

[181] See mHealth Country Feasibility Report, *supra* note 170.

The lack of regulation comes with perilous implications.[182] According to Anna Crowe,[183] persons using services provided via mobile devices in low resource settings are ignorant of the privacy risks to their use. For instance, while foreign sponsors or international funding bodies may see the provision of mHealth as a development initiative, it also raises questions about the use or the potential uses of the information provided by users. Huge volumes of data can be collected or generated from information provided by users of mHealth other than for the purpose for which they were provided. Otherwise known as 'big data'[184], health information provided through millions of mHealth users can positively contribute to public health as they can be analysed and used to track outbreaks of epidemics and to predict when infections would peak.[185]

On the flip side, this wealth of data could also be misused by actors whose intent may be to exploit mHealth for their own ends.[186] In some instances, misuse could lead to discriminatory outcomes[187] for example, where a group of people have a diseased condition, it is possible that the availability of this information to a foreign body or sponsor via mHealth could shape diplomatic or foreign relations with such a group or individuals.

Telecommunications companies that provide mHealth services would usually have the records of the individual's name, address, their health information if using a mHealth service directly provided by the company, or that the individual would be using a mHealth service for which they

---

[182] Anna Crowe, "The promise, and problems, of mobile phones in the developing world"(1 November 2013)online: Open democracy< https://www.opendemocracy.net/opensecurity/anna-crowe/promise-and-problems-of-mobile-phones-in-developing-world>.

[183] *Ibid.*

[184] Min Chen et al, *Big Data: Related Technologies, Challenges and Future Prospects* (Cham: Springer, 2014) at 2-5.

[185]Norman Rozenberg, "Big data: Benefits, drawbacks in addressing Ebola" (20 August 2014) online: Tech Page One<http://techpageone.dell.com/technology/big-data-benefits-drawbacks-in-addressing ebola/#.VBwl1PldVps>.

[186] *Ibid.*

[187] John Podesta, "Findings of the Big Data and Privacy Working Group Review (1 May 2014) online: The White House Blog <http://www.whitehouse.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review>.

provide connectivity. Privacy threats in this sphere could assume different forms. It could be an employee with data access privileges who pries into information provided by a mHealth user without any legitimate need, or to access potentially damaging health information provided by the user. It could also be an unauthorized person who infiltrates the telecommunications company network with the aim to steal data.

Another scenario is the opportunity presented for surveillance by the government. In countries such as Nigeria where there are laws[188] mandating Subscriber Identity Module (SIM) card registration by all mobile users, there is a risk that anonymous information provided by an mHealth user could be converted to personal information. With SIM registration, mobile users are required to provide personal details including biometrics, to the telecommunication companies.[189]According to the government, the advantages of SIM registration are diverse. Among other things, it could help track criminals who seize the opportunity of undocumented use of SIM card in Nigeria to their commit crimes; [190]help to develop a comprehensive database of Nigerians that could assist in verification of identities.

While the SIM registration law allows for collection of personal information may be lawful, and, usually the terms of service between telecommunication companies and their subscribers allow the companies to collect personal information, [191]anecdotal evidence suggests that as with other

[188] See *Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations,* 2011.
[189] *Ibid* at Part III.
[190] Bonnie Onukwube, "Why SIM Card Registration Exercise Needs to Succeed", *Daily Trust* (25 June 2012)online:allafrica.com<http://allafrica.com/stories/201206250697.html>;See also Kevin Donovan & Aaron Martin, "The Rise of African SIM registration: The emerging dynamics of regulatory change", online:(2014) First Monday 2 at para 3<http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820>.
[191] Perhaps an apt example is provided by MTN Nigeria, a major telecommunications company in Nigeria. Its privacy policy allows it to collect customers' personal information when mobile applications are downloaded by customers. See MTN Nigeria, *Privacy policy*, online: MTNOnline<http://nextapps.mtnonline.com/index/page/id/24>. See also *Registration of Telephone Subscribers Regulation,supra* note 188.

agreements, there is no evidence that users read or even understand these terms.[192] Thus, for an mHealth user who has provided their health information without reading or understanding such terms, the implication is that since SIM registration links every mobile device to a specific citizen, their health information, can easily be linked to their name, address or other personal information provided. Professor Sweeney's[193] seminal research has shown the limitations of anonymization and the possibility of re-identifying an individual from anonymous data by combining them with other bits of data. For mHealth, the risk is that details from SIM registration may be linked to the anonymous health information to serve some 'ends' by government agencies or law enforcement bodies.

In the political context, SIM registration is already being used for inappropriate ends. In Zambia, the ruling political party used the personal details of individuals registered with a mobile service provider to bombard mobile phone users with unsolicited messages canvassing for votes.[194] The implication for mHealth is that security or government agencies can trace an mHealth user, even where health information was anonymously provided, so long as the SIM was registered to the user by the telecommunications company.

---

[192] Ajibola Amzat, "How Telecom Firms Cheat, Frustrate Subscribers", *The Guardian* (22 December 2014)online: The Guardian http://www.ngrguardiannews.com/lead-story/191314-how-telecoms-firms-cheat-frustrate-subscribers>; Nduka Chiejina, "CBN recovers N8.6b for bank customer",*The Nation* (16 April 2013) online: The Nation http://thenationonlineng.net/new/cbn-recovers-n8-6b-for-bank-customers/>.

[193] Recommendations To Identify and Combat Privacy Problems in the Commonwealth: Hearing on H.R. 351 Before the H. Select Comm. on Info. Sec., 2005 Gen. Assemb., 189th Sess. (Pa. 2005), http://dataprivacylab.org/dataprivacy/talks/Flick-05-10.html. See also Ann Cavoukian & Khaled El Emam, *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy* (Ontario: Information and Privacy Commissioner of Ontario,2011) at 4 where the authors suggest that although anonymization is a good method of protecting privacy, however, anonymization techniques are not entirely iron clad.

[194] "PF using details of SIM registration to campaign, distributing cash", *Zambian Watchdog* (20 February 2013) online: Zambian Watchdog <https://www.zambianwatchdog.com/pf-using-details-of-sin-registrion-to-campaign/>.

Furthermore, although it is true that mHealth may help to improve access to healthcare in remote or rural communities, it is pertinent to reflect on the privacy implications where mobile phones are shared among family members. According to figures released by the International Telephone Union (ITU), Africa has the highest mobile penetration rate. However, according to de Silva & Zainudeen, the statistics may actually be misleading as the shared use of mobile phones, which is a popular phenomenon in developing countries, makes the notion of a subscriber complicated.[195] In some contexts, the dominant male in the household (usually the father) who owns the phone shares it with other members of the family,[196] while in some poor communities, mobile phone owners share their phones with other members of the community.[197] In Botswana, for example, household surveys reveal that 62.1% of the phone owners share their phones with their family, 43.8% with their friends and 20% share their phone also with their neighbours.[198]

Although no such statistic exists for Nigeria, informal sharing of mobile phones is the reality in most rural communities where the low income status of many households forces family members and relatives to share the use of their mobile phones. The informal sharing of mobile phones between people could have implications for mHealth. For example, it could give access to others regarding the HIV test results of a mHealth user when their information is relayed through a shared mobile phone or through reminders for treatment adherence[199] for health conditions such as HIV/AIDS that are still considered as taboo in Nigerian society. This could have serious

---

[195] Harsha de Silva & Ayesha Zainudeen, eds, *Teleuse on a Shoestring: Poverty Reduction Through Telecom Access at the 'Bottom of the Pyramid': Annual Symposium on Poverty Research for the Centre for* Poverty *Analysis, Colombo, 2007.*

[196] Anna Crowe, *supra* note 182.

[197] Jeffrey James & Mila Versteeg, "Mobile phones in Africa: how much do we really know?",online: (2007)84 Social Indicators Research <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2806217/>.

[198] *Ibid.*

[199] Benjamin H Chi & Jeffrey SA Stringer, "Mobile phones to improve HIV treatment adherence", online: (2010) 376:9755 The Lancet < http://www.sciencedirect.com/science/article/pii/S0140673610620466>.

implications for the social relations or acceptance of the mHealth user where the information gets into the wrong hands.

Given the current trend in the use of mHealth services in Nigeria, the question becomes what protection, if any, is available to protect the users? As indicated in Chapter One, the aim of this thesis is to consider whether the EU regime works to protect mHealth privacy in Nigeria. Bearing this in mind and being cognizant of the cross-cultural differences which may exist between the two jurisdictions, the rest of this chapter focuses on those socio-cultural peculiarities of Nigeria that may affect notions of privacy. The examination of these factors is for determining whether they may constitute a problem or challenge to argue, as this thesis does, that privacy protection for mHealth users in Nigeria can be secured by adopting the EU privacy regime.

3.3 Socio-Cultural Context of Privacy in Nigeria

In Geert Hofstede's research project on relativity of culture, four criteria[200] are used to explain the values by which cultural differences between countries can be measured. One of these is the relationship between the individual and the group which he labelled as 'individualism versus collectivism'.

According to Hofstede, this dimension represents the extent of relations between an individual and other members of society. In individualized societies, members have loosely knit relationships and everyone looks after their own self-interest and that of their immediate families. In collectivized societies, members are more tightly integrated and people are born into

[200] These dimensions are individualism versus collectivism; power distance including social inequalities; uncertainty avoidance referring to how the members are socialized into dealing with uncertainties and the masculinity versus feminism dimension referring to how the society prescribes roles to the male and female gender. See Geert Hofstede, "The cultural relativity of organizational practices and theories" (pre-1986)14 Journal of International Business Studies 75 at 79-83.

collectivities or groups comprised of extended family members and everyone looks after the interest of other members of the group and aligns themselves with the opinion and beliefs of the group. Hofstede's analysis shows that Nigeria is a collectivized society because it scored lower than other countries on the individualism dimension.[201]

Another dimension from Hofstede's analysis is masculinity/feministic aspect. Although Hofstede's research focused on how differences in culture could impact work-related values, his findings show that culture is relative and differs from one cultural setting to the other. Thus, in cultures with strong individualism indexes, there is higher value placed on the right to privacy as compared to cultures with a lower individualism index.[202] Further, based on his masculinity/femininity dimension, Nigeria is a masculine society as it stresses ambition and acquisition of wealth as masculine roles and nurturing or modesty as feminine roles. Against the background of Hofstede's work, it is necessary to investigate the cultural context in Nigeria and how it affects the consideration of a privacy framework for protection of health information.

3.3.1 Culture as a Factor

Culture is defined as the sum total of knowledge, attitudes and habitual behaviour patterns shared and transmitted by the members of a particular society.[203] This pattern when shared and transmitted over a period of time determines the way of life of the people. Culture prescribes what is acceptable within society in terms of the morals or standards of conduct that define the society's value system.The view is that within this notion of morals or standards, conception of

[201] Nigeria scored 30 on Hofstede's cultural survey.
[202] Sandra J Milberg, Jeff Smith & Sandra J Burke, "Information Privacy: Corporate Management and National Regulation" (2000) 11 Organization Science 35 at 40.
[203] Ralph Linton, *The Cultural Background of Personality* (New York: Appleton-Century Co., 1945) at 32.

rights, is determined by culture. This is the relativist view, and it holds that different cultures hold different moral views and have ethical standards on what is 'good' or 'bad'.[204]

Cultural relativists think that the western conception of human rights is strange to African cultures.[205] According to them, collectivist cultures unlike individualistic societies stress a 'we' consciousness. They emphasize such values as group solidarity, sharing, group decisions, duties and obligations, and minimize individualistic or atomistic attitudes.[206] These societies are strong and cohesive, and primacy is given to societal norms and practises which promote social harmony. In the result, people in such societies are often concerned about their roles in meeting the expectations of other members of the group and how to maintain social harmony.

The above is what Kwame Gyekye conceives as the notion of 'community' in traditional African societies. In his work, *Tradition and Modernity - Philosophical Reflections on the African Experience*, he notes that a "sense of community"[207] characterizes social relations among individuals in African societies. According to him, underlying this sense of community is sharing an overall way of life. Individuals within the community are aware that each has particular roles and obligations to play within the social context, which may be a family (nuclear and extended), the clan, the village, tribe or neighbourhood.[208] Through this sense of community, members are nurtured on common beliefs, attitudes, and actions which are required to make life orderly and peaceful within the community. The effect is that societal norms and rules of behaviour favour a

---

[204]See Xiaorong Li, *Ethics, Human Rights and Culture: Beyond Relativism and Universalism*(Basingstoke: Palgrave Macmillan, 2006)at 55.An example is provided about honour killings, a socially and morally accepted homicide in Pakistan where a woman regarded as bringing dishonor to her family is killed, whereas killing anyone is unacceptable in other societies.

[205]Serge Gurtwirth, *Privacy and the Information Age* (Oxford: Rowman & Littlefield Publishers, 2002) at 24.

[206]Uichol Kim, *Individualism and Collectivism: A Psychological, Cultural and Ecological Analysis* (Copenhagen: NIAS Books, 1991) at 4.

[207] Kwame Gyekye, *Tradition and Modernity - Philosophical Reflections on the African Experience* (Oxford: Oxford University Press, 1997) at 36.

[208] *Ibid.*

culture of sharing and openness in ways that may be inconsistent with claims to control one's health information under privacy legislation.

Gyekye's concept of the community is deeply entrenched in Nigeria as it is in many African countries.[209] Unlike some of these countries, Nigeria is a culturally diverse society comprising over 400 ethnic groups.[210] Each has its own ethnic origins, languages, traditional practices and customs that vary from each to the other. Notwithstanding the diversity, there is a strand that seems to connect all of the cultures of Nigeria, namely the deep sense of community that exists within the family system. The family structure in Nigeria is based on a consciousness in which members of the community see and relate to each other as brothers, sisters, mothers, fathers and so on.[211] In other words, the definition of family is not limited to the nuclear structure of the father, mother and children, it extends to kinship relations with members of the clan or lineage.

In this context, it is the responsibility of each member of the extended family to work towards protecting the wellbeing of other members, and, thus, the interests of the family as a whole. The impact of group support systems affect what may be viewed as 'private 'or what an individual would want to keep from other members of the family. For example, in the care of a patient diagnosed with HIV/AIDS, it is not uncommon for relatives and extended family members to be informed of the person's status in order that they rally to source traditional herbal 'remedies' or

[71]This concept has been variously termed in different countries or regions of the continent. In South Africa, it is expressed in Xhosa as 'Ubuntu'; in Zimbabwe, it is expressed in the majority Shona language as 'Unhu'; in South Sudan expressed in the Dinka language as 'Cieng'; Ujamaa in Tanzania.

[210] B Salawu, "Ethno-Religious Conflicts in Nigeria: Causal Analysis and Proposals for New Management Strategies" (2010) 13 European Journal of Social Sciences 345.

[211] Joseph CA Agbakoba, "An Evaluation of Theophilus Okere's conception of the place of African Traditional Values in Contemporary African Societies" in J Obi Oguejiofor and Godfrey Igwebuike Onah,eds, *African Philosophy and the Hermeneutics of Culture: Essays in Honour of Theophilus Okere* (Piscataway: Transaction Publishers, 2007) at 240.

a 'cure' for his ailment. This is so that the entire family is not stigmatized as an 'AIDS family' by other villagers.[212]

Also, because individuals have particular roles they play in Nigerian society, males and females have culturally defined gender roles.[213] The Nigerian culture is essentially heterogeneous, but it is homogeneous in terms of the patriarchal views on roles for men and women.[214] For instance, gender roles for men class them as having strength, vigour, self-confidence and intelligence.[215] Society views them as decision makers, breadwinners and heads of their households. On the other hand, women serve a subordinate status under men. Traditional norms and practices expect them to defer to the men in family, marriage, religion, education and participation in political life.[216] A process of socialization from childhood ensures that a woman is taught to be obedient, submissive and meek as part of their 'femaleness'.[217] This is true for women in Northern Nigeria, where as a result of the prevailing influence of Islam, a woman is socialized from birth to think of herself as the weaker, requiring the control of her father and brothers while young, and immediately she marries, to become the possession of her husband and in-laws.[218]

---

[212]O Alubo et al, "Acceptance and stigmatization of PLWA in Nigeria", online: Taylor and Francis <http://www.ncbi.nlm.nih.gov/pubmed/11798411>.

[213] Abidemi R Asiyanbola, "Patriarchy, male dominance, the role and women empowerment in Nigeria"(Paper delivered at the International Union for the Scientific study of Populations Conference, Tours, France,21 July 2005),[unpublished].

[214] Kola A Oyediran & Ayodele F Odusola, "Poverty and the Dynamics of Women's Participation in Household Decision-Making in Nigeria", online :(2004)19 African Population Studies<http://www.bioline.org.br/pdf?ep04023>.

[215] *Ibid.*

[216]Maureen Kambarami,"Femininity, Sexuality and Culture: Patriarchy and Female Subordination in Zimbabwe", online: African Regional Sexuality Resource Centre<http://www.arsrc.org/downloads/uhsss/kmabarami.pdf>.

[217]Dr C Otutubikey Izugbara, "Patriarchal Ideology and Discourses of Sexuality in Nigeria", online: African Regional Sexuality Resource Centre http://www.arsrc.org/downloads/uhsss/izugbara.pdf>.

[218]Morire OreOluwapo Labeodan, "The Family Lifestyle in Nigeria", online: Princeton< http://paa2005.princeton.edu/papers/51248>.

Cultural taboos and the influence of religion have contributed to these gender stereotypes and roles in society. For example, in most communities in Nigeria, it is a taboo to think of women being in charge of a communal shrine. This is not to say that there are not priestesses of some shrines in some places. However, religious rituals even in those shrines such as the invocation of the ancestors for blessing and protection, are usually left to the men.[219] No woman dares to attempt to perform this ritual, even if she is the eldest and most religious in the community. These taboos carry into the political life, women are perceived as being unworthy to govern or exercise political power in society. For instance, Essien & Ukpong report a popular saying in Akwa Ibom state of Nigeria that "*owo-nwanisidataanyin, asidatitit*" which literally means that a woman can only be active in bed as opposed to participating in the public domain or politics.[220]

Religious beliefs and practices also engender the subjugation of women. Nigeria is a deeply religious society, comprised of the Muslim-dominated north and the predominantly Christian south.[221] The Koran and the Bible form the textual bases for practice of patriarchy. Religious narratives from these holy books ascribe superiority of men over women, sometimes in subtle ways, by depicting the woman as the 'weaker sex'[222]whose role is to bear children[223] and comfort her husband and obey him at all times.[224]In turn, the man is expected to love and cater for his wife and fulfil all her needs.

---

[219] Anthonia M Essien & Donatus P Ukpong, "Patriarchy and Gender Inequality: The Persistence of Religious and Cultural Prejudice in Contemporary Akwa Ibom State, Nigeria", online :(2012) 2 International Journal of Social Science and Humanity 4 < http://www.ijssh.org/show-31-406-1.html>.

[220] *Ibid.*

[221] "Religion in Nigeria" online: Wikipedia <http://en.wikipedia.org/wiki/Religion_in_Nigeria>.

[222] See *The Bible New International Version* (Colorado Springs: Biblica, 2011) at Genesis Chapter 2 verse 23 [Bible].

[223] *Ibid* at Chapter 3 verse 16.

[224]See Imam Hassan Kalil, *Wife Obedience to Husband in Islam,* online: MyDeenIsIslam http://www.mydeenislam.com/wife-obedience-to-husband-in-islam.html> in his interpretation of *The Qu 'ran*, (4:34).

This patriarchal arrangement carries into the capability of women to take decisions concerning their own health. Societal roles and religious expectations also require that the woman defers to the man in the family. For example, with regards to her reproductive choices, she has little or no control. She cannot refuse to have sexual relations with her husband, as culture and religion frown on it.[225] In some cases, the man may take an additional wife if she refuses him. She is expected to be fertile and produce children. Her role is to perpetuate the lineage of her husband by producing strong, preferably male children. Even when she has had multiple births of female children, she cannot seek contraceptive advice without the consent of her husband. Where she has only female children, she is pressured by her husband and in-laws to try for a male child by having more children, in some cases putting her in danger.[226]

A woman in the above scenario who seeks contraceptive advice from a mHealth service would be fearful of the consequence of such information getting into the wrong hands. She would want to keep it 'secret' to prevent being subjected to societal ridicule or chased from her matrimonial home by her husband or in-laws, or from being disowned by her own family members for bringing dishonour and shame to the family name.

Similarly, because the man, in most cases, has the sole control of the economic resources of the home, there is the tendency that her capacity to make decisions, even a decision as to whether to purchase a mobile phone, is dependent on his consent. A study by Oyediran & Olusola notes that apart from the traditional norms and practices which relegate Nigerian women and limit their capacity to make decisions in the household, the sole control of economic resources by the

[225] Bible, *supra* note 222 at 1 Corinthians Chapter 7, verses 2-5.
[226]Chinyere Elele,"Nigeria: Male Child Remains a Family Pride and Honour", *Inter Press Service* (29 May 2002)online: Inter Press Service <http://www.sos-sexisme.org/english/male_child.htm>.

men,especially in the rural areas, also contributes to this.[227] The women have limited finances and this may hinder their ability to purchase a mobile phone or have access to mHealth services. At other times, they may share the use of their mobile phones with their husbands or some other family member such that privacy to exclusively access a mHealth service to seek contraceptive advice cannot be guaranteed. The implication is that the woman has to seek decisional control, the most basic safeguard of her privacy, from the men at all times.

From the foregoing, the cultural context for mHealth privacy in Nigeria presents a challenging scenario. A decision made to withhold one's health information from other members of one's family may be seen as cutting oneself off from other family members who interfere as part of their responsibility to take care of other family members. As noted earlier, there are circumstances they may demand to know the health status of a family member from a physician for a disease such as HIV/AIDS which may likely open the family to ridicule or discrimination from other members of society.

Similarly, for a woman for whom cultural practices and beliefs have placed her in a subordinate position to her husband, she cannot decide to keep information relating to her health from him or from some male member of the family consequently, for her to make a decision to obtain some health advice requires the consent of these men. In other situations, economic factors may limit her capacity to obtain a mobile device to enable her to make her own choices. For her to insist on the privacy of her health information in these circumstances may lead to problems in her marriage and subject her to ridicule and scorn.

[227] Oyediran & Olusola, *supra* note 214 at 116.

Clearly, the influence of the extended family, social obligations and values cannot be divorced from what is private to an individual in Nigerian society. It is obvious that the foregoing represent challenges to mHealth privacy in Nigeria and they must be appropriately handled within that society in the context of an mHealth regulation. Another factor which complicates it is the level of poverty and illiteracy in Nigeria. A brief look at the latter now follows.

3.3.2 Poverty and Illiteracy as Factors

Although Nigeria is a middle income country and Africa's largest oil producer,[228] years of corruption and mismanagement have created serious disparities in wealth distribution among its population. It is reported that almost 61% of its population, more than a hundred million people, live on less than a dollar a day.[229] As well, the country has low literacy levels; about 38% of its population cannot read or write.[230] In the rural areas, the burden of illiteracy is much greater on account of lack of educational facilities. Even in rural areas where there are schools, the pressures of poverty and survival demands force families to keep their children out of schools to help them eke out a living through farming.

The prevalence of poverty and illiteracy means people have less awareness of their legal rights, and are more likely to abide by what is said by someone of a presumably higher class. They are likely not aware of their constitutional right to privacy of their health information and the possible risks of any unauthorized use of their health information.

---

[228] Alex Whiting, "Middle-income countries leave their poorest behind – report" *Thomson Reuters Foundation* (7 December 2011), online: Thomson Reuters Foundation <http://www.trust.org/item/?map=middle-income-countries-leave-their-poorest-behind-report>.

[229] "Nigerians living in poverty rise to nearly 61%", *BBC News Africa* (13 February 2012) online:BBC News<http://www.bbc.com/news/world-africa-17015873>.

[230] Clement Idoko, "Literacy level in Nigeria now 62% —FG", *Nigerian Tribune* (5 August 2014) online: Nigerian Tribune <http://www.tribune.com.ng/news/news-headlines/item/12566-literacy-level-in-nigeria-now-62-fg/12566-literacy-level-in-nigeria-now-62-fg>.

Evidence of the impact of poverty and illiteracy on health in Nigeria was apparent in the aftermath of the 1996 Pfizer clinical trial in Kano State. Pfizer, an American pharmaceutical company, had conducted clinical trials of its antibiotic, Trovafloxacin in that Nigerian state.[231] The trial was to determine whether the oral form of Trovafloxacin was more effective in treating children infected with meningitis than other existing treatments, including Ceftrixacone.[232] Out of 200 children enrolled for the trials, 11 died, while others suffered seizures or became paralyzed.[233] Particularly noteworthy were indications that because of their illiteracy, the parents of the children were not adequately informed about the trials and therefore, were ignorant of its implications for the health of their children. Although not specifically related to unauthorized use of health information, the trial is relevant in explaining the impact of poverty and illiteracy on the awareness of rights, including the right to the privacy of one's health information. In mHealth systems where the players are usually comprised of mobile telecommunication companies, foreign sponsors and government bodies that provide specific mHealth service, the inequality in the relationships with the local populations easily weighs on the patient's decision to agree to the use of their health information. In addition, their illiteracy may prevent them from understanding the implications of use of their health information for a secondary purpose.

---

[231] Joe Stephens, "Panel Faults Pfizer in '96 Clinical Trial in Nigeria", *The Washington Post* (7 May 2006) online: The Washington Post<http://www.washingtonpost.com/wpdyn/content/article/2006/05/06/AR2006050601338.html>.

[232]Joe Stephens, "Where Profits and Lives Hang in Balance: Finding an Abundance of Subjects and Lack of Oversight Abroad, Big Drug Companies Test Offshore to Speed Products to Market", *The Washington Post* (17 December 2000)online: The Washington Post <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/02/AR2007070201255_pf.html>.

[233] *Ibid.*

3.4 Conclusion

This chapter has provided a brief description of the state of the health sector in Nigeria, and the mHealth context of health service delivery. It points out that unlike in developed countries, mHealth in Nigeria is driven by text messaging from mobile phones as opposed to platforms which may require more complex data infrastructure. The discussion asserts that while mHealth holds much promise to help to fill the gaps in Nigeria's health delivery system, to assure respect for the privacy of health information provided by users via these platforms is a major challenge. The challenge is accentuated by the socio-cultural realities that impact health service delivery in Nigeria. As pointed out, the country's communal conception and practice of mutual responsibility and caring through extended family relationships is a challenge to the notion of control of one's health information without interference by others. Also, with the extent of poverty and illiteracy among the majority of the population, conceptions of privacy take on issues that may be foreign to how privacy is understood and protected in western nations.

The broader implications of the socio-cultural factors descriptively addressed in the foregoing two sub-sections particularly in the context of the adopting the EU regime, are discussed later in the thesis (chapter six). An appreciation of the foregoing challenges and the chances of finding a workable solution for Nigeria partly depends on the nature and quality of its legal regime that is relevant to mHealth privacy protection. The next chapter thus analyses and assesses that regime.

Chapter Four

mHealth Privacy in Nigeria: The Legal Framework

4.1 Introduction

Much focus has been placed by the global community on the potential of mHealth to support and transform health systems especially in low and middle income countries such as Nigeria. But not much work is being done with regards to the potentials of the legal framework in these countries to protect personal health information that is collected and transmitted via mHealth.

This chapter provides an account of the Nigerian laws that have implications for mHealth privacy regulation. Currently, Nigeria has no data privacy framework, although there is the *Constitution*[234] and a patchwork of laws that may be considered relevant to mHealth. The *Constitution* guarantees a fundamental right to privacy for Nigerians. In addition to this, other instruments provide some guidance, specifically in the health context and the mobile telecommunications sphere in Nigeria. These are the *Code of Medical Ethics*[235] made by the Medical and Dental Council of Nigeria, and the *Consumer Code of Practice Regulations* made pursuant to the *Nigerian Communications Act.*[236]

This discussion finds that although the right to privacy is constitutionally protected, and that additional protection may, in fact be offered by the patchwork of laws, the protections they offer are altogether inadequate. This is because the provisions which seem to extend such protection are loosely drawn and are open to diverse interpretations. Beginning with the *Constitution,* the instruments are discussed and assessed one after the other in the sections that follow.

---

[234] *Constitution of the Federal Republic of Nigeria (Promulgation)* 1999 No. 24 [*Constitution*].
[235] *Medical and Dental Practitioners Act [cap M8] Laws of the Federal Republic of Nigeria 2004, Code of Medical Ethics* [*Code*].
[236] *The Nigerian Communications Act, 2003.*

4.2 The Nigerian Constitution and the Judicial Interpretation of the Right to Privacy

Chapter IV of the *Constitution* sets out the fundamental human rights which every Nigerian citizen is entitled to. One of these is the right to privacy for citizens in their homes, for correspondence, telephone conversations and telegraphic communications.[237]According to the Constitution, this right is sacrosanct and can only be fettered by reasonably justifiable laws made in the interests of national security, public safety, public health or morals or for the protection of the rights and freedoms of others.[238]

Anyone who alleges a violation of this right, whether by a public official or a private citizen may apply to the High Court of the State where the violation occurred.[239] A claim for such breach of the right to privacy as a fundamental right may entitle the claimant to an award for damages.[240] Thus, a person who alleges a breach of their right to privacy can be entitled to damages for invasion of their privacy.[241]

The court has had to consider the privacy provision in the Constitution in a limited number of cases. In *Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo[242],* the Supreme Court, which is the highest court in the judicial hierarchy, construed this right as involving the right to consent or refuse consent. This case involved informed consent to medical treatment. Here, a patient who had been a member of a religious sect, the Jehovah's Witnesses refused

[237] See *the Constitution*, s 37.
[238] *The Constitution*, s 45(1) (a) (b).
[239] *The Constitution*, s 46(1).
[240] *Shugaba Darman v. Minister for Internal Affairs*, (1981) 2 NCLR 459.
[241] In *Ajayi v AG Federation*, (1982) NCLR 915, the court in its discussion of damages in a claim for breach of fundamental rights stated that factors such as: the frequency of the type of violation in recent time; (b) the motivation for the violation; (c) the status of the applicant; (d) the undeserved embarrassment meted out to the applicant, including pecuniary losses, and (f) the conduct of the parties generally particularly that of the respondent, will be taken into consideration in calculating damages.
[242] *Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo*, [2001] 7 NWLR (Pt 711) 206 [*Okonkwo*].

blood transfusion which was required for her treatment. She made this refusal by signing a card stating this was contrary to her religious beliefs. She also signed a document discharging the physicians and the hospital from any untoward happening as a result of the refusal. The patient died and the respondent, who was the attending physician was charged on two counts for attending to the patient in a negligent manner and for acting contrary to his oath as a medical practitioner.

At trial, it was argued on behalf of the physician that the dead patient had the constitutional right to object to a course of treatment even if medically required for her treatment. The physician was found guilty by the disciplinary tribunal, whereupon he appealed.

On appeal, in setting aside the decision of the tribunal, the Supreme court, held that an adult of sound mind has a constitutional right to choose or refuse medical treatment made available to him. The court, per Ayoola JSC, noted that this constitutional right is founded on the right to privacy and right to freedom of thought, conscience and religion. On privacy, the court noted that "[this] implies a right to protect one's thought, conscience or religious belief and practice from coercive and unjustified intrusion; and, one's body from unauthorized invasion".[243] By this decision, the court recognized the right of an individual to determine to choose to accept or refuse a particular course of treatment as a direct consequence of their constitutional right to privacy.

In another case - *Sony Kahushiki Kaisha v Hahani & Co. Ltd*[244] bordering on the grant of an *anton piller* order to enter the defendant's premises to search and seize evidence, the Federal High Court which has original jurisdiction in matters relating to intellectual property and trademarks,

[243] *Okonkwo*, *supra* note 236 at para 73.
[244] *Sony Kahushiki Kaisha v Hahani & Co. Ltd* FHC/L/35/81.

opined that the grant of such orders should take cognizance of the right to privacy as provided under the Constitution. In that case, the court in refusing the order stated as follows:

> Can one say the use of a police to enforce an obligation is compatible with the defendant's fundamental rights when he had not had a hearing at all whether fair or unfair? It is common knowledge here in Nigeria that many business premises are also living accommodations, can intrusion on one's privacy without fair hearing be compatible with Section 34 of the 1979 Constitution[245]

The above decision suggests that the right to the privacy of one's home, in this case, the business premises of the defendant, is one protected by the constitution. Consequently, the courts have by these decisions stated that any order which potentially interferes with enjoyment of this right must be based on a fair evaluation.

4.3 The *Code of Medical Ethics*

The *Code of Medical Ethics* contains the rules for the conduct of medical and dental practice in Nigeria. The *Code* was passed pursuant to the *Medical and Dental Practitioners Act* [246] ("the Act") which provides that Medical and Dental Council of Nigeria,[247] the professional body to regulate the practice of medicine and dentistry in the country, should "[Review] and [prepare] from time to time a statement as to the code of conduct which the Council consider desirable for the practice of the professions in Nigeria".[248]

The *Code* among other things, contains general guidelines for practice of medicine including the rights and responsibilities of physicians; issues of professional conduct and malpractices; aspects

[245] *Ibid.*
[246] *Medical and Dental Practitioners Act [cap M8] Laws of the Federal Republic of Nigeria 2004* [The Act].
[247] *Ibid*, s 1.
[248] *Ibid*, s 1 (c).

of private medical or dental practice; conviction for criminal offences as well as miscellaneous issues such as enforcement of sanctions.

To ensure compliance, the *Act* provides for the establishment of the Medical and Dental Practitioners Disciplinary Tribunal to hear and determine complaints[249] and the establishment of an Investigation Panel to investigate and report such complaints.[250] The Tribunal upon a determination of wrongdoing under the provisions of the *Code* may, admonish; suspend; or strike out the name of an erring person from the register of medical practitioners.

Based on relevance, aspects of the *Code* Vis-a- Vis privacy of health information in the medical context are explored next.

4.3.1 The *Code* on Health Information Generally

One of the ethical principles laid down by the *Code* is that all "communications between the patient and the practitioner made in the course of treatment [is] treated in strict confidence"[251]While providing professional service, physicians are to ensure that the confidentiality of their patients are protected except in circumstances where the physician is compelled by the law, or there is concern for the safety of other persons, or where the patient has given his or her consent for the information to be divulged.[252]

4.3.2 The *Code* on Health Information via Computer and Telecommunication Technologies

The *Code* recognizes that the influences of computer and communication technologies are stealthily creeping into the practice of medicine in Nigeria.[253] It thus enjoins health professionals

[249] The *Act,* s 15 (1).
[250] The *Act*, s 15 (3).
[251] The *Code,* s 9 (f).
[252] *Ibid.*
[253] *Ibid at* s 21 & 22.

to protect themselves from "medico-legal pitfalls in areas such as confidentiality"[254] by making adequate arrangements for the security of information stored or received via electronic means. Physicians are to ensure that where patients' health information or records are transmitted over these networks, they are secure and cannot be intercepted by anyone other than the intended recipients of the information.[255]

Evident from the above is that the *Code* imposes a duty on physicians to keep their patients' confidences. Confidentiality here, refers to the responsibility of the physician to keep the confidences of the patient. The implication is that there is a duty on medical practitioners not to disclose information provided by their patients regarding a medical consultation.

In the field of bioethics, it is suggested that confidentiality plays a very important role in physician-patient relationships. According to Winston, "the duty to respect the confidentiality of personal medical information derives from a more basic duty to respect the autonomy of individuals"[256] This implies that keeping medical information confidential shelters the patient from interference by others. This is because knowledge of medical information by others can expose a person to discrimination, shame or stigma. Another role confidentiality plays is that, it is necessary for the maintenance of healthy relationships between the physician and the patient. According to Beauchamp and Childress, trust is critical in other for patients to be open to their physicians

> If a patient could not trust physicians to conceal some information from third parties, patients would be reluctant to disclose full and forthright information or to authorise a complete examination and a full battery of tests [257]

[254] The *Code* at *s 21 & 22.*
[255] *Ibid.*
[256]Morton E Winston, "AIDS, Confidentiality and the right to know" (1988) 2 Public Affairs Quarterly 99 at 104.
[257] Beauchamp & Childress, s*upra* note 96 at 307.

In essence, where patients do not believe that doctors can keep their confidences, then they would not disclose 'shameful' but potentially medically important information about themselves, thus reducing their chances of getting the best medical care. Thus, with the *Code*'s provision respecting the health information of patients, it implies that such information shared by patients with their physicians assume a confidential status and cannot be disclosed to others. As such, it would be an act of professional misconduct for a physician to give information concerning the condition of a patient to a person other than the patient except where such disclosure is within the recognized circumstances stated under the *Code*.

Also, the *Code* requires a security obligation on the part of physicians with respect to information to "stored or received…by electronic means".[258] It has been recognized that processing personal information via computer systems requires that adequate safeguards be put in place against unauthorized access, use or modification.[259] A failure to provide the necessary safeguards could expose owners such information to identity theft.[260] Particularly for health information, unauthorized disclosures or stealing could expose patients to mental anguish,[261] economic exposure[262] and even social stigma.[263] If patients are not confident that adequate security safeguards will be place to protect information stored via electronic means, the

[258] The *Code,* s 22 (a).
[259] Rein Turn & Willis Ware, "Privacy and Security Issues in Information Systems", online: Rand <http://www.rand.org/pubs/papers/P5684.html>.
[260] Thomas J Smedinghoff, "The New Law of Information Security: What Companies Need to Do Now" (2005) 22 Computer & Internet Lawyer Journal 9 at 9-25.
[261] Health Privacy Project, "Health Privacy Stories",online: Center for Democracy and Technology <https://www.cdt.org/files/healthprivacy/20080311stories.pdf>.
[262] *Ibid.*
[263] *Ibid.*

implication is that as with confidentiality, patients may not be forthright with their physicians or provide the information necessary for their care.[264]

Thus, an obligation to secure patient information stored or received electronically, is placed on physicians; failure of which could expose them to liability u *Code*.

4.4 The *Consumer Code of Practice Regulations*

As stated in chapter 2, mHealth refers to the use of mobile technologies in health through mobile devices such as laptops, mobile phones and so on. In Nigeria, mHealth is driven by mobile phones set up via text messaging which allow mobile users and providers to send and receive information *inter se*. The Nigerian Communications Commission is the principal regulator of the telecommunications industry in Nigeria.[265] This industry is comprised of mobile operators that provide telecommunication services in the country. Established by the *Nigerian Communications Act,*[266] the Commission is charged with responsibility of regulating the telecommunications[267] industry in Nigeria.[268]It can grant or renew communication licences[269] as well as fix and collect fees.[270]

As well the Commission has the responsibility of protecting and promoting the interests of consumers against unfair practices.[271] To carry out this responsibility, the Commission has the

[264] Laurinda B Harman, *supra* note 126 at Cathy A Flite & Kesa Bond, "Electronic Health Records: Privacy, Confidentiality, and Security" (2012) 14 American Medical Association Journal of Ethics 712 at 714.
[265] *Nigerian Communications Act*, 2003, s 3(1).
[266] *Ibid*.
[267] Telecommunications is defined in the Act to include any transmission, emission or reception of signs, signals, writing, images or sounds. See Pyramid Research, *supra* note 160.
[268] The *Act*, s 3(1).
[269] The *Act*, s 4(1) (e).
[270] The *Act*, s 4(1) (g).
[271] The *Act*, s 4(1) (b).

power to make and enforce regulations and issue guidelines[272] intended to protect the interests of consumers from unfair practices by industry players.[273]

One such regulations and which is relevant to the theme of this chapter is the *Consumer Code of Practice Regulations* 2007 [274] made pursuant to the *Nigerian Communications Act.*

Section 106 of the *Act* empowers the Commission to designate an industry body to prepare a Consumer Code for the purpose of protecting the interests of consumers, or a licensed company could prepare its own individual consumer code to regulate the provision of services to its consumers.[275] Such a Code may include matters on the protection of consumer information,[276] and it is subject to ratification and approval by the Commission.[277]

The 2007 *Regulations* do not have direct provisions on privacy of health information. However, they have implications for telecommunication operators that process the health information of consumers through mHealth services provided on their platforms.

The *Regulations* set basic principles for the "protection of individual consumer information".[278]One principle requires that the collection of consumer information be fair and lawful.[279] Further, information collected by licensed companies can only be processed for

[272] The *Act*, s 4(1) (i).
[273] See *Consumer Code of Practice Regulations 2007; Type Approval Regulations 2008; Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011; Nigerian Communications Act (No. 19 of 2003), Quality of Service Regulations, 2012; Nigerian Communications Commission Guidelines on Advertisements and Promotions; Consultation Guidelines on the Nigerian Communications Commission 2007 and the Nigerian Communications Commission, Dispute Resolution Guidelines 2004.*
[274] *Nigerian Communications Commission Act*, *Consumer Code of Practice Regulations* 2007 [*Regulations*].
[275] The *Regulations*, s 4(1).
[276] The *Act*, s 106 3 (c).
[277] The *Act* s 106 (2).
[278] Set out in Part VI of the *Regulations*.
[279] The *Regulations*, s 35(1) (a).

identified purposes.[280] Also, information collected by licensed companies must be relevant, not excessive, and should be limited to the amount of what is required to achieve the purposes of their collection.[281] In other words, collection of personal information should not be arbitrary, but whatever information is collected must be accurate.[282] This principle is reinforced by the requirement that consumers must have access to the information for the purpose of ensuring its accuracy.[283]

Another principle requires the licensee to ensure that the collected information is protected against accidental or improper disclosure, and where consumer information is transferred to any other party, such must be under terms agreed with the consumer.

Licensed companies are required to generally accept fair information principles by

> providing notice as to what individual consumer information they collect, and its use and disclosure; the choices individuals have with regard to the collection, use and disclosure of that information; the access consumers have to that information, including to ensure its accuracy; the security measures taken to protect the information, and the enforcement and redress mechanisms that are in place to remedy any failure to observe these measures.[284]

The *Regulations* apply to telecommunication companies who provide mobile services[285] in Nigeria. In particular, its aim is to protect consumers who use the mobile services provided by these telecommunication companies. Increasingly, these services are not limited to voice calls and texts but also added services to improve access and provide health services in areas where

[280] The *Regulations,* s 35(1) (b).
[281] The *Regulations,* s 35(1) (c).
[282] The *Regulations*, s 35(2) (c).
[283] The *Regulations,* s 35(1) (e).
[284] The *Regulations, s* 35(2) (a)-(d).
[285] See Section 1 of the Regulations.

there is a pressing need.[286] As such, the *Regulations* could provide some guidance for managing health information collected by telecommunication companies providing these services.

It is instructive that the above provisions of the *Regulations* offer a broader protection for information collected by telecommunication companies through the fair information principles. As would be stated in chapter 5, fair information principles are principles that specify the minimum requirements for protection of personal information. Thus telecommunication companies who provide mHealth services through their mobile platforms by ensuring that the minimum requirements for protecting users such as notifying users of the purpose of use of their information. In this way, uses outside of the identified purpose are excluded, except where the user has been notified and has given their consent. The *Regulations* also protects mHealth users by requiring telecommunication companies to provide adequate security measures for the protection of collected information against accidental or improper disclosures.

By embodying these principles, the *Regulations* set the ground rules for telecommunication companies for collection of personal information of individuals. For mHealth, this basically means that at the time of collection, individuals must be clearly informed of the reasons for collecting personal information. The advantage is that the information provided by the individual is used to provide the particular mHealth service requested and not deployed for other purposes. Moreover, this implies that for uses outside the scope of the mHealth service, the consent of the owner of the health information must have been obtained.

[286] An example of this mHealth service is the Etisalat Mobile Baby, provided by Etisalat, one of the largest mobile telecommunications company in Nigeria. This service provides a complete suite of services for pregnant women to cover remote monitoring of their pregnancies; step by step protocol to identify and report danger signs during labour and also facilitate emergency transfer from the traditional birth attendants or midwives to obstetricians. See "Etisalat Mobile Baby"online: <http://www.ictet.org/downloads/Mob_ejtJpe_jfnJ.pdf >.

Further, the principle on access to personal information is instructive. The import of this principle is that individuals can request from telecommunication companies who provide mHealth services, how their health information has been used or to whom such information has been disclosed. It also gives individuals the opportunity to correct or amend any inaccurate or incomplete information about them. The advantage is that individuals can control or determine who has access to their health information, other than the mHealth service providers. Moreover they can correct any inaccurate information that may lead to loss of an advantage. For example, where such information is to be transmitted by the mHealth service provider to security agencies in a criminal investigation context. The opportunity of access ensures that an individual can correct information which is inaccurate, and may potentially expose them to a criminal investigation.

4.5 Identified Shortcomings of the Legal Framework for mHealth Privacy in Nigeria

4.5.1 *The Constitution*

4.5.1.1 *Determining the Scope of the Right to Privacy*

It was shown above that a right to privacy exists via Section 37 of the *Constitution*. Also, the cases cited above, show that the courts recognize the existence of this right as by the *Constitution.* However, what is not clear is the scope of applicability of this right in regards to privacy of health information. The import of this broad and imprecise scope is that the extent of this right may be expanded or contracted by judicial interpretation and thus subject to varying interpretations by different judges.

As noted by Matemba, before pre- 1999 in Nigeria, there was a tendency by Nigerian judges to adopt the method of considering the Constitution as a whole to determine the intention of the

legislature as a guide to the interpretation of a constitutional provision.[287] At other times, they have adopted the "ordinary and natural language"[288] which best convey the intention of the legislature. He notes however, that post 1999, the style of judicial interpretation have tended to lean towards a broader approach in the interpretation of constitutional provisions.

In between these differences in methods of judicial interpretation of constitutional provisions, question that arises is whether the court will be willing to recognize privacy of health information as falling within the scope of the right to privacy as stated in the *Constitution*. As such, it may be argued that as a result of the failure of the *Constitution* to do so, it is subject to judicial discretion to recognize whether or not the privacy of health information comes within the ambit of this provision.

4.5.1.2 *Cost of Enforcing Fundamental Rights Actions*

Another shortcoming in the consideration of the *Constitution* is the cost of fundamental rights in Nigeria. Cost, here implies the monetary expense of initiating actions in court as well as the cumbersome and technical rules and procedures of the adjudicatory process.

As noted in chapter 3, more than a hundred million people live on less than a dollar a day.[289] Although the Constitution guarantees a right to privacy, this right is almost meaningless if citizens cannot afford the cost of legal representation and filing matters in court. For example,

[287] Reyneck Thokozani Matemba, *Judicial Activism: Usurpation of Parliament's and Executive's legislature functions, or A Quest for Justice and Social Transformation* (LLM Thesis, Institute of Advanced Legal Studies,University of London, 2010) [Unpublished] at 27-28.

[288] *Ibid* at 27.

[289] See Chapter Three for the discussion on the poverty level in Nigeria.

the cost of filing matters is so high that in some courts, litigants are required to pay 0.5% as filing fees for claims higher than a million naira.[290]

Added to the economic consideration is the tendency of judges to consider technicalities in actions involving fundamental rights actions. For example, in *Ransome-Kuti v Attorney General of the Federation & Ors*[291] the plaintiffs sued the Federal Government for the willful destruction of their building and chattels, assault and battery by soldiers of the Nigerian Army. The claim, proceeded mainly as a claim in tort but referred to the breach of the right to private and family life of the plaintiffs. According to the court in this case, the jurisdiction conferred by section 46(1) of the Constitution was for the enforcement of a fundamental right. It follows therefore that an action seeking to enforce the fundamental right to privacy must be filed strictly as a stand-alone claim and not as an ancillary to a claim in tort.

The effect is that even if by conjecture, it is agreed that privacy of health information can be enforced pursuant to the privacy provision in the *Constitution*, the economic cost of filing actions in court coupled with the complex rules and processes for commencement of actions dulls the prospects of such conjecture.

4.5.2 The *Code of Medical Ethics*

4.5.2.1 *Silence on Patient's Decisional Control over Their Health Information*

A major shortcoming of the *Code* is the assumption that by requiring that physicians maintain the confidences of their patients, it has conclusively placed the physician in a position of acting in the best interests of the patient by protecting their health information. It is arguable how this

[290] See for example*, Federal High Court (Civil Procedure) Rules* 2009, Order 55, Appendix 2.
[291]*Ransome-Kuti v Attorney General of the Federation & Ors,* [1981] 2 NWLR (Pt 6) 211 [*Ransome*] See also *S Olawoyin v Att-Gen Northern Region of Nigeria,* (1961) 1 All NLR. 269.

ethical obligation suffices in a context such as Nigeria. As stated in chapter 3, there is a communal practice of mutual responsibility and caring through extended family relationships leaving little boundaries for individuals to maintain a personal space. Thus, for a woman living in Northern Nigeria where the communal attitude regards the use of family planning methods as unacceptable, knowledge of such information could lead to possible rejection or stigmatization by family members. In such situations it may be best to allow the patient determine who has access to such information as opposed to leaving this aspect with physicians.

4.5.2.2 *Construction of 'Consent' Limited to Medical Procedures*

Construction of consent in the *Code* does not appear to envisage that health information may need to be shared between health care professionals for the care of the patients; or for purposes other than a patients' care, such as for research; or that with the advent of technology, health advice and care may be provided over mobile devices. Thus, aspects of the *Code* provide an extensive explanation of consent and its requirements in medical procedures whereas a cursory reference is made to consent as one of the exceptions to breach of physician-patient communication.

The use of patient health records or information has extended beyond the therapeutic context to use for purposes such as research and electronic collection and use thus, consent has become a way for patients to control such use. One way this has been done is through legislation. There are data protection laws, such as the European model, examined in chapter 5, which set out consent requirements for processing of personal information. Another way is through health information specific statutes. Canada, is very instructive with regard to consent provisions for collection, use

and disclosure of personal health information.[292] Consent provisions spell out where the express consent of the patient, either verbally or in writing is required before collection, use or disclosure of a patient's health information. They also recognize circumstances where health care providers may infer circumstances where the patient can reasonably agree to same. In Ontario, for example, the *Personal Health Information Protection Act* provides that the express consent of the patient would be required where

(a) a health information custodian makes the disclosure to a person that is not a health information custodian; or

(b) a health information custodian makes the disclosure to another health information custodian and the disclosure is not for the purposes of providing health care or assisting in providing health care.[293]

A health care provider may only assume consent where information is exchanged with other providers who are involved in the provision of healthcare to the patient.[294]

This is not the same construction as under the *Code* or any other Nigerian legislation for that matter. The implication is that a physician may assume consent even in circumstances not related to the care of the patient, such as disclosure to a third party for research purposes.

[292]In Canada, various provincial privacy laws which establish standards for protecting personal health information. For example in Alberta, there is the *Health Information Act*, 2000; Saskatchewan, the *Health Information Protection Act, 2003*; in Manitoba, the *Personal Health Information Act*, 1997 and in Ontario, the *Personal Health Information Protection Act*, 2004.
[293] *Ontario, Ibid at* s 18 (3).
[294] *Ibid*.

4.5.2.3 *Silence on other Principles for Fair Processing of Personal Information*

It has been recognized that privacy of personal information such as health information either processed manually or through an automated system such as a mobile phone should be evaluated through a framework of principles which form the basis of statutes aimed at protection of personal information all over the world. These principles are known as the fair information principles. Although the security safeguards employed by an organization is one of the criteria for judging its compliance, it is not limited to this alone. For example, what may be distilled from general privacy statutes which encompasses protection of health information is that: consent to collect, use or disclose health information; individual right of access to rectify errors; and the duty of an organization to be transparent and to account as to the use of a patient's health information, are some of the criteria for weighing compliance with the respect for privacy requirement. To the extent that the *Code* recognizes only security safeguards as sufficient for compliance with all of these principles, it cannot be said to offer adequate protection for the health information of Nigerians at the hands of their doctors and their dentists, and in regards to mHealth service providers.

4.5.3 The *Consumer Code of Practice Regulations*

4.5.3.1 *Rules for Protection of Personal Information are Determined by Industry Players*

As stated above, the *Regulation* provides that each licensed company could prepare its own individual consumer code to regulate the provision of services to its consumers. In other words, the regulator has no uniform requirements for protection of personal information applicable to industry players. This leaves a vacuum of control, and leaves the protection of health information to the whim of telecommunication companies who provide mHealth services.

Contrast this with what obtains in other climes. In most countries, there are strong privacy regimes which set the ground rules for use or disclosure of individuals' personal information by telecommunication companies. For example, in Canada, the *Personal Information Protection and Electronic Documents Act (PIPEDA),*[295] sets such rules for handling of personal information by telecommunication service providers. It requires providers to obtain consent from individuals with respect to the collection, use and disclosure of their personal information. Additional guidance is also provided by the Canadian Radio-television and Telecommunications Commission (CRTC).Under this guidance, confidential customer information other than publicly available information, cannot be disclosed except with the express consent of the customer.[296]

Unlike the above, Nigeria's regulation leaves such consent, which has been described as a "guardian of personal information"[297] to the discretion of industry players. A precise construction of consent, for example, would have been in view of the socio-cultural values prevailing in Nigeria. The communal nature of Nigerian society and the influences of the extended family system may potentially determine whether individuals can provide and independently give consent, or whether consent to any use of their personal information would be given by others. For example, studies confirm that the influence of the community or family head can determine if an individual participates in a medical research.[298] Also, in a patriarchal society like Nigeria, women often need to obtain their spouse's permission for personal

[295] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Schedule 1,s 5, Principle 4.3.

[296]See Canadian Radio-television and Telecommunications Commission, "Telecom Decision CRTC 2003-33", online: CRTC < http://www.crtc.gc.ca/eng/archive/2003/dt2003-33.htm> .

[297] Jennifer Barrigar, Ian R Kerr & Jacquelyn Burkell, "Let's not get psyched out of privacy: Reflections on withdrawing consent to the collection, use and disclosure of personal information"(2006)44 Can Bus LJ 54 at 56. In their paper, Barrigar et al stated that consent sets the boundary between the individuals' interest to determine what information about them is known, against the society that has become increasingly information hungry.

[298] ER Ezeome & PA Marshall, "Informed Consent Practices in Nigeria" (2009) 9 Developing World Bioethics 138 at 140;Anant Bhan, Mina Majd & Adebayo Adejumo," Informed Consent in International Research: Perspectives from India, Iran and Nigeria"(2006) 3 Medical Ethics 36 at 40.

decisions.[299]It is thus pertinent that any law that deals with the processing of personal information should be clearly constructed and clearly identify who gives consent in this context. This, the *Regulation* fails to do.

4.5.3.2 *No Special Rules Apply to Health Information*

The *Regulation* also fails to address whether the same requirements for information processing would apply where sensitive information, specifically, health information, is to be processed by telecommunication companies. As noted earlier, more and more telecommunication companies are coming into the mHealth market in Nigeria. This suggests that processing of health information not envisaged by these companies has become inevitable. It would thus have been appropriate that this is specifically addressed in this *Regulation*.

The trend in data protection regimes in most parts of the world is to categorize personal health information as 'sensitive information'.[300] With this categorization, special conditions are required for their use, collection or disclosure. The view is that health information goes to the personal integrity of the person,[301] and disclosure of this information could expose the individual to social stigmatization or physical harm. For example, in countries where women are not allowed to make free choices about their reproductive health such as the use of birth control, disclosure of such information could expose the woman to physical harm from family members or other members of the community. This is why under these data protection regimes, apart from the general rules which apply to processing all categories of personal information, there are

[299] Anant Bhan,*Ibid*.
[300] This has been the trend since it was first set out in Article 6 of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, ETS108.Latter data protection regimes such as the EU Data Protection Directive to be examined later in this thesis have followed this trend.
[301] McInerney, *supra* note 112 at 148.

special preconditions that must be complied with before processing sensitive information such as health information.

Nigeria's *Regulations* provide, however, that the same rules apply to all classes of personal information, or, in effect, the applicable rules are left to the discretion of the telecommunications companies. For a woman who lives in a rural community in Nigeria where she is expected to have a high fertility rate, and where the community views fertility and children as symbols of prosperity and blessing her,[302]any innocent or inadvertent release of information relating to a request for contraception via a service provided by a telecommunication company could have grave consequences for her status as a 'blessed' woman in society, and as to her acceptability within the community.

4.5.3.3 *Silence on Protection for Cross Border Transfers*

Added to the foregoing, the regulation does not expressly address the issue of cross border transfer of information, although it requires that any transfer of an individual's information to a third party must be upon terms and conditions agreed with the patient.[303] For cross border processing of information, the *Regulations* leave a vacuum, especially in mHealth, where a number of entities are likely to process, store or access a data subject's personal information, and many of these entities may be located in multiple countries. Where these entities are outside the borders of Nigeria, will the same terms and conditions for transfer of information still apply? The regulation is silent on this matter. The implication this silence is that where health information

[302] Abdulkarim Mairiga et al, "Sociocultural factors influencing decision-making related to fertility among the Kanuri tribe of north-eastern Nigeria" (2010) 2 African Journal of Primary Health Care & Family Medicine <http://www.phcfm.org/index.php/phcfm/article/view/94/85>.
[303] *Ibid.*

are collected for mHealth purposes, their protection cannot be guaranteed where they are transferred outside of Nigeria's borders.

4.6 Conclusion

The foregoing analysis of the Nigeria legal regime on the protection applicable to mHealth privacy shows that the right to privacy exists in Nigeria as constitutionally protected right. But as analyzed, the *Constitution*'s protection lacks any tooth for mHealth privacy specifically. The advance made on this by the *Code of Medical Ethics* is its coverage of confidentiality of communication between physicians and their patients. The *Consumer Code of Practice Regulations* further advances this through a set of principles it contains to guide the processing of personal information by telecommunications companies in Nigeria.

The foregoing may seem to say that a legal framework exists. However, that framework is currently incomplete and deficient. Neither of the subsidiary instruments contain clearly defined provisions on processing of health information such as on consent for the use or disclosure of health information, or detailed principles that prescribe the criteria for a fair processing of personal information. That these matters must be addressed via privacy legislation is obvious, and the next chapter seeks to address them. It does this by looking at the current framework available in Europe through the *European Union Data Protection Directive 95/46/EC*[304] and the *Directive on privacy and electronic communications, 2002/58/EC.*[305]

[304] *EC,Commission 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 information and the free movement of such data*, [1995] OJL 281/31.

[305] EC, *Commission Directive 2002/58/EC of 31 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, [2002] OJ, L 201.

Chapter Five

mHealth and Privacy Models: *The European Union Directive* and the *E-Privacy Directive*

5.1 Introduction

The analysis of the privacy regime in Nigeria in the preceding chapter established that although the *Constitution*, the supreme law, recognizes and protects the right to privacy, the *Code of Medical Ethics* which protects confidentiality of health information in the medical context and the *Code of Consumer Practice Regulations* that regulates the processing of personal information by mobile operators contain a lot of gaps in regard to the adequate protection that mHealth users in Nigeria need. The logical inquiry is how Nigeria can close those gaps in this legal architecture. Given the novel nature of this area of legal regulation, it is useful to examine international standards in terms of how issues of mHealth privacy protection are addressed through the law.

The aim of this chapter is not to take an inventory of the international standards and national legislation on mHealth privacy protection. Rather, it considers protection for health information from a developed world perspective with a view to how similar standards could be adopted in a developing country context as Nigeria. The *European Union Data Protection Directive 95/46/EC* [306] and the *Directive on privacy and electronic communications, 2002/58/EC* [307] are analysed for this purpose.

---

[306]EC, *Commission 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 information and the free movement of such data*, [1995] OJL 281/31 [Directive].

[307]EC, *Commission Directive 2002/58/EC of 31 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, [2002] OJ, L 201 [E-Privacy Directive].

The *Directive* is the regional legislation on privacy to which all Member States of the EU must conform.[308] It sets out comprehensive regulations for the protection of all classes of personal information in the European Union. For this thesis, the *Directive* is looked at in relation to the protection it offers to personal information generally, and specifically, its application to personal health information.

The *Directive* is considered for two reasons: First, it has been more widely applied than other models, having been transposed into the laws of all member states of the EU. Across Europe, member states have adopted its general principles into national laws, albeit with divergent attitudes and variations in enactment and implementation where necessary to suit local needs.

Second, it is useful to consider the *Directive* because of its growing influence outside Europe. In a study of 33 non-European countries, Greenleaf found that the data privacy laws of each country had visible, sometimes explicit influences of the *Directive* in terms of content.[309] In others, a conscious effort was made to ensure that the national privacy regimes comply with the requirements of the *Directive*.[310]

---

[308] World Health Organization, *Legal Frameworks for eHealth: Based on the Findings of the Second Global Survey on eHealth,* online: Global Observatory for eHealth <http://www.who.int/goe/publications/ehealth_series_vol5/en/>. The *Directive* was presaged by the Council of Europe, CA, 32nd Sess, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*, Texts adopted, ETS 108 (1981) adopted by the Council of Europe, the body that ensures that promotes uniform standards across Europe with regards to legal standards, human rights and cultural co-operation. However, unlike the *Directive*, the Council of Europe Convention have the status of an agreement among member states of the European Union while the Directive has a binding effect but allows flexibility among states as to the means to achieving the goal of data protection. As a matter of fact, because of its nature, not all countries in Europe ratified the Council of Europe Convention. See Andrej Savin, *EU Internet Law* (Massachusetts: Edward Elgar Publishing, 2013) at 195.

[309]Graham Greenleaf, "The influence of European Data Privacy Standards outside Europe: Implications for globalization of Convention 108" (2012) 2 International Data Privacy Law 68 at 77.

[310] *Ibid.*

The *Directive* was passed in 1995 when communications technology was emerging and at that time, posed lesser privacy risks for personal information.[311] As such, a subsequent framework, the E-Privacy Directive[312] was passed to provide further protection from privacy risks resulting from advancements in technology. Although, the European Commission in 2012 proposed a reform of the current *Directive*,[313] however the aim of the proposed reform is to make a single set of rules on data protection applicable across Europe. This is in contrast to the present arrangement where implementation of the *Directive* in member countries may be tailored to suit local circumstances.[314]

The following sections consider these two-pieced EU-wide statutes[315] in terms of their scope, their inadequacies or shortcomings, and particularly how they serve the purpose of mHealth information protection in this thesis. The aim of this examination is to consider the usefulness of the *Directive* and the *E-Privacy Directive* for mHealth privacy protection and whether both can be merged into a singular privacy framework for Nigeria.

[311]Savin, *supra* note 308 at 211.

[313] See EC, *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),* online: European Union Law < http://eur-lex.europa.eu/procedure/EN/201286>.

[314] Jan Philipp Albrecht, "EU General Data Protection Regulation State of play and 10 main issues"(7 January 2015),online:Janalbrecht<http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf>.

[315] Throughout this thesis, EU Model or the EU Regime shall be used in joint reference the *European Union Data Protection Directive 95/46/EC* and the Directive *on privacy and electronic communications, 2002/58/EC.*

5.2 *The European Union Directive*

5.2.1 Background and Scope

On 24th October 1995, the European Union Parliament passed a *Directive* to protect the processing of personal information within Europe. This *Directive*, commonly cited as *Directive 95/46/EC*, sets out broad regulations for the protection of personal information among Member States of the European Union.

The *Directive* has two objectives. First, to "protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal information."[316] Its second objective is to promote the free flow of personal information within the European Union.[317]

The *Directive* applies to "any operation or set of operations which is performed upon personal data,"[318] called "processing'" of data. Such operations would include any collection, recording, storage, use or disclosure of personal data.[319]It also applies to data processed by automatic means and to data that are part of or intended to be part of non-automatic "filing systems" such as the traditional paper filing systems.[320] By this application to data processed by automatic means, personal information generated or transferred through computerised or electronic means, such as mobile phones or devices, comes within the purview of the *Directive*.

[316] *The Directive*, Art 1 (1).
[317] *The Directive*, Art 1 (2).
[318] *The Directive,* Art 3 (1).
[319] *The Directive,* Art 2 (a).
[320] *The Directive,* Art 3 (1).

Apart from applying to all forms of personal information, the *Directive* delimits certain categories of information, such as health information, as "special"[321] and thus provides for additional requirements for their processing apply. As a result, other than the basic requirements for the processing of personal information generally, it imposes additional specific requirements for processing the categories of information that fall within this special class. These requirements, specified as principles, are examined below, beginning with those relating to the processing of personal information generally, followed by those relating specifically to health information.

5.2.2 Processing Personal Information Generally (i.e Non-health Specific Information)

5.2.2.1 *Purpose Specification*

As the name suggests, the first principle requires that an individual should be informed of the specific purposes for which their personal information is collected. Article 6 (1)b of the *Directive* provides that the purpose for which personal information is to be processed must be specified beforehand.[322] As well, where there will be a further operation or processing of such information, the *Directive* requires that the subsequent processing must be compatible with the purpose identified.[323] For example, where a patient provides their health information via an mHealth platform to obtain advice about a medical condition, the use of the health information should be limited to the provision of this service and not any other purpose not specified to the patient.

[321] *The Directive*, Art 8.
[322] *The Directive,* Art 6 (1) b.
[323] *Ibid.*

Once the purpose for collecting the information has been fulfilled, the information must not be retained for longer than necessary.[324]In other words, once the motivating purpose has been fulfilled, the *Directive* envisages that the information would no longer be kept.

5.2.2.2 *Transparency*

This principle emphasizes the need for proper information in the collection of personal information. The *Directive* provides that proper information should be given to the individual about the information being collected, the purpose of the collection and the person(s) who would be recipients of the information.[325]

Being properly informed would enable the individual to make a choice as to giving his consent to the collection of the information. Consent, as an indication of the transparency of the process must be "freely given, specific and [be an] informed indication…by which the data subject signifies his agreement to personal data relating to him being processed".[326]

Consent can be indicated in written form, oral statement, or through conduct from which an intent to consent can be deduced or concluded.[327] There is no express statement in the *Directive* as to the form the consent may take, but it must have been freely given, with the data subject being able to exercise their choice without intimidation, deception, coercion or pressure possibly from a situation of dependence or fear that they would suffer some disadvantage.[328]

---

[324] *The Directive,* Art 6 (1) (e).
[325] *The Directive,* Articles 10 & 11.
[326] *The Directive,* Art 2 (h).
[327] Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (13 July 2011), online: European Union< http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>.
[328]*Ibid* at 13-14.

The consent must specifically relate to the scope and purpose of the processing.[329]In other words, the scope of consent cannot be infinite; it must not apply to other possible uses of the personal information which were not contemplated, and about which the data subject was not informed at the time of the processing.

5.2.2.3 *Right of Access, Rectification and Cancellation*

Article 12 of the *Directive* provides individuals with a right of access, that is, the ability of individuals to control access to their personal information by requesting what information about them is being processed, or details about who is processing what information about them and for what purpose.[330] Further, under this provision, the person whose personal information is being processed can also request that otherwise inaccurate data be corrected or removed.[331]

This right is however not absolute. Article 13 recognizes that there are instances where it may be proper to limit or restrict the right in order to safeguard national security, defense, or to prevent the commission of a crime.[332] An instance of derogation may also occur to protect the rights and freedoms of the data subject or that of other members of society.[333]

5.2.2.4 *Security*

The security principle in the *Directive* is focused on the safeguards that must be put in place to protect the collection, use and transfer of the personal information.[334] These safeguards consist of

[329] *Ibid* at 17.
[330] *The Directive*, Art 12 (a).
[331] *The Directive*, Art 12 (b).
[332] *The Directive* Art 13 (1) (a)-(f).
[333] *The Directive*, Art 13 (g).
[334] *The Directive*, Art 17.

the technical and organizational measures put in place[335]to protect individuals' health information from accidental loss or destruction, and unauthorised access and disclosure, especially where they are transmitted over a network.[336] In instances where the personal information is being processed by a third party, known as the data processor, on behalf of the data controller under a contract, similar obligations would also be expected of the former.[337]

5.2.2.5 *Restrictions on Transfer of Personal Information*

There are instances where personal information may cross national borders for reasons of commercial exigencies, national security, or to facilitate international cooperation to fight crime and terrorism. For example, government agencies in different countries may share information about their citizens.[338] Similarly, private bodies, such as healthcare organizations, may need to exchange medical information in the care of a patient, for example, where specialists are based abroad.

With regards to cross border transfer of personal information generally, the *Directive* makes a distinction between transfers to countries[339] that have an 'adequate level of protection' and those countries that do not. To assess whether or not a country has an adequate level of protection, consideration is given to such factors as the nature of the data; the purposes and duration of the proposed transfer; the country of origin and country of final destination of the personal information; the rules of law in the country of destination as well as the security measures taken

[335] The data controller is required to comply with the principle on safeguards or where he has contracted a data processor, the latter would be bound. See *the Directive,* Art 17 (2).
[336] *Ibid*.
[337] *The Directive*, Art 17(3).
[338] Sarah Bridge, "Canadians with mental illnesses denied U.S. entry: Data entered into national police database accessible to American authorities: WikiLeaks", *CBC News* (9 September 2010) online: CBC News<http://www.cbc.ca/news/canada/canadians-with-mental-illnesses-denied-u-s-entry-1.1034903>.
[339] They are referred to as transfers to third countries. Although not defined in the *Directive,* the term is usually used in European Commission documents to describe a countries other than European countries.

in that country.[340] These factors, as well as the domestic and international commitments[341] of the particular country, are critical elements to be considered by the European Union Commission (the Commission),[342] the executive arm of the regional body, in making a determination.

To practically demonstrate this provision of the *Directive*, in 1998, the US Department of Commerce entered into an arrangement with the Commission for the recognition of the country as one that has an adequate level of protection with the Commission. This arrangement, known as the 'Safe Harbour 'arrangement, in literal terms allows a safe harbour for US organizations to receive personal information concerning citizens of the EU from countries in the EU.[343] The arrangement comprises a set of seven principles[344] that are similar in terms to the requirements of the *Directive* on the processing of personal information. In sum, the Safe Harbour regime requires that: notice is given to EU data subjects regarding the collection and use of their personal information; that the data subject can choose to opt out of secondary uses and disclosures of their personal information to third parties; that where personal information is disclosed to a third party that is acting as an agent, the latter is similarly bound to the principles on privacy protection; that personal information is relevant for the purpose for which they are

[340] *The Directive*, Art 25 (2).
[341] *The Directive,* Art 25 (6).
[342]Currently, the Commission has so far recognized twelve countries as providing an adequate level of protection. These are Andorra, Argentina, Australia, Canada (commercial organizations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand and Uruguay. See Commission decisions on the adequacy of the protection of personal data in third countries, online: European Union<http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm>.
[343] EC, *Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number (2000)2441),* [2000] OJ,L215 [Safe Harbour].
[344] They include notice to the EU data subject regarding the collection and use of personal information; the choice of the data subject to opt out of secondary uses and disclosures to third parties; compliance with the requirement on onward transfer; security of personal information, data integrity, access and enforcement are other principles of the Safe Harbour.

collected and that individuals have access to correct, amend or delete any information about them which is inaccurate.[345]

Further, transfers of personal information to countries outside of the EU may be authorized in circumstances "where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals".[346] These safeguards may be by contractual clauses[347] or terms contained in agreements to transfer personal information. In this vein, the Commission has issued certain data protection clauses that may be incorporated into contracts to show that a third country has sufficient safeguards for protecting privacy of information it receives from within the EU.[348]

For countries without an adequate level of protection, the only instances where personal information may be transferred to them are where the data subject has given their unqualified consent to the transfer. Exceptions also apply on grounds of public interest to protect the data subject[349], the interest of others[350] or to comply with the requirements of a law.[351]

---

[345] Safe Harbour, *supra* note 332. See also US Department of Commerce, "U.S. - EU Safe Harbor Framework A Guide to Self-Certification", Online: US Department of Commerce<http://trade.gov/media/publications/pdf/safeharbor-selfcert2009.pdf>.

[346] *The Directive*, Art 26 (2).

[347] *Ibid*.

[348] Three sets of such standard contractual clauses have so far been issued by the Commission. They include two sets of standard contractual clauses for transfers from data controllers to data controllers outside the EU and one set for transfer to processors established outside the EU. See "Model Contracts for the transfer of personal data to third countries", online: European Union <http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm>.

[349] *The Directive*, Art 26 (1) (e).

[350] *The Directive*, Art 26(1) (d).

[351] *The Directive*, Art 26 (1) (f).

5.2.2.6 *Enforcement of the Provisions of the Directive*

To give effect to the privacy principles expressed through the provisions of the *Directive*, a mechanism for enforcement is provided. As a precursor for enforcement, the *Directive* requires the establishment of a body, referred to as "supervisory authority"[352] with oversight functions over data controllers and all persons involved in data processing operations.[353] These supervisory authorities shall be independent[354] and have powers to investigate complaints brought by individuals with regards to the processing of their personal information;[355] to appraise or assess data processing systems[356] and to institute legal proceedings where any provisions of the *Directive* have been violated.

Apart from this administrative side to enforcement, individuals can enforce their right and seek remedy directly through the courts.[357] Remedies would be by way of compensation for the damage suffered[358] and sanctions may be imposed as the court deems fit.[359]

5.2.2.7 *Summary of the General Principles on Processing of Personal Information.*

The provisions of the *Directive* above lay down the standards for processing of any class of personal information. They prescribe the rights of individuals with regards to their personal information. These rights begin from when such information is collected from the data subject. There is an obligation on the part of the data controller to ensure that the information use is for the purposes specified. Data subjects are also given significant control over their personal

[352] *The Directive*, Art 18.
[353] *Ibid.*
[354] *The Directive*, Art 28 (1).
[355] *The Directive*, Art 28 (4).
[356] *The Directive*, Art 28 (3).
[357] *The Directive*, Art 22.
[358] *The Directive*, Art 23.
[359] *The Directive*, Art 24.

information and may decide whether or not to consent to the collection of their information including the right to access and apply to amend or delete any collection of data held on them by any organization for inaccuracies.

Below, the *Directive*'s protection for health information classified in the special category of personal information is examined.

5.2.3 Processing of Health Information

As indicated earlier, the *Directive* regulates the processing of two realms of personal information: personal information in the general class, that is personal information broadly, and a particular class of personal information identified as those in the special category. The latter is the pivot of Article 8 of the *Directive* which classifies certain categories of personal information as 'special'.[360] A class of personal information in this category is that concerning the health of an individual.[361] To convey their special status, the *Directive* prohibits the processing of all information regarding the health of an individual by public and private bodies.

However, this prohibition does not apply in all cases. There are instances of derogation or exemptions where the health information may be processed, such as where the individual has given his explicit consent to the processing.[362] In addition, health information may be processed

[360] The term' special' is not defined anywhere in the *Directive*. Rather it is described in terms of the personal information within this class. They include personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning sex life. See *The Directive*, Art 8.
[361] *Ibid.*
[362] *The Directive*, Art 8 (2) (a).

in the "vital interest of the data subject or another person"[363] or where the individual has on their own, made such data available to the public.[364]

As well, the rule on prohibition would not apply where processing of the health information is necessary to promote preventive health, to carry out a medical diagnosis, or to provide care and treatment for the patient.[365] For this purpose, an exemption would only apply where the health information is processed by a health professional or some other person bound to an oath of secrecy.[366]

5.3 *The E-Privacy Directive*

Like the *Directive*, the *E-Privacy Directive* seeks to protect "fundamental rights and freedoms…in particular the right to privacy, with respect to the processing of personal data".[367]However, it offers a more self-contained regime as it only applies to personal data in the electronic communications sector.[368] The intent of the EU is for the *E-Privacy Directive* to complement the *Directive* by addressing privacy issues in the electronic communications sector as a result of advances in digital technology.[369] In this sense, the *E-Privacy Directive* has direct relevance to the protection of privacy regarding mHealth information.

[363] Vital interests are defined in the Directive to involve instances where the data subject or such other person is legally or physically incapable of providing their consent. See *The Directive*, Art 8 (2) (c)
[364] *The Directive*, Art 8 (2) (e).
[365] *The Directive*, Art 8 (3).
[366] *Ibid.*
[367] *The E-Privacy Directive*, Art 1.
[368] *Ibid*.
[369] Paul Bernal, *Internet Privacy Rights: Rights to Protect Autonomy* (London: Cambridge University Press, 2014) at 94. See also *E-Privacy Directive* at Article 1(2).

The *E-Privacy Directive* lays down specific rules applicable to network and service providers for processing of "traffic"[370] and "location"[371] data generated by using electronic communications viatelecommunications or mobile network[372] or the internet.[373]

According to the *E-Privacy Directive*,

> New advanced digital technologies are currently being introduced in public communications networks in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. The development of the Information society is characterized by the introduction of new electronic communications services. Access to digital mobile networks has become available and affordable for a large public. These digital networks have large capacities and possibilities for processing personal data. The successful cross-border development of these services is partly dependent on the confidence of users that their privacy will not be at risk.[374]

The *E-Privacy Directive* lays down rules applicable to location and traffic data. Location data refers to data indicating the geographical location or whereabouts of a user over an electronic communications network.[375] On a mobile phone, location data may be derived from a GPS feature on a mobile which allows tracking of the mobile phone user, contents such as geo-tagged images, video, audio and text documents, or location-based applications which identify the location of users.[376] Traffic data is data generated by a network.[377] It includes for example, data

[370] *The E-Privacy Directive,* Art 2 (b).
[371] *The E-Privacy Directive,* Art 2 (c)
[372] *The E-Privacy Directive*, Recital 5.
[373] *The E-Privacy Directive,* Recital 6.
[374] *The E-Privacy Directive,* Recital 5.
[375] *The E-Privacy Directive*, Art 2 (b).
[376] The Location Forum, "Location Data Privacy: Guidelines, Assessments and Recommendations *"Privacy Association* (1 May 2013) online: Privacy Association <https://privacyassociation.org/media/pdf/resource_center/LocationDataPrivacyGuidelines_v2.pdf>.
[377] *The E-Privacy Directive*, Art 2 (c).

relating to the routing-the movement of network messages from one network to the other-, duration or time of a communication.[378]

However, for the purpose of this thesis, the discussion will be limited to location data. This is because as a result of the advances in technology, many mobile devices have GPS capabilities that can identify the device, and thus the user's location. Moreover, there are mobile health related applications capable of tracking the location of users.[379] Traffic data, on the other hand is data used by service providers for operational purposes such as billing,[380] as such no privacy interest may need to be protected in regards to such data.

Recognizing the risks to privacy from location data, the *E-Privacy Directive,* like the EU Directive, requires "service providers to take appropriate technical and organisational measures to safeguard the security of [their] services… and to inform subscribers of any particular risk[s]of a breach of the security of the network."[381]

Specifically, in relation to location data, the *E-Privacy Directive* covers the following issues

(i) Conditions for processing of location data

(ii) Use of location data for unsolicited communications.

5.3.1 Conditions for Processing of Location Data

Article 9 of the *E-Privacy Directive* provides that processing the location data of a subscriber or user of an electronic communication service may only be done where such data has been made

[378] "Traffic Data", online: UK Information Commissioner's Office < https://ico.org.uk/for-organisations/guide-to-pecr/traffic-data/>.
[379] "Mobile Health and Fitness Apps: What Are the Privacy Risks?" online: Privacy Rights Clearing House < https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks>.
[380] Traffic data, supra note 378.
[381] *The E-Privacy Directive,* Art 4.

anonymous, or the processing is done with the consent of the user. Prior to obtaining their consent, the service provider must provide such information as the type of the location data to be processed, the purpose of the processing and the duration of the processing.[382]Further,

> [Even] where the consent of the users or subscribers has been obtained for the processing of location data…the user or subscriber must continue to have the possibility… of refusing the processing of such data[383]

In other words, this means that subscriber may withdraw their consent to the use of their location at any time.

5.3.2 Use of Location Data for Unsolicited Communications.

The *E-Privacy Directive* provides that using subscriber details for unsolicited communications, such as for marketing purposes through emails, text messages or automated calling machines, is prohibited except where the subscriber has provided their prior consent.[384] In other words, where the location data of a subscriber have been collected in the context of a particular service, such may only be used in that particular context (providing the agreed service) and nothing more. Thus given that new technologies, such as mobile devices are able to collect information other than those provided by the user, such as location data, that may be used for advert purposes, the *E-Privacy Directive* specifically provides a standard to be observed in this respect.

[382] *The E-Privacy Directive,* Art 9.
[383] *The E-Privacy Directive,* Art 9 (2).
[384] *The E-Privacy Directive,* Art 13 (1).

5.4 The EU-wide privacy models: analysis and assessment

5.4.1 *The Directive*

Unlike the legal framework for Nigeria examined in Chapter four, the privacy principles enunciated by the *Directive* provide a broader framework for privacy protection particularly in the area of mHealth. Some of the reasons this is so are examined below.

5.4.1.1 *Specific Application to Health Information*

The *Directive* specifically categorizes health information among the special class of personal information whose processing is prohibited.[385] As stated earlier, an individual's health information can reveal or hide the most intimate details about their lives.[386] It can show information on demographics, such as name, sex, race or occupation of the individual. It could contain genetic information which details facts about the manifestation of a disease or disorder in a family or among a people, or medical information about diagnosis or treatments for a disease on sexual or mental health. Clearly, unauthorized disclosures of such information comes with potentials for risk to the individual. It could expose them or their families to social stigma[387] and discrimination in terms of access to employment or access to public services.[388]

Recognizing the above, the *Directive* identifies two instances where health information may be processed. On the one hand it may be processed to protect the "vital interest of the data

---

[385] *The Directive,* Art 8.

[386] Nass et al, *supra* note 107 at 78.

[387]Madison Powers, "Privacy and the Control of Genetic Information "in Mark S Frankel & Albert Teich, eds, *The Genetic Frontier: Ethics, Law and Policy* (Washington DC: American Association for the Advancement of Science, 1994) at 77.

[388] Lawrence O Gostin & James G Hodge, Jr., "The "Names Debate": The Case for National HIV Reporting in the United States" (1998) 61 Alb L Rev 679 at 724.

subject"[389] or "for reasons of substantial public interest".[390] Although "vital interest" is not defined in the *Directive*, it presupposes instances where health information is required in the treatment of a patient in circumstances where the patient cannot consent because they are "physically or legally incapable"[391] of doing so. This appears to be intentional, as Article 8(3) allows for such use for "purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services".[392].

For health information processed on research grounds, the *Directive* provides that such information be anonymized or de-identified so as not to allow for a re-identification by 'all means likely reasonably'[393] to be used. Anonymization in data protection is defined as the process of de-identifying sensitive data while preserving its format and data type.[394] Thus with the *Directive*, anonymized data that can no longer be used to identify a natural person by using "all the means likely reasonably to be used" is excluded from the scope of its application.

5.4.1.2 *Individual Control of Processing of Their Personal Information*

Given that one of the objectives of the *Directive* is to 'protect the fundamental rights …in particular [the] right to privacy with respect to processing of personal data'[395], there is an emphasis on consent as an aspect of the individual's right to control the processing of their personal data. "Explicit consent' is one of the recognized instances of derogation for processing

[389] *The Directive,* Art 8 (2) (c).
[390] *The Directive,* Art 8 (4).
[391] *The Directive,* Art 8 (2) (c).
[392] *The Directive,* Art 8 (3).
[393] *The Directive,* Recital 26.
[394] Balaji Raghunathan, *The Complete Book of Data Anonymization: From Planning to Implementation*,(Florida: CRC Press,2013).
[395]*The Directive,* Art 1.

of health information. Additionally, it is one of the means to ground a legitimate processing of personal data.[396]

In this respect, where consent is sought, it must be freely given and voluntary.[397] In situations where the data subject is incapable of providing consent such as where the information is required to save his life, such as in emergency, the situation comes under the 'vital interest' exemption stated above. To be valid, consent must be "specific"[398] in the sense that it sets out the possible instances or uses of health information, and it is not absolute permission to continually use the personal information. For example, where the data subject has provided their health information for diagnostic purposes over an mHealth platform, this is not a general authorization to an open-ended use of the information beyond the purpose for which it was specifically provided. There is the further element that consent must be informed. As much as possible, information must be provided as to the identity and contact details of the data processor, the specific categories of information that would be collected and for what purpose.[399] This implies that use must be limited to the purpose stated and not any other.

5.4.1.3 *Reference to mHealth Captured under Rubric of "automatic Processing"*

Unlike the Nigerian framework examined in Chapter three, the *Directive* is directly relevant to mHealth. Specifically, the *Directive* aims to protect personal information processed "automatically".[400] The sphere of this automatic processing is broad; it covers any collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure

[396] *The Directive,* Art 7 (a).
[397] *The Directive,* Art 2 (h).
[398] *The Directive,* Art 2 (h).
[399] *The Directive,* Art 11.
[400] *The Directive,* Art 3 (1).

by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal information.[401]

"Automatic" is not defined by the *Directive.* However, the UK Court of Appeal[402] in the case of *Durant v. Financial Services Authority,*[403] had cause to provide an interpretation, albeit cursory, to the meaning of the term. In that case, the Appellant had made a request for disclosure or access to information relating to him held by the Respondent, the Financial Services Authority. The request was made pursuant to Section 7 of the Data Protection Act. The information relating to the Appellant was held in manual files and in computerized form. The Respondent had released personal information held in computerized form, but failed to release those held or stored in manual files on the ground that it did not constitute 'data' within the meaning of the Data Protection Act. The court, opined that it does not matter whether the data is held in manual form or in computerized or electronic forms, so long as the information is filed in a manner that it can be easily accessed by a searcher.[404]

This suggests that information collected via a mobile device, such as a laptop, an iPad, a mobile phone or other computing device and digitally transmitted over mobile networks and stored or held in any manual or electronic form, would come within the definition of "automatic" processing under the *Directive*. Thus, this provision brings in mHealth where patients provide their health information to physicians for the purpose of diagnoses, or to seek health advice over mobile networks within the scope of application of the *Directive*.

---

[401] *The Directive,* Art 2(b).
[402] England, being one of the member countries of the European Union had enacted the Data Protection Act to give effect to the provisions of the *Directive.* See *Data Protection Act* 1998 (UK), c 29.
[403] *Durant v. Financial Services Authority,* Case No: B2/2002/2636 [*Durant*].
[404] *Durant, supra* note 403 at para 45-48.

Notwithstanding the foregoing virtues of the *Directive*, important downsides to its application are identified.

5.4.1.4 *Exclusion of 'anonymous Data' from the Scope of its Application*

As noted, the *Directive* applies to identifiable data about a natural person. Such data must identify a person by reference to some physical, physiological, mental, economic, cultural or social identity factors.[405] As such where data has been stripped of these identifying features, it is considered anonymous data and for the purpose of the *Directive*, the principles on protection of personal data would not apply.[406]

By anonymizing data, complex techniques which make it difficult to link an individual to the data, or to obscure the connection between the individual and such information or data are employed. Markers like the name and or other identifiers which reveal personal facts about the owner of the data are removed, or in some cases, replaced with pseudonyms or replacement identifiers.[407] With health information, the rationale is that with anonymization, it is possible to obscure large volumes of data which can be processed and analysed by researchers for surveillance of public health issues and to guide future plans and conduct by governments.[408]

However, whether anonymization protects from health information from privacy risks is arguable. For example, Professor Latanya Sweeney provides an instance showing the limitations of anonymization. She had conducted a study aimed at linking de-identified medical data with

[405] *The Directive,* Art 2 (a).
[406] *The Directive,* Recital 26.
[407] David J Walton, "Big Data raises big legal issues As the laws and regulations within the United States evolve, companies must be extremely attentive",online:Inside Counsel<http://www.insidecounsel.com/2014/03/28/big-data-raises-big-legal-issues>.
[408] Canadian Institute of Health Research, *Secondary Use of Personal Information in Health Research: Case Studies* (Ontario: Public Works and Government Services Canada, 2002) at 15.

particular patients by name. She conducted her research by using anonymized data of health insurance purchased for state employees by the Group Insurance Commission (GIC), a government agency. GIC had decided to release records indicating state employees' hospital visits at no cost to any researcher who requested them. GIC assumed that by removing fields containing name, address, social security number, and other "explicit identifiers," it had protected their privacy. Sweeney demonstrated that this was, in fact, the opposite, as she was able to merge the otherwise anonymized records with the voter registration records to identify the health records of the then Governor of Massachusetts.[409]

A similar scenario, which demonstrated the failure of anonymization, occurred in 2006 when America Online (AOL), released twenty million search queries of 650,000 users of AOL's search engine over a period of three months. The move by AOL was part of an initiative tagged "AOL Research".[410] Before the release, AOL had tried to anonymize the information to protect the privacy of users. It suppressed any obviously identifying information, such as AOL username and IP address, in the released data and instead, replaced them with unique identification numbers. While the initial argument had been that the released data did not violate anyone's privacy as nobody had linked them to actual individuals,[411]it did not take long for *New York*

[409] Recommendations To Identify and Combat Privacy Problems in the Commonwealth: Hearing on H.R. 351 Before the H. Select Comm. on Info. Sec., 2005 Gen. Assemb, 189th Sess. (Pa. 2005), http://dataprivacylab.org/dataprivacy/talks/Flick-05-10.html . Similar studies or examples that have challenged this view include the Netflix Prize Data Study of 2006 where Netflix, a popular online movie rental store released records revealing how nearly a half-million of its users had rated movies from December 1999 to December 2005.All identifying features such as the username were removed from these records, but researchers found that it was still possible to re-identify people in the database and hence their movie watching preferences so long as this record was still present in Netflix data set.

[410]Abdur Chowdhury's email, online: <http://sifaka.cs.uiuc.edu/xshen/aol/20060803_SIG-IRListEmail.txt>.See also Michael Arrington,"AOL Proudly Releases Massive Amounts of Private Data", online: TechCrunch <http://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/ >.

[411]Geeking with Greg, "A chance to play with big data", online: Glinden BlogSpot <http://glinden.blogspot.ca/2006/08/chance-to-play-with-big-data.html>.

Times reporters, Michael Barbaro and Tom Zeller, to recognize clues to the identity of a user tagged as number 4417749 through search queries such as ""dog that urinates on everything", "landscapers in Lilburn, Ga.", which linked the queries to Thelma Arnold, a sixty-two-year-old widow from Lilburn, Georgia.[412]

On the other hand, Cavoukian & El Emam argue that anonymization reduces the risk to privacy.[413] They contend that employing anonymization techniques such as randomizing to remove direct identifiers such as name, email address, home address, telephone number or quasi-identifiers such as gender, marital status, postal code or location information.[414] Another way is to mask the data by adding unrelated information or generalizing the data such that it is difficult to link it a particular person.[415] But then, reduction does not totally eliminate the risk. For them, no 'iron clad' guarantee exists to completely anonymize data. They thus suggest a novel approach known as "privacy by design"[416] which literally means building privacy into technologies and processes for collecting, using or disclosing information. They conclude that this approach would anticipate risks to privacy and prevent them from occurring as opposed to an approach that provides redress after the fact.

But the position of Cavoukian & El Emam above is arguable. Their approach in one breath acknowledges the unreliability of anonymization techniques in re-identifying anonymized data.

---

[412] Michael Barbaro & Tom Zeller,"A Face Is Exposed for AOL Searcher No. 4417749", *New York Times* (August 9, 2006)online: New York Times < http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=2&>

[413] Ann Cavoukian & Khaled El Emam, *supra* note 193.

[414] *Ibid.*

[415] Ross Fraser & Don Willison, "Tools for De-Identification of Personal Health Information", online: Pan Canadian Health Information Privacy (HIP) Group <https://www.infoway-inforoute.ca/index.php/component/docman/doc_download/624-tools-for-de-identification-of-personal-health-information>.

[416] *Ibid*.

Their suggested approach, privacy by design, is not meant to prevent either but rather to embed practices for protecting privacy "in processes in which personal health information is collected, used and disclosed".[417] Their suggestion is that the designs of products and systemic processes of organizations take protection of privacy into account from the outset.[418] In other words, that privacy is "built"[419] in the design of technologies such as mobile devices and also incorporated in the operational practices of companies. However, the exact specifics of how this approach works in practice is presently indeterminable,[420] as such any discussion on it would be limited.

Thus for the *Directive*, limiting its scope to strictly identifiable data fails to take cognizance of the risk to individual privacy from re-identified anonymous data. Against this background, because of the risk of reidentification, it is suggested that the provisions of the *Directive* should also be applicable to anonymous data.

5.4.1.5 *Absence of Any Reference to Location Data*

As noted, although the *Directive* lacks specific reference to mHealth, however it is directly relevant because it aims to protect personal information processed "automatically".[421] As was decided in the case of *Durant* above, any processing in electronic or computerized form would come within the definition of automatic processing under the *Directive*.[422] However the *Directive* leaves one in doubt as to how this would apply to location data generated by mobile devices or mobile health applications.

---

[417] *Ibid*.
[418] See Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices", online: Office of Information and Privacy Commissioner of Ontario < https://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf>.
[419] Ira S Rubinstein, "Regulating Privacy by Design" (2011) 26 Berkeley Law Journal 1409.
[420] *Ibid* at 1421.
[421] *The Directive,* Art 3 (1).
[422] Durant*, supra* note 403.

As noted earlier, apart from the text-messaging capabilities of these mobile devices, some have advanced features, such as GPS navigation capabilities, which make it possible to track users. Some use information provided by the GPS feature to track or identify where health service is required.[423] In some cases, although this feature is totally unrelated to the provision of a mHealth service they collect users' location data and create a profile about them on the basis of their location.[424] With the profile created, service providers can send targeted advertisements that are not related to the mHealth service even where users have not consented to the collection of their location data.

In the absence of any guidance, it may be argued that this means that the data controller has the absolute discretion to determine what information, including location data of the subject, would be required for processing. It may also decide that other bits of information apart from the health information of the user are required for its purpose. This raises the issue whether a mHealth user should be subject to the whim of a data controller in this manner.

5.4.2 *The E-Privacy Directive*

The provisions of the *E-Privacy Directive* appear to supplement the provisions of the *Directive* in regard to matters it did not specifically cover in the face of challenges posed by new technologies.

[423]Ngala Kilian Chimton, "New mHealth project helps save lives in Cameroon" online: SciDev <http://www.scidev.net/sub-saharan-africa/icts/news/mHealth-project-helps-save-lives.html>.
[424]"A Consumer Privacy Bill of Rights, Part I"(Dec 25, 2013),TheSpiderOak Blog <*https://spideroak.com/privacypost/cloud-security/consumer-privacy-rights-part-i-protection-of-user-data-on-mobile-apps/* >.

Like the *Directive*, the *E-Privacy Directive* aims to "harmonise the provisions of member states… with respect to the right to privacy, with respect to the processing of personal data".[425] The *E-Privacy Directive*, however goes a step further to provide rules on the use of location data, unsolicited commercial messages or data for telemarketing purposes.

Unlike the *Directive*, it is more limited in scope as it applies to privacy in the electronic communication sector. First, it governs location data which has become the subject of increased use by mobile applications and platforms. Data about a user's geographical location can be used to provide context-based service, such as information about one's surroundings[426] or maps for directional purpose. Although they make life easier, they also present new concerns. According to Lothar Fritsch, location data may be used to profile a person or a particular class of people with the implication that may be potentially stereotyped or stigmatized.[427] They could even be marked out for surveillance and monitoring.

As indicated, what the *E-Privacy Directive* has done is lay down the rules regarding the processing of location data when made anonymous, or when they are collected with the prior consent of the user.[428]This is absent under the *Directive*. Since the *E-Privacy Directive* supplements the *Directive,* the implication is that reliance can be placed on this aspect of the *E-Privacy Directive* when providers of mobile services collect the location data of users without their knowledge or consent.

---

[425] *The E-Privacy Directive*, Art 1.

[426] Carlo Ratti et al, "Mobile Landscapes: Using Location Data from Cell Phones for Urban Analysis "online: SENSEable<http://senseable.mit.edu/papers/pdf/RattiPulselliWilliamsFrenchman2005E&PB.pdf >.

[427] Lothar Fritsch, "Profiling and Location-Based Services (LBS)" in M. Hildebrandt and S. Gutwirth, eds, *Profiling the European Citizen: Cross-Disciplinary Perspectives* (New York: Springer, 2008)147 at 150.

[428] *The E-Privacy Directive,* Art 9.

Further, because of its provision on unsolicited communications, data provided by a user may only be used in the context of the service or sale agreed between the parties.[429] Using a user's data for commercial purposes to send them unsolicited communications via text messages on mobile phones is prohibited except where the user has given their consent to such use.

For mHealth, apart from the fact that unwanted text messages could be annoying, the implication of sending out unsolicited communications is that the sensitive health information of the mHealth user is being shared with third parties in circumstances which constitute an invasion of the privacy of the user. Such communication also implies that the commercial advertisement was generated using the data provided by the mHealth user.[430]

5.5 Conclusion

From the foregoing, the *Directive* in combination with the *E-Privacy Directive* provide sufficient protection for mHealth privacy. The *Directive* provides the standards for processing of personal information generally. In addition, it delimits health information as part of a special category requiring additional conditions for their processing. While the challenges posed by the use of location data in new technologies is not covered by the *Directive*, the *E-Privacy Directive* provides a supplementary prescription by bringing location data, which may be used provide

[429] *The E-Privacy Directive,* Art 13 (1).

[430]See "PIPEDA Report of Findings #2014-001:Report of Findings Use of sensitive health information for targeting of Google ads raises privacy concerns", online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/cf-dc/2014/2014_001_0114_e.asp>.In that Report, the Office of the Privacy Commissioner of Canada investigated a complaint laid against Google Inc. (Google) for delivery of tailored contents relating to medical devices based on sites by visited the complainant. The complainant had used Google to search online for medical devices for sleep apnea. Since conducting the search, he was inundated with various websites that display advertisements of similar devices. The complainant stated that since he did not provide Google with consent to display or share his personal medical information, Google should not use same for commercial purposes. The outcome of the Privacy Commissioner's report aligned the complainant's position. It found that Google had contravened the provisions of the *PIPEDA* by using his information collected from his online experience to deliver adverts without seeking and obtaining his consent.

context-based service to a user without their consent, within its purview. Thus, this makes the EU regime constitutes a credible framework to build a potentially effective regime for protection of health information through mobile devices.

The preceding analysis of the EU-wide legislation and the *Directive* and the *E-Privacy Directive* shows that more protection exists for personal information under the structure they provide, than under the legal regime in Nigeria examined in the previous chapter. The *Directive* covers the general requirements for processing of personal information generally, and more specifically in relation to processing of health information which is categorized as special.

In addition, the *E-Privacy Directive* expands the protection available in the EU with focus on, technological innovations in electronic communications such as mobile phones. Among others, it provides that location data could be generated by these technologies and it protects users' rights in regard to violations in ways not mentioned in the *Directive*. In essence, the *E-Privacy Directive* fills in apparent gap left by the *Directive*. Thus, the suggestion is that since one caters for the apparent gap in the other, they should be considered as a single framework that works for mHealth privacy.

It is noteworthy that although the European regime is not without deficiencies, however it is better than no protection at all. Against this background, the lessons offered by this chapter are drawn on in chapter six to analyse what improvements it could influence within the Nigerian context. The analysis admits that though the conceptual framework could be adopted for Nigeria, the socio-cultural problems discussed in chapter 3 and institutionalizing their implementation could present constraints to their consideration. Overall, the next chapter considers these issues in the light of Nigerian context and offers some suggestions on how they may be tackled.

Chapter Six

Reforming Nigerian Privacy Legislation

6.1 Introduction

As shown in chapter three, mHealth is growing at a rapid rate in Nigeria. Increasingly, it has become a useful tool to address the challenges and shortages in the health sector. It was shown that although there is a huge market for mHealth in Nigeria, the same cannot be said for its legal regime on protection of the health information of citizens who use mHealth.

The two pieces of legislation examined in chapter five serve as a model for the promulgation of data protection laws in Europe. Particularly, the *The European Union Data Protection Directive 95/46/EC* has become reference material for data privacy laws for countries outside Europe. For mHealth, the *Directive* is useful because it classifies health information as belonging to a special category which may only be processed where certain conditions have been met. This is in addition to the processing meeting all the requirements for processing of other classes of personal information. As well, The *E-Privacy Directive* is instructive as it complements the *Directive* by laying down the conditions for processing of location data from mobile devices and the use of such data for marketing purposes. These are issues missing from the *Directive*.

Notwithstanding the potential which the EU regime offer for mHealth, however, in considering the application of its rules and principles to Nigeria, the question to grapple with is what promise they hold for being adopted and to constitute an effective regulatory regime in the country.

The challenge is that while the socio-economic and cultural realities in Europe may have made the application of the EU wide legislation possible, the contextual differences with Nigeria in

those socio-economic and cultural regards requires toeing a fine line between the ideal and what is practical in the latter environment. With respect to the cultural context aspect, it was discussed in chapter 3 that Nigeria's communal values in terms of their impact on inter-personal and privacy issues may make the rules and principles of the EU-wide legislation difficult in application within Nigeria's cultural environment.

This dim prospect is compounded by the systemic problems of corruption and related concerns which constitute the socio-economic realities in Nigeria and into which those rules and principles may be called upon to intervene for the protection of mHealth information.

Against this background, this chapter examines the prospects for adapting lessons from the European regime to, at least suggest a conceptual framework for privacy legislation for mHealth in Nigeria. The hope that the European influence could take root in Nigeria in this matter is offered by the example of South Africa which has a similar background to Nigeria. Drawing on that example, an argument is made that notwithstanding socio-economic and cultural differences with Europe, South Africa demonstrates that the protection of the privacy of citizens need not be held back by such differences. South Africa has adapted the European model for its needs, and this means Nigeria can do the same.

In the following sections, the prospects of adopting the EU regime are considered. Two prospects, albeit from an economic standpoint for Nigeria, are identified. The challenges and problems in the light of socio-economic and cultural realities are also discussed. Regarding the cultural challenge, it will be argued that although the culture of communalism pervades social relations in Nigeria, respect for personal privacy or its protection cannot be ousted.

6.2 Prospects of Adopting the European wide Legislation as a Conceptual Framework

6.2.1 Opportunity to Participate in a Globalized Regime for Privacy Protection

At present, apart from the EU countries, 33 non-European countries have data privacy laws with visible influences of the *Directive,*[431] thus making it a global standard for privacy protection all over the world.

According to Roos, there seems to be an international consensus to adopt data privacy legislation embodying the principles espoused in the *Directive*. This consensus is without regard to differences in legal traditions, culture or social values that should ordinarily be pleaded to defend not adopting it.[432]

Many commentators have sought to explain the basis for this international consensus.[433] Bennett posits that the rationales behind this broad international consensus are fivefold.[434]

First, he notes that "technological determinism"[435] is a major force behind this consensus. In the industrial age, the major economic, social and environmental problems of countries were unemployment, diseases, pollution and uneven distribution of wealth between the rich and poor in society.[436] However, because the solutions to these problems depended on the ability of each nation to direct its resources -- both human and material to this end, each country framed its

---

[431] Graham Greenleaf, *supra* note 309.

[432] Anneliese Roos, "Core principles of data protection law"(2006) 39 The Comparative and International Law of Southern Africa 102 at 107.

[433] Michael D Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy"(1980)16 Stan J Int'l L 29, cited in Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States,*(New York: Cornell University Press,1992)at 118-43.

[434] Colin J Bennett, "Privacy in the Political System: Perspectives from Political Science and Economics", online: Colin Bennett < http://www.colinbennett.ca/wp-content/uploads/2012/06/Privacyin-the-Political-System.pdf>.

[435] *Ibid.*

[436]Sjur Kasa,"Industrial Revolutions and Environmental Problems", online: Confluence<http://www.cas.uio.no/Publications/Seminar/Confluence_Kasa.pdf>.

solutions according to its specific needs**.** He opines that in post-industrial society (the information age), however, information has replaced human and material resources as the key resource. Information, unlike the social, economic and economic problems of the industrial age, has however had little or no cultural elements to constrain state responses to the threats in similar ways.[437]

Second, he notes that the consensus was founded on a motivation to draw upon lessons from abroad. According to him, data privacy presents new policy problems that most states do not have readily available solutions for. As such, nations are willing to draw from the experiences of others. This does not imply an outright imitation or adoption of the policy response in one country by another, but rather a consideration of the evidence of the policy impact abroad and the utilization of this evidence in law making.

Third, he identified that interactions among key policy actors, interest groups, and elite members of national governments who are bound by their shared expertise as data protection experts, enable them to exchange ideas, and thus to sufficiently influence the cause of data protection within their respective countries.[438]

Fourth, he cited the emergence of international organizations and the trend towards a harmonized legal order among countries as another reason for the consensus. International organizations such as the Council of Europe and the Organization for Economic Cooperation and Development, have developed international agreements embodying data protection principles to guide conduct in member states on data and privacy protection.[439]

---

[437] Bennett, *supra* note 433 at 118-22.
[438] *Ibid* at 127-29.
[439] *Ibid* at 130-40.

Finally, there is consensus because the world has become "interdependent". As such the implications of the policy framework adopted in a particular country may force other countries to conform or suffer the consequences of retaining a different legal framework. For example, where a country fails to legislate a data privacy legislation with an adequate level of protection as required by the Council of Europe Convention,[440] such a country risks being isolated economically.

Of all Bennett's reasons, the technological paradigm seems to be a particular imperative for common data privacy legislation. Advances in the field of technology have transformed the way data is collected and stored. According to Solove, details that were once captured on scraps of paper can now be preserved forever on gigantic databases that house such personal data as an individual's race, gender, income, sex and it is possible to build an electronic collage about a person's life.[441] The public or private bodies amassing these databases could be located across the world, and they could use technology to collect a trove of information about individuals worldwide unknown to the persons concerned,[442] notwithstanding the varied implications of doing so. In some cases, collection of these non-identifiable pieces of data is beneficial to society, such as when they provide data for public health surveillance purposes. But the manner in which these bits of data are amassed and sold or transferred across organizations and countries calls for some control.

---

[440]Council of Europe, CA, 32nd Sess, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*, Texts adopted, ETS 108 (1981).

[441]Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001)53 Stan L Rev 1393 at 1394.

[442]James Ball, "NSA collects millions of text messages daily in 'untargeted' global sweep" *The Guardian* (16 January 2014), online: The Guardian< http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep>.

Further, increasing integration and interdependence among national governments and the trend towards a uniform legal order have informed this uniformity. These linkages are encouraged by advances in information and communications technology which is driving the world towards a global society. For example, increasingly governments provide personal information about their citizens to governments of other nations for various reasons, such as to control terrorism. Private organizations also transfer data on their customers from one country to the other.[443] These situations raise the question as to which domestic legislation would be applicable when legal problems arise. At this time, it is felt that the existing legal protections in most countries of the world are insufficient to address the potential disputes that would arise from the uses of advanced information technologies.[444]

Beyond legal concerns, the consensus was driven by intense lobbying from states and political actors. These players have reasoned that a disjointed approach to data privacy legislation could work against their interests.[445] The consequence is the articulation of certain general principles regarding the use, collection and disclosure of personal information. These principles, known as the 'Fair Information Principles',[446] emanated from a 1973 report by the US Advisory Committee on Automated Personal Data Systems.[447]Thereafter, they became popular through

[443]Ulrich Sieber, "Legal Order in a Global World– The Development of a Fragmented System of National, International, and Private Norms" (2010) 14 Max Planck Yearbook of United Nations Law 4.

[444]Roger Clarke, "The OECD Data Protection Guidelines: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law", online: Roger Clarke <http://www.rogerclarke.com/DV/PaperOECD.html>.

[445] Abraham L Newman, *Protectors of Privacy*: *Regulating Personal Data in the Global Economy* (London: Cornell University Press, 2008) at 11.

[446] Some refer to these principles as Fair Information Practice Principles (FIPPS) or Fair Information Practices (FIPS). It is pertinent to note that they are comprised of essentially the same principles, although in this thesis, Fair Information Principles are used.

[447] See The United States Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens* (Cambridge:MIT Press,1973).In the United States, they also appear in other legislation such as the US Privacy Act, which deals on personal information may be collected, used and disseminated by federal agencies; the *Privacy Rule* issued by the

their endorsement by the world's major economies[448] via the 1980 Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*[449] The principles have since been codified and appear in many national data protection laws and international agreements on data privacy.[450] Though formulated with variations, they share the common purpose of seeking to protect individuals and requiring adequate safeguards for the privacy of their personal information.[451]

Nigeria could participate in this global trend. By adapting the European model, it would assure adequate protection within its territory, and also benefit from the free but controlled flow of information that the European model facilitates.

The major benefit that Nigeria could gain, which is relevant to private information protection, is in terms of its cross-border transfer. This point is briefly discussed next.

6.2.2 Protection for Cross Border Transfer of Personal Information

As earlier discussed in chapter 5, an important aspect of the *Directive* is its restriction on cross border transfers of personal information. It requires that personal data should not be transferred outside Europe to countries that do not offer adequate protection.[452]In other words, the transferee country must in the estimation of the European Commission, have an acceptable level of

---

Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act and the Children's Online Privacy Protection Act (COPPA), which articulates requirements for parental notice or consent for collection of personal information from children under the age of 13 by websites or online services.

[448] Fred Cate, Peter Cullen &Viktor Mayer-Schönberger, "Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines", online: Oxford Internet Institute<www.oii.ox.ac.uk/.../Data_Protection_Principles_for_the_21st_Century.pdf>.

[449] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1981,online: Organization for Economic Co-operation and Development< http://www.oecd.org/>/ .

[450] Colin J Bennett & Charles D Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press, 2006) at 19.

[451] Colin J. Bennett, "What Government Should Know about Privacy: A Foundation Paper", online: Colin Bennett <http://www.colinbennett.ca/wp-content/uploads/2012/06/What-Government-Should-Know-about-Privacy.pdf>.

[452] *The Directive*, Art 25.

protection which is reflected in factors such as its rules and security measures.[453] Alternatively, adequacy may be evidenced by contracts with terms or clauses showing that sufficient safeguards are being employed for the transfer to the non-EU country.[454]

For mHealth, health information or data about an individual may need to be transferred outside the country for processing by healthcare practitioners involved in the care of the patient. The benefit is that timely and accessible healthcare is provided to the patient and efficiency of the health sector is improved as a whole. As such for countries not complying with the EU standards as to adequacy, the implication is that the health information of the patient may not be transferred.

Again, as earlier discussed for Nigeria, its health sector is fraught with many challenges, including shortage of skilled medical personnel and inadequate infrastructure or access to medical services. Particularly, rural dwellers are underserved in terms of health service provision and access. These are the challenges mHealth has come to address. The implication of adopting a framework in the style of the *Directive* is that where the health information of Nigerians may need to be transferred to countries with similar protections; there is a guarantee of their protection, and vice versa. But as set out in the Introduction, there are roadblocks in the way for Nigeria even if it wishes to adopt and adapt the EU model. These socio-cultural challenges are considered in the next section.

[453] *Ibid.*
[454] *Ibid.*

6.3 Potential Challenges or Problems to the Adoption of the European framework

6.3.1 Culture and the Place of the Individual in Society

Cultural considerations and the perception of the individual within Nigerian society are important to a contemplation of the *Directive* and its adoption into Nigeria's legal system. Perhaps, the first factor to be considered in the nation's cultural system is the assignment of stereotypical roles to men and women. As stated earlier, in some respects, women in Nigeria do not enjoy social parity. The cultural system categorizes the man as the head of the family who takes all decisions concerning all members of his household, including the woman. This constrains the ability of women to take decisions without a male figure such as a husband, a father or a brother. As already discussed in chapter 3, the woman may not seek abortion, sterilization, contraceptive or family planning advice without the involvement of a man. [455]

Secondly, it was also discussed that culturally, the communal style of social relationships in Nigeria lays emphasis on extended family bonds[456]. Relationships in Nigeria are deeply cohesive with emphasis on extended family bonds and institutionalize the expectation for mutual care throughout the extended family. This also means far-removed relatives can make decisions relating to a person's otherwise private personal concerns[457] especially as to their health and welfare, notwithstanding the existence of confidentiality between the person and their physician.

---

[455] Joshua Oyeniyi Aransiola, Akanni Ibukun Akinyemi & Adesegun Olayiwola Fatusi, "Women's perceptions and reflections of male partners and couple dynamics in family planning adoption in selected urban slums in Nigeria: a qualitative exploration", online:(2014) 14 BMC Public Health at 2 <http://www.biomedcentral.com/content/pdf/1471-2458-14-869.pdf>.

[456] Toyin Falola, *Culture and Customs of Nigeria* (Westport: Greenwood Press,2001) at 118

[457] John Mbiti, *African Religions and Philosophy* (Oxford: Heinemann, 1990) at 175-81.

This openness to the larger community[458] includes open accessibility of one's private information to many others. A secretive person or one who sets boundaries with others is perceived as hiding something, and this is a socially unacceptable behaviour.[459]

Nigeria's communal culture contrasts with the Western philosophical conception of the individual where the libertarian philosophy of John Locke gives primacy to the individual [460] to ground its basis for modern rights including the capacity to make rational decisions independently of others.[461]Indeed, Locke espoused that each individual should be allowed "a sphere owned [by him and] untouched by others".[462]The upshot is that individuals in Western societies form their identities separate from the groups or communities to which they belong. Each person is perceived as capable to order their own affairs independently without interference. Unlike the African viewpoint, the Western individual is not socially entrenched and dependent on the community.

To consider the adoption of the *Directive* for Nigeria raises two implications. First, it becomes problematic to determine the voluntariness of consent. As discussed earlier, one of the preconditions for the processing of personal information under the *Directive* is that the data subject must have provided their consent. According to the *Directive*, evidence of consent is one of the ways to show that personal information was lawfully processed.[463] To prove this fact, the

---

[458] See Segun Gbadegesin, *African Philosophy: Traditional Yoruba Philosophy and Contemporary African Realities* (London: Peter Lang, 1991) at 292.

[459] Philip Brey, Frances Grodzinsky & Lucas Introna, *Western Privacy and Ubuntu: Influences in the forthcoming data privacy bill: Proceedings of the Sixth International Conference of Computer Ethics, Enschede,The Netherlands, 2005*.

[460] John Locke, *Second Treatise of Government,*1690 at 6 cited in digitized form by David Gowan, "Second Treatise of Government by John Locke "online: Oregon state < http://oregonstate.edu/instruct/phl302/texts/locke/locke2/locke2nd-a.html>.

[461] *Ibid.*

[462] Privacy in the Political System, *supra* note 434.

[463] *The Directive*, Art 7 (a).

Directive requires that consent must be voluntary in the sense that it was freely given by the data subject. In other words, the individual is viewed as an autonomous being with the ability to decide and act on the basis of their independent thought. However, the reality of the cultural setting in Nigeria shows that it may be problematic to ascribe voluntariness to consent. The expression of an individual's will is subject to the influence of the relationships the individual has with other people, especially family members and relatives.

Second, considering the family situation in Nigeria where kinship bonds with extended family members is the norm, it may not be as easy to determine true consent where family members could request access or disclosure of the health information or records of their relative who is a patient. As discussed earlier, it is not strange for family members to be deeply involved in the care their distant relative. In this communal situation, separating the individual from the family could be tantamount to cutting him or her off from relationship with family members.

Even so, does the difference in the cultural philosophy oust the consideration of the *Directive* for Nigeria? Several explanations have been proffered to show that differences in cultural values could impact privacy from one culture to the other. A report commissioned by the European Commission acknowledged this fact as follows

> 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.[464]

Others[465] have identified a relationship between culture and privacy. Hofstede's seminal work on cultural differences, finds that countries like Nigeria has high social inequalities, and members

[464] Charles D Raab et al, "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", online :European Commission <http://ec.europa.eu/justice/data-protection/document/studies/files/19980901_adequacy_methodology_en.pdf>.

are tightly knit, organized and order their lives as collectives. Walczuch, Singh and Palmer also argue that countries like Nigeria are less likely to legislate or enact data privacy laws as the main purpose of such laws is to protect individual rights as opposed to communal or collective rights.[466]

Though plausible, the foregoing explanations may also constitute a sweeping argument for a generic pan-cultural worldview that applies to these societies.

Nigeria is a heterogeneous society. It consists of over two hundred and fifty ethnic groupings with more than five hundred languages.[467]Although the predominant ethnic groups are the Yorubas in the West, the Hausas in the North and the Igbos in the Southeast, even within the three major tribes, there are a mix of other smaller groupings or cultures.

Within these cultures, traditions and customs have come to be influenced and defined by societal changes and external influences. Undoubtedly, before Africa came into contact with western colonization, relations in society were based on family and kindred ties associated with communalism.[468] However, ideas and cultures from other parts of the world have come to affect or sometimes displace traditional norms and practices. With the increased rate of urbanization and movement of people into the commercial hubs for economic reasons, and the fragmentation of otherwise close-knit family structures,[469] there is the tendency for imported ideas and cultures

---

[465] See Sandra J Milberg et al, "Values, personal information privacy, and regulatory approaches" (1995)38 Communications of the ACM 65.

[466] Rita M Walczuch, Snajay Singh & Todd Palmer, "An analysis of the cultural motivations for Transborder data flow legislation", online: ProQuest<http://search.proquest.com/docview/222414212/ED5A89FFD085437DPQ/3?accountid=10406>.

[467] "Nigerian Culture", online: Government of Nigeria, http://www.nigeria.gov.ng/2012-10-29-11-05-46/2012-11-05-09-51-17

[468] Walter Rodney, *How Europe Underdeveloped Africa* (Nairobi: East African Educational Publishers, 1972) at 47.

[469] Dare Arowolo, "The Effects of Western Civilization and Culture on Africa" (2010)1 Afro Asian Journal of Social Sciences.

to displace traditional norms and practices, especially for people who have become alienated from their communal family structures as a result of movement into urban centres.

The implication is that there is a shift in traditional practices, or in some cases, that they are abandoned. For example, there is a gradual displacement of the culturally sexist view of women as caregivers, mothers and nurturers who are regarded as the lesser sex to be forever under the control of their husband or male relatives.[470]So also alienation from extended family as a result of urbanization has led to a change in the traditional African family pattern or family dynamics established on earlier closely knit structures.[471]

This cultural situation is not peculiar to Nigeria. It pervades in most countries in Africa where it is possible to implicate a clash between existing cultural systems and beliefs with the promulgation of a law on informational privacy. As stated earlier, South Africa is one country in Africa that has replicated the *Directive* into its local laws. As with other African countries, it also has cultural traditions of kinship relations and roles. The way South Africa has, in the face of its socio-economic structure, adapted the *Directive* for use is instructive for Nigeria. This example is now considered.

6.4 Through the Eye of Ubuntu: The Replication of the *Directive* in South Africa's *Protection of Personal Information Act*

The Republic of South Africa is a multicultural society comprising a mix of the Ngunis (i.e. the Zulu, Xhosa, Ndebele and Swazi people); the Sotho-Tswana who include the Southern, Northern and Western Sotho (Tswana people); the Tsonga; the Venda; the Afrikaners; the English; the Coloured people (comprising mixed-race descendants of early white settlers and indigenous

[470] Oseni Taiwo, "Power and Womanhood in Africa: An Introductory Evaluation" (2010) 3 Journal of Pan African Studies 229 at 235.
[471] Peter C W Gutkind, "The African Urban Milieu: A Force in Rapid Change" (1962)12 Civilizations 167 at 195.

people), and the Indian people.[472] Of these multiple ethnic groups, the majority are Africans or black South Africans who make up more than half the population.[473]

In this multicultural society, the culture centres on communalism. Expressed as the *"Umuntu ungumuntu ngabanye abantu"*[474] *(*a person is a person through other persons) in the Nguni language, this expression, shortened as *Ubuntu*, has come to define the African view on communalism in South African society.

Ubuntu is a relational concept which suggests that the only way to develop one's humanity is to relate to others in a positive way. One becomes a person through other persons, meaning that one's true self can only be realized in association with others and not in opposition or isolation from them. Values such as respect, humaneness, compassion and dignity implied by the aphorism are also critical to the attainment of personhood in society. Thus, a person has *Ubuntu* where he or she

> …is open and available to others, affirming of others, does not feel threatened that others are able and good, for he or she has a proper self-assurance that comes from knowing that he or she belongs in a greater whole and is diminished when others are humiliated or diminished, when others are tortured or oppressed.[475]

An essential aspect of *Ubuntu* is its understanding of the human person as a communal being who is interdependent and mutually bound with others in society. Because they are mutually bound, each is expected to look out for the interests of the others, and each person has a role to play in ensuring that the existing system of social cohesion is not interrupted in any way.

---

[472]"Pocket Guide to South Africa 2011/12: South Africa's People"online: Government of South Africa <http://www.gcis.gov.za/sites/default/files/docs/resourcecentre/pocketguide/004_saspeople.pdf>.

[473] *Ibid.*

[474]Philip Brey, *supra* note 459.

[475]See "Archbishop Desmond Tutu on Ubuntu", online: Tutu Foundation <http://www.tutufoundationuk.org/ubuntu.php>.

According to Kamwangamalu[476], *Ubuntu* in South African culture is evident in oral traditions of proverbs and maxims which demonstrate its importance in society. One such proverb is: *Nkunda ya bangi itu iboba ne mata*,which literally means "Beans cooked by many can cook with saliva", in other words, it says "Unity is Strength". Another proverb is: *Babidi kabakukumi batu bakushiya diulu nsoso*, which literally means "if two people fight against one person they will win the fight". These proverbs show the importance of communal solidarity and unity.

Thus, unlike the West, in South Africa, *Ubuntu* defines personhood in communal terms. An individual is not an isolated entity whose personhood is expressed in autonomous space separate from others in society. Rather, the individual is expressed in terms of mutual relationships and the interdependence formed with other members of the community.

Against this *Ubuntu* background, one would doubt that privacy legislation in the nature of the *Directive* could be passed into law in South Africa. Ndebele et al, have argued that since *Ubuntu* espouses notions of family, community, and sharing and solving of life problems with family members,[477] it would be difficult for physicians to maintain the confidences of patients who have HIV/AIDS or for such patients to assert control over who has information about their health conditions. They identify that due to this culture, medical personnel must inform family members about the health status of a patient, the origins of the disease and sometimes the treatment options, and that this is necessary to show respect for the communal practice of

[476]Nkonko M. Kamwangamalu, "Ubuntu in South Africa: a sociolinguistic perspective to a pan-African concept" (1999)13 Critical Arts: South-North Cultural and Media Studies 24 at 28.

[477] Paul Ndebele, Joseph Mfutso-Bengo & Francis Masiye, "HIV/Aids reduces the relevance of the principle of individual medical confidentiality among the Bantu people of Southern Africa" (2008) 29 Theoretical Medicine and Bioethics 331 at page 337.See generally Mogobe Ramose, *African Philosophy through Ubuntu* (Zimbabwe: Mond Books Publishers, 2002).

problem sharing under *Ubuntu*.[478]Where a physician or medical personnel decide to be secretive, the patient may be neglected by family members, or the decision could strain family ties.[479]

Thus, the position of Ndebele *et al* suggests that, notwithstanding its merits, *Ubuntu*, reduces or takes away patients' privacy. But according to Olinger et. al., "*Ubuntu* is an idealised concept… [because] there exists no *Ubuntu*-specific references to privacy".[480] To do so would be to draw a wrong inference of a value which is not present, unlike values of respect, humaneness, compassion and dignity which have strong expression within the *Ubuntu* philosophy. The aim of *Ubuntu* is to achieve social harmony and peaceful coexistence through close social relations between members of society, rather than have an atomistic society.

Indeed, the communitarian leaning of *Ubuntu* did not deter the enactment of a data privacy law. When asked about the what extent to which the Department took into account cultural sensitivities when drafting the Bill that eventually became the *Protection of Personal Information Act*,[481] Ms. Ananda Louw, Principal State Law Adviser in the Justice Department said:

> [E]ach person had a conception of what privacy was. Some people would argue that one had no privacy. If a person signed up for Facebook, then one had no privacy. What the department found in all the different cultures was that if one had a lovely face, one did not mind having a picture of one's face taken, but if one had ugly legs then one would not want a person to take a picture of those legs. Something was private if the

[478]Paul Ndebele, *Ibid* at 335-36.
[479] *Ibid* at 338.
[480] Philip Brey, *supra* note 459 at 17.
[481] Republic of South Africa, *Protection of Personal Information Act*, 2013. It is noteworthy that although the South African Act was passed into law in 2013, only establishment provisions relating to the powers and functions of a regulatory body as well as other procedural provisions on filing of complaints, investigations administrative fines, came into effect as at April 2014. There is as yet no indication of when its substantive provisions would come into effect. See Striata, "POPI - to Act or not to Act? That is the question..." (2 March 2015),online:WebTech Forum<http://www.itweb.co.za/index.php?option=com_content&view=article&id=141547:POPI-to-Act-or-not-to-Act-That-is-the-question-&catid=355#prcontacts>.

person concerned regarded it as being private. The law was there to protect those who indicated that they want their privacy protected.[482]

The above indicates that though legal reform should be sensitive to its cultural context, culture may play a limited role in influencing the law's duty to protect people where there are concerns about privacy. If anything, the implication of the use of an individual's information, for example, an HIV/AIDS patient being exposed to discrimination and stigma, has come to impel privacy concerns in South Africa and, thus, the law's response to its protection.

The foregoing may be represented thus: communalism (whether expressed as *Ubuntu*) is vital to the ordering of social relationships in African societies. It provides a structure for cohesion and harmony in society by defining 'personhood' in terms of interconnectedness rather than in terms of an isolated view of the individual as a person. Its objective is to ensure that people look out for each other rather than only for their self-interest[483] and to form interdependent relationships with others for their survival, and to promote social harmony. Symptomatic of this culture is that individuals should be open rather than isolated from others.[484] All these do not indicate that personal privacy is antithetical to the *Ubuntu* culture.

In sum, despite the perceived inference that *Ubuntu* contradicts protecting one's personal information from others, South Africa enacted a privacy legislation modelled after the *Directive*. Although one can say that by modelling its legislation on just the *Directive* alone and not in combination with the *E-Privacy Directive*, the South African legislation does not offer an adequate regime for personal information protection. However, one thing the South African

[482]Parliamentary Monitoring Group (PMG), "Protection of Personal Information Bill [B9-2009] briefing"(6 October 2009)online: Parliamentary Monitoring Group <http://www.pmg.org.za/report/20091006-protection-personal-information-bill-b9-2009-briefing

[483] Moeketsi Letseka, "African philosophy and educational discourse", in Phillip Higgs et al, eds, *African Voices in Education* (Juta Academic: Cape Town, 2000) at 180.

[484] Philip Brey, *supra* note 459.

example has clearly shown is that the *Ubuntu* culture may be an ideal cultural concept, but it does not override the individuals' right to privacy and its protection.

This is not to say that law cannot be influenced by culture. In many aspects of the legal systems in Africa, it is possible to see customs or indigenous practices on marriage or inheritance[485] given prominent influence in personal law on inheritance succession. Some of these traditional customs and practices have been passed down from preceding generations and remain visible, though unwritten rules in society. In some instances, they become subjects of litigation before the courts. The same cannot be said for communitarianism or *Ubuntu*'s perceived stance on personal privacy.

How then does the foregoing impact a consideration of the *Directive* by Nigeria? First, if we adopt the view that communalism is a feature of all the ethnic groups in Nigeria, then it means that individuals are perceived as interconnected and mutually bound with others in society. Yet, just as *Ubuntu*, there are no express norms in any Nigerian culture that indicate that pursuing one's privacy is an antithetical value. On the other hand, even if we accept the view that the culture of openness and social cohesion exists in these cultures negates individual privacy, the cultures do not provide any solution regarding the need to protect one's personal information from the increasing risks brought about by advances in technology.

Another potential challenge to a consideration of the *Directive* for Nigeria stemming from culture is the assignment of gender stereotypes and cultural views on respect for elders and older kinsmen. This challenge and its effect on the construction of consent as provided in the *Directive* is discussed below.

[485] Muna Ndulo, "African Customary Law, Customs, and Women's Rights" (2011) 18 Ind J Global Legal Stud 87 at 89-93.

6.5 Cultural Views on Respect for Elders and Gender Stereotyping

It has been shown that Nigeria is a society based on hierarchical social structure with differentiated roles founded on age and gender. Age is believed to confer wisdom, and so society requires that the older ones be respected and revered[486] as repositories of communal wisdom.[487] In Nigeria, it is not strange for the elders of a clan to make decisions intended to direct clan members in the course they think is best in a particular situation.

Along with this is the patriarchal nature of traditional Nigerian society which promotes male domination and the marginalization of women by the men. As discussed earlier, women are not favoured for economic opportunities as regards the ability to make decisions concerning their lives.[488]

As currently framed in the *Directive*, for consent to be valid, it must have been freely given by the data subject.[489] For Nigeria, implementing this requirement would be a challenge. This key element to authorize the collection and use of health information under the *Directive*, is according to the Opinion of the Article 29 Working Party on data protection in electronic health records, based on the idea that consent is freely given when it is voluntary and the individual was able to exercise a genuine choice without interference or control from any person.[490]

---

[486] Richard M Steers, Carlos J Sanchez-Runde & Luciara Nardon, *Management Across Cultures: Challenges and Strategies* (Cambridge: Cambridge University Press, 2010) at 113. They are considered to be the vast reservoirs of the collective wisdom that has been accumulated over time. See also Ian Macdonald, "The Counsel of Elders", online: South Africa the Good News < http://www.sagoodnews.co.za/newsletters/773-the-counsel-of-elders.html>.

[487] Chris Esionwu, "African Cultural Values"online: Academia.Edu <http://www.academia.edu/5015800/African_cultural_values>.

[488] Oyediran & Olusola, *supra* note 214 at 117-18.

[489] *The Directive*, Art 2 (h).

[490] Council of Europe,PA,3rd Sess,*Working Document on the processing of personal data relating to health in electronic health records (EHR*), (2007).

The problem here is that this provision fails to note that human beings are a product of social relations.[491] As a prescriptive rule, they internalize society's constructs and answers to its demands and expectations. In a Nigerian context, constructs on gendered roles determines who owns 'property' in the household, such as a mobile phone, and who can take decisions, such as seeking medical advice through mHealth or a decision to share health information. For example, available studies show that apart from economic factors, cultural issues like the traditional roles of men and women are essential determinants of mobile phone ownership.[492] These gender roles promote subjugation of women by men, and more men than women own mobile devices like mobile phones. The result is that even for women who own mobile phones, authorization to consult for medical treatment or to consent to the use of their health information may emanate from the males in their family or within the community. The same goes for the elderly who could make decisions on behalf of other family members.

The question may then be whether an understanding of 'freely given consent' can be tailored to fit the Nigerian context. The solution may lie in domesticating the construction of consent to fit societal stereotypes about gender roles and the culture of respect for elders in issues as decision making. Alternatively, a threshold may be created for consent which is framed around the contextual peculiarities of the Nigerian society.

Beyond the foregoing are issues of differences in the socio-economic environment between Nigeria and Europe. The latter has robust economies and less corruption. Nigeria is a society which thrives on the use of public office for private gains, and this culture impacts the efficiency

---

[491] Catriona Mackenzie & Natalie Stoljar, *Relational Autonomy: Feminist Perspectives on Autonomy, Agency, and the Social Self* (New York: Oxford University Press, 2000) at 58.

[492] "Women & Mobile: A Global Opportunity A study on the mobile phone gender gap in low and middle-income countries", online: GSMA<http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/01/GSMA_Women_and_Mobile-A_Global_Opportunity.pdf>.

of its legal system. Second, the level of illiteracy and poverty in Nigeria as compared to the countries in Europe where the *Directive* and the *E-Privacy Directive* operate, is another source of concern in the consideration of the EU-wide legislation for Nigeria. The next two sections take these challenges up one after the other.

6.6 The European Model in a Corrupt Legal System

It has been discussed already that one of the features of the *Directive* is that it requires the establishment of a supervisory body to monitor the application of its provisions with regard to the processing of personal information. This body has the power to investigate any complaint of wrongdoing under the provisions of the *Directive*, and to issue orders, such as placing a ban on processing. In addition, this body is required to act with complete independence in carrying out its functions.

While emphasizing the need for such a body to be independent, the Court of Justice of the European Union, in a case concerning the independence of the Hungarian Data Protection Commission, stated as follows

> …Article 28(1) of Directive 95/46 must be interpreted as meaning that the supervisory authorities responsible for supervising the processing of personal data must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes inter alia any directions or any other external influence in whatever form, whether direct or indirect, which may have an effect on their decisions and which could call into question the performance by those authorities of their task of striking a fair balance between the protection of the right to private life and the free movement of personal data…the operational independence of supervisory authorities…is thus an essential condition that must be met.[493]

In this case, the appointment of a data protection supervisor was prematurely brought to an end by the Hungarian Parliament. Instead of serving a full term of six years, the supervisor four years

[493] *Commission v Hungary*, C-288/12, [2014] ECR at I-12[Hungary].

and was replaced with a new supervisor who was appointed to serve a term of nine years.[494] An action was thus brought by the European Commission against Hungary for failure to fulfill its obligations under the Directive to ensure the independence of supervisory authorities. The Court declared that by prematurely bringing to end, a term served by the data protection supervisor, Hungary had failed to perform its obligations as required by the *Directive*.[495]

By this decision, the European Court of Justice indicated that the independence of a supervisory body is imperative to enable such bodies to carry out their functions without influence. This independence would also have an effect on individuals' rights and how personal information are protected.

As noted earlier, Nigeria has a high corruption index[496] with devastating effects on economic growth and sustainable development in the country. It is visible in how public funds are appropriated by public officials for personal benefit and gain. It is also evident in how the sectional or the moneyed class meddles in the affairs of public institutions to protect their interests.[497] This means that even where a data privacy protection body is created to be autonomous, their independence would, for the most part, exist only on paper.[498]

---

[494] "Judgement of the Court in Case C-288/12", online:Info Curia-Case Law of the Court of Justice < http://curia.europa.eu/juris/document/document.jsf?docid=150641&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=57358..

[495] *Ibid*.

[496] Daniel Jordan Smith, *supra* note 142.

[497]"Impact of Political Interference on Aviation Devt in Nigeria", *This Day Newspapers* (22 March 2013) online: This Day<http://www.thisdaylive.com/articles/impact-of-political-interference-on-aviation-devt-in-nigeria/142837/>.

[498] *Ibid*. See also Ejikeme Nonso Alo, "Independent Commissions in Anti-Corruption Fights: The Nigeria, Uganda and Botswana Examples, 2000-2007" (2014) 16 Journal of Sustainable Development in Africa 47 at 51-54.

It is true that meddling in the affairs of public institutions is not unique to Nigeria as evident in the interference with the affairs of the Hungarian Data Protection Commission.[499] However, past events relating to the activities of independent public bodies in Nigeria seem to show that the problem is markedly pronounced in that country. For example, experience with the functioning of the regulatory body for the mobile communications sector in Nigeria, the Nigerian Communications Commission, shows that such bodies are not free from interference from both government officials and mobile service providers who seek to protect some primordial or selfish interests.[500]

In an atmosphere of corruption, the challenge is that the independence of a body charged with protecting the right to citizen privacy with regards to the processing of health information cannot be guaranteed. Its decisions can be encroached upon by the state, a person or a group of persons, for purposes of their own interest.

6.7 Illiteracy and Poverty

In addition to its corruption index, as already discussed, Nigeria has one of the lowest literacy levels in the world ranking 161 out of 184 countries on a comparison index of countries by literacy levels.[501]Illiteracy is rife in the Northern part of Nigeria where girls are married off in their early teens,[502] and boys are conscripted under the tutelage of Qur'anic teachers so that they do not go to regular schools. In the South- East, most parents would prefer that their children or

[499] *Hungary*, *supra* note 494.

[500] Solomon O Ogundele, "Unbridled bribery and corruption in the Nigerian communications commission (NCC): Dr. Hamadoun Touré, Secretary-General of ITU, guilty by association", Letter to the Editor, *Sahara Reporters* (16 March 2010) <http://saharareporters.com/2010/03/16/unbridled-bribery-and-corruption-nigerian-communications-commission-ncc-dr-hhamadoun>.

[501] Bayo Olupohunda, "The burden of illiteracy in Nigeria", *Punch Newspapers* (24 September 2012) online :< http://www.punchng.com/opinion/the-burden-of-illiteracy-in-nigeria/ >.

[502]Action Health Incorporated, "Insights into Early Marriage and Girls' education in Northern Nigeria"online:Action Health Incorporated < http://www.ungei.org/files/innovators.pdf>.

wards learn a vocation or a trade rather than attend school. This is exacerbated by the significantly high levels of poverty, with more than half of the population living on less than a dollar a day.[503]

The significance of illiteracy and poverty is that people are only concerned about how mHealth provides low-cost or free healthcare services to them. They do not worry about the risks or the means available for their protecting the information they provide in accessing the services.

It was also earlier discussed how poverty and illiteracy brought death when the American multinational company, Pfizer, tested its antibiotic drug Trovafloxacin on the children of predominantly poor and illiterate parents following an outbreak of meningitis in several states in Northern Nigeria.[504]Although this case is not related to protection of health information, it shows that because of their poverty, participation in the trial was the only chance for the research participants to receive any treatment at all.[505] Further, the parents of the participants did not ask questions about the trials due to their illiteracy, and protocols for obtaining informed consent for use of human subjects were not complied with by the pharmaceutical company.[506]

Thus, the concern is not about the existence of a privacy framework, but that people understand how mHealth works, the potential risks to the use of their health information, and are able to seek the protection of the law for a breach or possible breach. Clearly, the solution may lie in addressing the structural issues of poverty and illiteracy in Nigerian society. This would be a

---

[503]"World Bank report on poverty in Nigeria", Editorial, *The Daily Independent* [nd] online: The Daily Independent<http://dailyindependentnig.com/2014/05/world-bank-report-poverty-nigeria/>.

[504] Cheluchi Onyemelukwe, "Regulating Research Involving Humans in Nigeria: Some Recent Improvements" (2008) 16 Health Law Review 36 at 38.

[505]Emmaline Brouwer, "Clinical trials in developing countries" online: Global Medicine <http://globalmedicine.nl/issues/issue-5/clinical-trials-in-developing-countries-2/>.

[506] Cheluchi, *supra* note 504.

broad solution to the problem. A more exact approach, may be for the law to reflect and take into account these inequalities in its provisions. .

6.8 Feasibility of Adoption for Nigeria.

The discussion has highlighted that the regime of the EU as discussed may not be adopted as is without considering some issues for Nigeria. However, using the example of South Africa, a country with similar socio-economic and cultural peculiarities like Nigeria, it has been shown that notwithstanding communalism, the vacuum left by customary norms of protection can be filled in by privacy legislation without undermining the communal solidarity or values.

Further, where it is argued that the construction of consent under the *Directive* may clash with aspects of communal life, the South African example has shown that although traditional customs and practices favor a communal culture of caretaking, this is not a hindrance to the construction of consent as 'freely given' and emanating from an independent individual without any form of influence whatsoever.

With regards to the malaise of corruption which may affect the institutional implementation of the EU regime, it is suggested that this no argument against its consideration. This is because although corruption is widespread and affects all aspects of national life in Nigeria, some government institutions still achieve positive results in carrying out their functions.

In terms of illiteracy and poverty the analysis suggests that a solution may be provoked by the rules of the adopted legal framework. In other words, the law should make provision for education of the poor and illiterate in society about the potential risks to their health information when they subscribe to mHealth.

6.9 Conclusion

There is no doubt that Nigeria and the countries in the EU operate in different socio-economic and cultural milieux. As such, what is feasible in the one context for information protection regulation may be problematic in the other. As shown, Nigeria faces serious socio-economic and cultural challenges if it seeks to provide for privacy protection.

Obviously, it makes economic sense for Nigeria to follow the EU model law on this subject. The move would give it a smoother participation in the emerging global regime on personal information protection. It would also allow for protection of personal information according to international standards, when citizens require external health expertise from mHealth services.

As shown in regard to South Africa, the communal structure of social relations in Nigeria does not negate the necessity and the presence of individual spaces and the need to protect them and the information inherent. Also no culture within the Nigerian matrix has any normative rules on how individual privacy may be protected. Indeed, Nigerians like people all over the world lay claim to their personal privacy. This leaves room to step in by adopting the EU regime to cater for this gap. Even in the face of the potential adverse influences of public corruption on the potential effectiveness of the regime, that this vacuum must be filled is no longer an option. Aside from that, doing so offers a chance for inclusion in an emerging and economically-beneficial global arrangement. At the very least, the illiterate poor will ultimately begin to know that they must ask questions and demand answers or clarification as to use before they give out any information about themselves to anyone, whether such information borders on their health or general matters.

Consequently, although the contextual realities differ, they do not prevent Nigeria from considering the *Directive* and the *E-Privacy Directive* as a single privacy framework for mHealth.

Chapter Seven

Conclusion

The integration of information technology into healthcare is changing the traditional perception of healthcare in many ways, and this has a significant influence on how health services are accessed and delivered. For Nigeria, this integration has come through mHealth, the provision of health services via mobile technologies to assist in addressing the challenges of healthcare access and delivery. However, unlike conventional physician-patient relationships, patients in mHealth provide their health information within a technological context, this makes it hard to determine who has access or with whom such information is shared. The risks from unauthorized disclosure or misuse of health information are that the mHealth user could be discriminated against as a result of their health status, become a subject of surveillance by the government or become stigmatized by society where their health information becomes known to others. It was argued that those dangers have been largely overlooked in the mHealth sector in Nigeria.

A matter of central importance is how the existing legal framework in Nigeria protects personal health information that is collected and transmitted via mHealth. The analysis of Nigerian laws that have implications for mHealth privacy regulation finds that although a right to privacy is constitutionally protected, the patchwork of laws that cater to its protection are inadequate. The *Constitution*, guarantees the rights of citizens to their privacy. However, the problem with this constitutional provision is that its scope is so imprecise that it cannot be determined if it applies to mHealth information. The *Code of Medical Ethics* is also limited in the sense that while it places a duty on physicians to keep the confidences of their patients, the ability of patients to exercise control over such information is constrained as consent as used in the *Code* only exists

in the context of medical procedures and not use of health information. Moreover, although the *Code* places a duty on physicians to take steps to secure patients' health information sent or received electronically, it has been shown that security alone does not wholly protect privacy of health information, there are other principles or criteria that should guarantee fair processing. For the *Consumer Code of Practice Regulations*, while it may appear that principles on fair processing are more detailed, however, the *Regulations* leaves the operation of these principles to telecommunication companies who provide mHealth services. The implication is that these principles are not strictly required and a telecommunication company may decide not to abide some of the principles as laid by the *Regulations* thus giving room for divergent compliance by these companies. The result of the foregoing is that the privacy framework in Nigeria is insufficient and as such huge volumes of data can be generated from information provided by mHealth users, and used in unauthorized ways without regard for their protection.

For Nigeria, mHealth is a novelty. Therefore, to fill the obvious gaps in the legal framework on health information privacy protection, this thesis suggested to look at international standards on mHealth privacy protection. The model pointed to is the current framework available in Europe through the *European Union Data Protection Directive 95/46/EC* and the *Directive on privacy and electronic communications, 2002/58/EC.*

It was pointed out that the *European Union Data Protection Directive 95/46/EC* provides comprehensive regulations for the protection of all classes of personal information, and in particular, it imposes detailed obligations on those who collect personal information. As well, it provides for the rights of the owner of such information to request access to, and to rectify or cancel otherwise wrong information about them. It also has rules on security safeguards for personal information, such as when they are transferred outside of Europe. Particularly, health

information is categorized as a special class, and additional conditions are laid down for its processing.

One weakness in the *European Union Data Protection Directive 95/46/EC* is lack of provision regarding protection for location data. The importance of location data regulation is particularly relevant in mHealth as there are mobile devices with GPS navigation capabilities, as well as mHealth services that collect users' location data. The absence of any rule on this issue implies that location data may be used by service providers to target advertisements that are not related to the mHealth service even where users have not consented to the collection of their location data. This gap is closed by the *Directive on privacy and electronic communications, 2002/58/EC* which lays down rules on processing location data. In sum, it provides that location data may not be used to send unsolicited communications via text messages or by way of targeted commercial advertisements, except where the user has provided their consent to such use.

This thesis finds that although Nigeria could draw on the important lessons provided by these two pieces of legislation on protecting mHealth privacy, the prospect is challenged by the realities of the socio-economic and cultural environment of the country. In particular, it was emphasized that social relations in Nigeria favour sharing and openness in ways that may be inconsistent with claims to the control of one's health information under a privacy legislation. Moreover gender stereotyping and social obligations may so influence a person's consent to the extent that the idea of consent as 'freely given' may not be easy to assure in some sections of Nigerian society. The socio-economic factors that compound this difficulty are poverty, illiteracy, and the high corruption rate among public institutions in Nigeria. These factors make it difficult for individuals to secure their privacy interests. As well, corruption undermines the potential of state institutions to effectively enforce the provisions of such legislation.

It was argued that South Africa has a socio-cultural climate similar to Nigeria, but passed a privacy legislation modelled after the *European Union Data Protection Directive 95/46/EC.* As suggested, South Africa's example argues for the fact customs or indigenous practices do not override the individual's right to privacy and its protection. This is especially so where there the cultural norms have no regulatory rules or principles on how to protect personal privacy in view of the increasing risks brought about by advances in technology.

The thesis puts forth the hopeful view that though corruption is widespread and affects all aspects of national life in Nigeria, positive results may still be achieved where the will exists to protect personal privacy. As well, illiteracy and poverty may be reduced where steps are taken to educate poor and illiterate in society about the potential risks to their health information when they subscribe to mHealth.

Overall, this thesis recommends the adoption of the EU regime as a conceptual framework for mHealth regulation in Nigeria. The thesis has suggested that it is potentially beneficial to combine the two pieces of legislation under the EU regime - *European Union Data Protection Directive 95/46/EC* and the *Directive on privacy and electronic communications, 2002/58/EC*- into a single privacy framework for Nigeria. This combination is useful both to cater for the perceived gap in one for the other and to specifically cater for protection for location data generated in mHealth. However, future research may provide better guidance on how both pieces of legislation may be effectively combined to create a workable privacy framework for mHealth.

It is also hoped that this thesis would encourage efforts to understand the roles which socio-economic issues such as corruption and poverty, identified in this thesis, play in any consideration of legal reform especially in developing country contexts such as Nigeria. It is my

view that more research in this area will assist in developing sound regulatory regimes which measure with international standards for protection of health information in novel systems such as mHealth but, most importantly promote the privacy of health information of users in those countries.

BIBLIOGRAPHY

LEGISLATION

Alberta, *Health Information Act*, 2000.

Federal High Court (Civil Procedure) Rules 2009.

Constitution of the Federal Republic of Nigeria (Promulgation) 1999 No. 24, s 37.

Data Protection Act 1998 (UK), c 29.

EC, Commission 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 information and the free movement of such data, [1995] OJL 281/31.

EC, *Commission Directive 2002/58/EC of 31 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, [2002] OJ, L 201.

Manitoba, *Personal Health Information Act*, 1997.

Medical and Dental Practitioners Act [cap M8] Laws of the Federal Republic of Nigeria 2004, Code of Medical Ethics.

Nigerian Communications Commission Act, Consumer Code of Practice Regulations 2007

Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011.

Personal Health Information Protection Act, 2004, c 3.

Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

Republic of South Africa, *Protection of Personal Information Act*, 2013

Saskatchewan, *Health Information Protection Act, 2003*.

The Nigerian Communications Commission Act, 2003.

JURISPRUDENCE

Ajayi v AG Federation, (1982) NCLR 915.

Attorney General v Guardian Newspapers Ltd (1988) [1990] 1 AC 109.

Commission v Hungary, C-288/12, [2014] ECR.

Dagg v Canada (Minister of Finance), [1997] 2 SCR 403.

Durant v. Financial Services Authority, Case No: B2/2002/2636.

Jones v Tsige 2012 ONCA 32.

Katz v United States, 389 US 347 (1967).

McInerney v *Macdonald* [1992] 2 SCR 138.

Medical and Dental Practitioners Disciplinary Tribunal v Okonkwo, [2001] 7 NWLR (Pt 711) 206.

R v Dyment, [1988] 2 SCR 417.

R v Tessling [2004] 3 SCR 432.

Ransome-Kuti v Attorney General of the Federation & Ors, [1981] 2 NWLR (Pt 6) 211.

S Olawoyin v Att-Gen Northern Region of Nigeria, (1961) 1 All NLR. 269.

Schloendorff v Society of New York Hospital, 211 NY 125, 105 NE 92 (1914).

Shugaba Darman v. Minister for Internal Affairs, (1981) 2 NCLR 459

Sony Kahushiki Kaisha v Hahani & Co. Ltd FHC/L/35/81.

Whalen v Roe, 429 US 589 (1977).

SECONDARY MATERIAL: MONOGRAPHS

Acquisti, Alessandro et al, eds. *Digital Privacy: Theory, Technologies and Practices,* (New York; Auerbach Publications, 2008).

Arowolo, Dare. "The Effects of Western Civilization and Culture on Africa" (2010)1 Afro Asian Journal of Social Sciences

Beauchamp, Tom L & James F Childress. *Principles of Biomedical Ethics,* 4th ed (New York: Oxford University Press, 1994).

Bennett, Colin J & Charles D Raab. *The Governance of Privacy: Policy Instruments in Global Perspective* (Cambridge: MIT Press, 2006).

Bernal, Paul. *Internet Privacy Rights: Rights to Protect Autonomy* (London: Cambridge University Press, 2014.

Bhan, Anant, Mina Majd & Adebayo Adejumo. "Informed Consent in International Research: Perspectives from India, Iran and Nigeria" (2006) 3 Medical Ethics 36.

Canadian Institute of Health Research. *Secondary Use of Personal Information in Health Research: Case Studies* (Ontario: Public Works and Government Services Canada, 2002).

Cavoukian, Ann & Khaled El Emam. *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy* (Ontario: Information and Privacy Commissioner of Ontario, 2011).

Chen, Min et al. *Big Data: Related Technologies, Challenges and Future Prospects* (Cham: Springer, 2014).

Ezeome, ER & PA Marshall. "Informed Consent Practices in Nigeria" (2009) 9 Developing World Bioethics 138.

Falola, Toyin. *Culture and Customs of Nigeria* (Westport: Greenwood Press, 2001).

Gbadegesin, Segun. *African Philosophy: Traditional Yoruba Philosophy and Contemporary African Realities* (London: Peter Lang, 1991).

Gurtwirth, Serge. *Privacy and the Information Age* (Oxford: Rowman & Littlefield Publishers, 2002).

Gyekye, Kwame. *Tradition and Modernity - Philosophical Reflections on the African Experience* (Oxford: Oxford University Press, 1997).

Ho, Kendall. "Health in the Digital World: Transformational Trends" in Stefane M Kabene, ed, *Healthcare and the Effect of Technology: Developments, Challenges and Advancements* (Hershey: IGI Global, 2010).

Inness, Julie C. *Privacy, Intimacy and Isolation* (New York: Oxford University Press, 1992).

Kim, Uichol. *Individualism and Collectivism: A Psychological, Cultural and Ecological Analysis* (Copenhagen: NIAS Books, 1991).

Li, Xiaorong. *Ethics, Human Rights and Culture: Beyond Relativism and Universalism* (Basingstoke: Palgrave Macmillan, 2006).

Linton, Ralph. *The Cultural Background of Personality* (New York: Appleton-Century Co., 1945).

Mackenzie, Catriona & Natalie Stoljar, *Relational Autonomy: Feminist Perspectives on Autonomy, Agency, and the Social Self* (New York: Oxford University Press, 2000).

Mbiti, John. *African Religions and Philosophy* (Oxford: Heinemann, 1990).

Miles, Steven H. *The Hippocratic Oath and the Ethics of Medicine* (Oxford: Oxford University Press, 2005).

Mill, John Stuart. *Principles of Political Economy with Some of their Applications to Social Philosophy* (Toronto: University of Toronto Press, 1965).

Miller, Arthur R. *The Assault on Privacy*: *Computers, Databank and Dossiers* (Ann Arbor: University of Michigan Press, 1971).

Nass, Sharyl J, Laura A Levitt & Lawrence O Gostin, eds. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* (Washington DC: National Academies Press, 2009).

Newman, Abraham L. *Protectors of Privacy*: *Regulating Personal Data in the Global Economy* (London: Cornell University Press, 2008).

O' Brien, David. *Privacy, Law, and Public Policy* (New York: Praeger Publishers, 1979).

Raghunathan, Balaji. *The Complete Book of Data Anonymization: From Planning to Implementation* (Florida: CRC Press, 2013).

Ramose, Mogobe. *African Philosophy through Ubuntu* (Zimbabwe: Mond Books, 2002)

Rodney, Walter. *How Europe Underdeveloped Africa* (Nairobi: East African Educational Publishers, 1972).

Savin, Andrej. *EU Internet Law* (Massachusetts: Edward Elgar Publishing, 2013).

Smith, Daniel Jordan. *A Culture of Corruption: Everyday Deception and Popular Discontent in Nigeria* (Princeton: Princeton University Press, 2008).

Solove, Daniel J. *Understanding Privacy* (Cambridge: Harvard University Press, 2008).

Steers, Richard M, Carlos J Sanchez-Runde & Luciara Nardon. *Management Across Cultures: Challenges and Strategies* (Cambridge: Cambridge University Press, 2010).

The United States Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems. *Records, Computers and the Rights of Citizens* (Cambridge: MIT Press, 1973).

Wacks, Raymond. *Personal Information: Privacy and the Law* (Oxford: Clarendon Press, 1989).

—. *Privacy*, 1st ed (New York: New York University Press).

Waziri, Farida. *Corruption and Governance Challenges in Nigeria* (Lagos: Cleen Foundation, 2010).

Westin, Alan. *Privacy and Freedom,* Ist ed (New York: Atheneum Press, 1967).

SECONDARY MATERIAL: ARTICLES

Adesina, Ademola O et al. "Ensuring the security and privacy of information in mobile health-care communication systems" (2011) 107 South African Journal of Science.

Agbakoba, Joseph CA. "An Evaluation of Theophilus Okere's conception of the place of African Traditional Values in Contemporary African Societies" in J Obi Oguejiofor and Godfrey Igwebuike Onah,eds, *African Philosophy and the Hermeneutics of Culture: Essays in Honour of Theophilus Okere* (Piscataway: Transaction Publishers, 2007).

Alo, Ejikeme Nonso. "Independent Commissions in Anti-Corruption Fights: The Nigeria, Uganda and Botswana Examples, 2000-2007" (2014) 16 Journal of Sustainable Development in Africa 47.

Bailey, Jane. “Framed by Section 8: Constitutional Protection of Privacy in Canada” (2008) 50 Canadian Journal of Criminology and Criminal Justice 279.

Bakare, Adewale Stephen. “The crowding-out effects of corruption in Nigeria: An empirical study” (2011)2 Journal of Business Management and Economics 59.

Barrigar, Jennifer, Ian R Kerr & Jacquelyn Burkell. “Let’s not get psyched out of privacy: Reflections on withdrawing consent to the collection, use and disclosure of personal information” (2006)44 Can Bus L 54.

Beaney, William M. “The Right to Privacy and American Law” (1966) 31 Law and Contemporary Problems. 253.

Bygrave, Lee. “The Place of Privacy in Data Protection Law” (2001) 24 UNSWLJ 277 at 280.

Fried, Charles. “Privacy” (1968) 77 Yale LJ 475.

Fritsch, Lothar. “Profiling and Location-Based Services (LBS)” in M. Hildebrandt and S. Gutwirth, eds, *Profiling the European Citizen: Cross-Disciplinary Perspectives* (New York: Springer, 2008)147.

Gavison, Ruth. “Privacy and the Limits of Law” (1980) 89 Yale LJ 421.

Gormley, Ken. “One Hundred Years of Privacy” (1992) Wisconsin Law Review 1335.

Gostin, Lawrence O & James G Hodge, Jr. “The "Names Debate": The Case for National HIV Reporting in the United States” (1998) 61 Alb L Rev 679.

Greenleaf, Graham. “The influence of European Data Privacy Standards outside Europe: Implications for globalization of Convention 108” (2012) 2 International Data Privacy Law 68.

Gutkind, Peter C W. “The African Urban Milieu: A Force in Rapid Change” (1962)12 Civilizations 167

Harman, Laurinda B, Cathy A Flite & Kesa Bond. “Electronic Health Records: Privacy, Confidentiality, and Security” (2012) 14 American Medical Association Journal of Ethics 712.

Hofstede, Geert “The cultural relativity of organizational practices and theories” (pre-1986)14 Journal of International Business Studies 75.

Isabona, Joseph. “Harnessing Telecommunications Revolution in Nigeria: A Case Study” (2013) 1 Wireless and Mobile Technologies 20.

Jones, Chris. “The utilitarian argument for medical confidentiality: a pilot study of patients’ views” (2003) 29 Journal of Medical Ethics.

Kamwangamalu, Nkonko M. "Ubuntu in South Africa: a sociolinguistic perspective to a pan-African concept" (1999)13 Critical Arts: South-North Cultural and Media Studies 24.

Kirby, Michael D. "Transborder Data Flows and the 'Basic Rules' of Data Privacy"(1980)16 Stan J Int'l L 29, cited in Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States,*(New York: Cornell University Press,1992.

Krouse, Alex. "iPads, iPhones, Androids and Smartphones: FDA Regulation of Mobile Phone Applications as Medical Devices" (2012)9 Indiana Health Law Review 731.

Letseka, Moeketsi. "African philosophy and educational discourse", in Phillip Higgs et al, eds, *African Voices in Education* (Juta Academic: Cape Town, 2000).

Milberg, Sandra J, Jeff Smith & Sandra J Burke. "Information Privacy: Corporate Management and National Regulation" (2000) 11 Organization Science 35.

Milberg, Sandra J et al. "Values, personal information privacy, and regulatory approaches" (1995)38 Communications of the ACM 65.

Mohammed, Usman. "Corruption in Nigeria: A challenge to sustainable development" (2013) 9 European Scientific Journal 118.

Moore, Adam. "Defining Privacy" (2008) 39 Journal of Social Philosophy 411.

Moskop, John C et al. "From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine-Part: 1 Conceptual, Moral, and Legal Foundations" (2005) 45 Annals of Emergency Medicine 53.

Narasimhan, Krishnan. "Text Message Appointment Reminders" (2013) 88 American Family Physician.

Ndebele, Paul, Joseph Mfutso-Bengo & Francis Masiye. "HIV/Aids reduces the relevance of the principle of individual medical confidentiality among the Bantu people of Southern Africa" (2008) 29 Theoretical Medicine and Bioethics 331.

Ndulo, Muna. "African Customary Law, Customs, and Women's Rights" (2011) 18 Ind J Global Legal Stud 87.

Onyemelukwe, Cheluchi. "Regulating Research Involving Humans in Nigeria: Some Recent Improvements" (2008) 16 Health Law Review 36.

Powers, Madison. "Privacy and the Control of Genetic Information "in Mark S Frankel & Albert Teich, eds, *The Genetic Frontier: Ethics, Law and Policy* (Washington DC: American Association for the Advancement of Science, 1994).

Post, Robert. “Three Concepts of Privacy” (2001) 89 Geo LJ 2087.

—. “The Social Foundations of Privacy: Community and Self in the Common Law Tort” (1989) 77 Cal L Rev 957.

Prosser, William L. “Privacy [A Legal Analysis]” in Ferdinand David Schoeman, ed, *Philosophical Dimensions of Privacy* (Cambridge: Cambridge University Press, 1984)104.

Rachels, James. “Why Privacy is Important” (1975) 4 Philosophy and Public Affairs at 323.

Rexler, Jonah. “Beyond the Oil Curse: Shell, State Power, and Environmental Regulation in the Niger Delta” (2010) 12 Stanford Journal of International Relations 26.

Roessler, Beate & Dorota Mokrosinska. “Privacy and social interaction” (2013) 39 Philosophy and Social Criticism 771.

Roos, Anneliese. “Core principles of data protection law"(2006) 39 The Comparative and International Law of Southern Africa 102.

Rubinstein, Ira S. “Regulating Privacy by Design” (2011) 26 Berkeley Law Journal 1409.

Salawu, B. “Ethno-Religious Conflicts in Nigeria: Causal Analysis and Proposals for New Management Strategies” (2010) 13 European Journal of Social Sciences 345.

Sieber, Ulrich. “Legal Order in a Global World– The Development of a Fragmented System of National, International, and Private Norms” (2010) 14 Max Planck Yearbook of United Nations Law 4.

Smedinghoff, Thomas J. “The New Law of Information Security: What Companies Need to Do Now”(2005) 22 Computer & Internet Lawyer Journal 9.

Solove, Daniel J “A Taxonomy of Privacy” (2006) 154 U Pa L Rev 477.

—. “Privacy and Power: Computer Databases and Metaphors for Information Privacy” (2001)53 Stan L Rev 1393.

Taiwo, Oseni. “Power and Womanhood in Africa: An Introductory Evaluation” (2010) 3 Journal of Pan African Studies 229.

Tavani, Herman. “Privacy and the Internet” in Madeleine Plascenscia & Paul Finkelman, eds., *Privacy and the Constitution* (New York: Routledge, 1999).

—. “Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy” (2007)38 Metaphilosophy.

Turn, Rein & Willis Ware. “Privacy and Security Issues in Information Systems”,online: Rand <http://www.rand.org/pubs/papers/P5684.html>.

Westin, Alan F. “Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy” (1966) 66 Colum L Rev 1003.

Winston, Morton E. "AIDS, Confidentiality and the right to know" (1988) 2 Public Affairs Quarterly 99.

INTERNET SOURCES

"Abdur Chowdhury's email", online: <http://sifaka.cs.uiuc.edu/xshen/aol/20060803_SIGIRListEmail.txt>.See also Michael Arrington,"AOL Proudly Releases Massive Amounts of Private Data", online: TechCrunch <http://techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/ >.

"A Consumer Privacy Bill of Rights, Part I"(Dec 25, 2013),TheSpiderOak Blog <*https://spideroak.com/privacypost/cloud-security/consumer-privacy-rights-part-i-protection-of-user-data-on-mobile-apps/* >.

Action Health Incorporated. "Insights into Early Marriage and Girls' education in Northern Nigeria"online:Action Health Incorporated < http://www.ungei.org/files/innovators.pdf>.

Adepoju, Paul. "Doctors warn against uncertified health tips", *Health News NG* (22 January 2014) online: Health News NG<http://www.healthnewsng.com/2014/01/nigerian-doctors-warn-against.html>.

Ajaegbu, Okechukwu. "Perceived Challenges of Using Maternal Healthcare Services in Nigeria" (23 May 2013), online: Aston Journals < http://astonjournals.com/manuscripts/Vol2013/ASSJ-65_Vol2013.pdf>.

Aker, Jenny C & Isaac M Mbiti. "Mobile Phones and Economic Development in Africa", online :(2010) 24 Journal of Economic Perspectives 3< https://www.aeaweb.org/articles.php?doi=10.1257/jep.24.3.207 >.

Akinbajo, Idris. "The Massive MDG Fraud: How the Health Ministry Steals From The Sick and Dying",*SaharaReporters*(20 July 2012) online: Sahara Reporters <http://saharareporters.com/2012/07/20/massive-mdg-fraud-how-health-ministry-steals-sick-and-dying-premium-times >.

Albrecht, Jan Philipp. "EU General Data Protection Regulation State of play and 10 main issues"(7January2015),online:Janalbrecht<http://www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf>.

Alubo, O et al, "Acceptance and stigmatization of PLWA in Nigeria", online: Taylor and Francis <http://www.ncbi.nlm.nih.gov/pubmed/11798411>.

American College of Physicians, *Ehealth and its impact on medical practice*, online: American College of Physicians http://www.acponline.org/advocacy/current_policy_papers/assets/ehealth.pdf>.

Amzat, Ajibola. “How Telecom Firms Cheat, Frustrate Subscribers”, *The Guardian* (22 December 2014)online: The Guardian http://www.ngrguardiannews.com/lead-story/191314-how-telecoms-firms-cheat-frustrate-subscribers>.

An analysis of Mobile Technology in West Africa: The Case of Nigeria, Ghana and Cote D’Ivoire”online: research ihub < http://research.ihub.co.ke/uploads/2012/october/1351001605_819_249.pdf >.

Appari, Ajit & M Eric Johnson. “Information Security and Privacy in Healthcare: Current State of Research”, online: Institute for Security Technology Studies <http://www.ists.dartmouth.edu/library/416.pdf>.

Aransiola, Joshua Oyeniyi, Akanni Ibukun Akinyemi & Adesegun Olayiwola Fatusi. “Women’s perceptions and reflections of male partners and couple dynamics in family planning adoption in selected urban slums in Nigeria: a qualitative exploration”, online:(2014) 14 BMC Public Health at 2 <http://www.biomedcentral.com/content/pdf/1471-2458-14-869.pdf>.

“Archbishop Desmond Tutu on Ubuntu”, online: Tutu Foundation <http://www.tutufoundationuk.org/ubuntu.php>.

Article 29 Working Party. “Advice paper on special categories of data (“sensitive data”), online: EuropeanCommission<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf>.

—. “Opinion 15/2011 on the definition of consent” (13 July 2011), online: European Union< http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf>.

Ball, James. “NSA collects millions of text messages daily in 'untargeted' global sweep” *The Guardian* (16 January 2014), online: The Guardian< http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep>.

Bamgboye, Ayo. “Ondo State use Mobile phones to Improve Maternal and Child Health”, *Africa Health IT News* (11 July 2012) online: Africa Health IT News <http://africahealthitnews.com/blogs/2012/07/ondo-state-use-mobile-phones-to-improve-in-maternal-and-child-health/>.

Barbaro, Michael & Tom Zeller. “A Face Is Exposed for AOL Searcher No. 4417749”, *New York Times* (August 9, 2006) online: New York Times < http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all&_r=2&>.

Bennett, Colin J. “Privacy in the Political System: Perspectives from Political Science and Economics”, online: Colin Bennett < http://www.colinbennett.ca/wp-content/uploads/2012/06/Privacyin-the-Political-System.pdf>.

—. “What Government Should Know about Privacy: A Foundation Paper”, online: Colin Bennett <http://www.colinbennett.ca/wp-content/uploads/2012/06/What-Government-Should-Know-about-Privacy.pdf>.

Blanc, Ann K et al. “Myths and misinformation: An analysis of text messages sent to a sexual and reproductive health Q&A service in Nigeria”, online: Population Association of America < http://paa2014.princeton.edu/papers/141862>.

“Brain Drain: Read How Nigeria Turned a Manufacture[r] for Medical Doctors Production”, (17 November 2013) online: Informed Minds Blog< http://www.naij.com/47348.html>.

Bridge, Sarah. “Canadians with mental illnesses denied U.S. entry: Data entered into national police database accessible to American authorities: WikiLeaks”, *CBC News* (9 September 2010) online:CBC News<http://www.cbc.ca/news/canada/canadians-with-mental-illnesses-denied-u-s-entry-1.1034903>.

Brouwer, Emmaline. “Clinical trials in developing countries” online: Global Medicine <http://globalmedicine.nl/issues/issue-5/clinical-trials-in-developing-countries-2/>.

“Building Foundations for eHealth, Progress of Member States: Report of the Global Observatory for eHealth”, online: World Health Organization <http://www.who.int/goe/publications/bf_FINAL.pdf>.

Canada Health Infoway. “Mobile Health Computing between Clinicians and Patients”, online: Canada Health <https://www.infoway-inforoute.ca/index.php/resources/technical-documents/emerging-technologynfoway>.

Canadian Radio-television and Telecommunications Commission. “Telecom Decision CRTC 2003-33”, online: CRTC < http://www.crtc.gc.ca/eng/archive/2003/dt2003-33.htm>.

Cate, Fred, Peter Cullen &Viktor Mayer-Schönberger. “Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines”, online: Oxford Internet Institute<www.oii.ox.ac.uk/.../Data_Protection_Principles_for_the_21st_Century.pdf>.

Cavoukian, Ann. “Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices”, online: Office of Information and Privacy Commissioner of Ontario < https://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf>.

Centre for Devices and Radiological Health. *Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff,* (9 February 2015) online: U.S. Department of Health and Human Services Food and Drug Administration<http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf>.

Chi, Benjamin H & Jeffrey SA Stringer. “Mobile phones to improve HIV treatment adherence”, online :(2010)376:9755TheLancet < http://www.sciencedirect.com/science/article/pii/S0140673610620466>.

Chiejina, Nduka. "CBN recovers N8.6b for bank customer",*The Nation* (16 April 2013) online: The Nation http://thenationonlineng.net/new/cbn-recovers-n8-6b-for-bank-customers/>.

Chimton, Ngala Kilian. "New mHealth project helps save lives in Cameroon" online: SciDev <http://www.scidev.net/sub-saharan-africa/icts/news/mHealth-project-helps-save-lives.html>.

Clarke, Roger. "The OECD Data Protection Guidelines: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law", online: Roger Clarke <http://www.rogerclarke.com/DV/PaperOECD.html>.

Clinton Foundation, News Release. "The Government of Nigeria Launches "Saving One Million Lives" with support from CHAI" (17 October 2012) online: Clinton Foundation https://www.clintonfoundation.org/main/clinton-foundation-blog.html/2012/10/17/the-government-of-nigeria-launches-saving-one-million-lives-with-support-from-chai>.

"Colleen Stamp found guilty of illegally accessing patient records" *CBCNews* (30 September 2014) online: CBCNews<http://www.cbc.ca/news/canada/newfoundland-labrador/colleen-stamp-found-guilty-of-illegally-accessing-patient-records-1.2782794>

"Consent: A separate privacy principle dealing with consent?" online: Australian Law Reform Commission <http://www.alrc.gov.au/publications/19.%20Consent/separate-privacy-principle-dealing-consent>.

Crowe, Anna. "The promise, and problems, of mobile phones in the developing world"(1 November 2013)online: Open democracy< https://www.opendemocracy.net/opensecurity/anna-crowe/promise-and-problems-of-mobile-phones-in-developing-world>.

De´glisen, Carole et al. "SMS for disease control in developing countries: a systematic review of mobile health applications" online: Academia. Edu < http://www.academia.edu/2311064/SMS_for_disease_control_in_developing_countries_a_systematic_review_of_mobile_health_applications >.

Deloitte. *Sub-Saharan Africa Mobile Observatory 2012*, online: GSM Association <http://www.gsma.com/publicpolicy/wp-content/uploads/2013/01/gsma_ssamo_full_web_11_12-1.pdf>.

Diez-Canseco, Francisco et al. "Design and Multi-Country Validation of Text Messages for an mHealth Intervention for Primary Prevention of Progression to Hypertension in Latin America", online: (2015) 3:1 JMIR mHealth uHealth 19 < http://mHealth.jmir.org/article/viewFile/mHealth_v3i1e19/2>.

Dike, Victor "Corruption in Nigeria: A New Paradigm for Effective Control", online: African Economic Analysis<http://www.africaeconomicanalysis.org/articles/gen/corruptiondikehtm.html>.

Donovan, Kevin & Aaron Martin, "The Rise of African SIM registration: The emerging dynamics of regulatory change", online :(2014) First Monday 2 at para 3<http://firstmonday.org/ojs/index.php/fm/article/view/4351/3820>.

Ebuehi, Olufunke & Princess Campbell. "Attraction and retention of qualified health workers to rural areas in Nigeria: a case study of four LGAs in Ogun State, Nigeria", online :(2011)11:1 Rural and Remote Health 1515 < http://www.rrh.org.au/articles/subviewafro.asp?ArticleID=1515>.

EC, *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),* online: European Union Law < http://eur-lex.europa.eu/procedure/EN/201286>.

Ejiofor, Blessing. "A message for maternal and child health", online: UNICEF <http://www.unicef.org/nigeria/media_8457.html>.

Electronic Privacy Information Centre and Privacy International (PI), "Overview of Privacy" in Privacy and Human Rights Report, online: WORLDLII <http://www.worldlii.org/int/journals/EPICPrivHR/2006/>.

Elele, Chinyere. "Nigeria: Male Child Remains a Family Pride and Honour", *Inter Press Service* (29 May 2002) online: Inter Press Service <http://www.sos-sexisme.org/english/male_child.htm>.

Epocrates, online: Epocrates < http://www.epocrates.com/products>.

Essien, Anthonia M & Donatus P Ukpong. "Patriarchy and Gender Inequality: The Persistence of Religious and Cultural Prejudice in Contemporary Akwa Ibom State, Nigeria", online :(2012) 2 International Journal of Social Science and Humanity 4 < http://www.ijssh.org/show-31-406-1.html>.

Esionwu, Chris. "African Cultural Values"online: Academia.Edu <http://www.academia.edu/5015800/African_cultural_values>.

"Etisalat Mobile Baby"online: <http://www.ictet.org/downloads/Mob_ejtJpe_jfnJ.pdf >.

Eysenbach, G. "What is e-health?", online :(2001) Journal of Medical Internet Research<http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761894/>.

Fraser, Ross & Don Willison."Tools for De-Identification of Personal Health Information", online: Pan Canadian Health Information Privacy (HIP) Group <https://www.infoway-inforoute.ca/index.php/component/docman/doc_download/624-tools-for-de-identification-of-personal-health-information>.

"First Report of the Working Group on mHealth: m-Powering Development Initiative" (31 March 2014), online: International Telecommunication Union <http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Documents/mHealth_Report_of_the_Working_Group.pdf>.

Geeking with Greg, "A chance to play with big data", online: Glinden BlogSpot <http://glinden.blogspot.ca/2006/08/chance-to-play-with-big-data.html>.

Gold, Judy et al. "What's in a message? Delivering sexual health promotion to young people in Australia via text messaging", online :(2010)10:792 BMC Public Health <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3022861/>.

Goldman, Jeff. "Stolen Computers, Mobile Phones Expose Thousands of Patients' Medical Data" (3 February 2015), online: eSecurityPlanet<http://www.esecurityplanet.com/network-security/stolen-computers-mobile-phones-expose-thousands-of-patients-medical-data.html>.

"Green Paper on Mobile Health ("mHealth")" (10 April 2014), online: European Commission<http://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mHealth>.

GSMA Mobile for Development."mHealth Country Feasibility Report: Nigeria", online: GSM Associationhttp://nigeria.gsmamHealthfeasibility.com/GSMA_Country_Feasibility_Report_Nigeria_2014.pdf >.

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1981, online: Organization for Economic Co-operation and Development< http://www.oecd.org/>/ .

Health Privacy Project, "Health Privacy Stories",online: Center for Democracy and Technology https://www.cdt.org/files/healthprivacy/20080311stories.pdf.

Hersh, William. "A stimulus to define informatics and health information technology", online :(2009) BMC Medical Informatics and Decision Making <http://www.biomedcentral.com/1472-6947/9/24>.

"Human Resources for Health: Country Profile", online: United Nations Population Fund<http://www.unfpa.org/sowmy/resources/docs/library/R050_AHWO_2008_Nigeria_HRHProfile.pdf>.

"ICT4SOML: Leveraging ICTs to Save the Lives of One Million Women and Children in Nigeria"(11 February 2013),online: Health Level Seven <http://wiki.hl7.org/images/5/5c/SOML_Situational_Analysis_FINAL_20130909.pdf>.

Idoko, Clement. "Literacy level in Nigeria now 62% —FG", *Nigerian Tribune* (5 August 2014) online: Nigerian Tribune <http://www.tribune.com.ng/news/news-headlines/item/12566-literacy-level-in-nigeria-now-62-fg/12566-literacy-level-in-nigeria-now-62-fg>.

"Impact of Political Interference on Aviation Devt in Nigeria", *This Day Newspapers* (22 March 2013) online: This Day<http://www.thisdaylive.com/articles/impact-of-political-interference-on-aviation-devt-in-nigeria/142837/>.

"iTunes Preview", online: Apple Itunes <http://itunes.apple.com/us/app/istethoscopepro/id322110006?mt=8# >.

Izugbara, Dr C Otutubikey. "Patriarchal Ideology and Discourses of Sexuality in Nigeria", online: African Regional Sexuality Resource Centre <http://www.arsrc.org/downloads/uhsss/izugbara.pdf>.

James, Jeffrey & Mila Versteeg. "Mobile phones in Africa: how much do we really know?", online: (2007)84 Social Indicators Research <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2806217/>.

Kahn, James G, Joshua S Yang & James S Kahn. "Mobile' Health Needs And Opportunities In Developing Countries", online: (2010)29:2 Health Affairs < https://www.k4health.org/sites/default/files/Kahn,%20Yang,%20Kahn%20Mobile%20Health%20Needs%20and%20Opportunities%20in%20Developing%20Countries.pdf>.

Kalil, Imam Hassan. *Wife Obedience to Husband in Islam,* online: MyDeenIsIslam <http://www.mydeenislam.com/wife-obedience-to-husband-in-islam.html>.

Kambarami, Maureen. "Femininity, Sexuality and Culture: Patriarchy and Female Subordination in Zimbabwe", online: African Regional Sexuality Resource Centre<http://www.arsrc.org/downloads/uhsss/kmabarami.pdf>.
Kasa, Sjur. "Industrial Revolutions and Environmental Problems", online: Confluence<http://www.cas.uio.no/Publications/Seminar/Confluence_Kasa.pdf>.

Kayode, Asaju, Sunday Onah Adagba & Silas Felix Anyio. "Corruption and service delivery: the case of Nigerian public service", online :(2013) 1 Wudpecker Journal of Public Administration< http://www.wudpeckerresearchjournals.org/WJPA/pdf/2013/July/Kayode%20et%20al.pdf>.

"Key Malaria Facts", online: Roll Back Malaria<http://www.rbm.who.int/keyfacts.html>.

Kluge, Eike-Henner W. "Informed Consent to the Secondary Use of EHRs: Informatic rights and their limitations", online: (2004) 107 Studies in Health Technology and Informatics http://www.cs.mun.ca/~harold/Courses/Old/CS6772.F04/Diary/4115Kluge.pdf .

KPMG Services."Nigeria: Country Profile", online: KPMG Services <http://www.kpmg.com/Africa/en/KPMG-in-Africa/Documents/NIgeria.pdf>.

Kwankap, Yunkap. "eHealth in developing countries: contemporary issues, challenges and opportunities for hospitals", online: Africa Health <http://www.africa-health.com/articles/march_2011/13.%20Yunkap%20opinion.pdf>.

Labeodan, Morire OreOluwapo "The Family Lifestyle in Nigeria", online: Princeton<http://paa2005.princeton.edu/papers/51248>.

Labrique, Alain. "Opportunities and Challenges for mHealth Strategies in Resource-Limited Settings"(4 September 2012) (Youtube) online: Johns Hopkins University

< http://www.jhumHealth.org/content/alain-labrique-director-gmi-and-assistant-professor-jhsph-discusses-opportunities-and >.

Landman, Adam et al. "A mobile app for securely capturing and transferring clinical images to the electronic health record: description and preliminary usability study", online: JMIR Publications < http://mHealth.jmir.org/2015/1/e1/>.

Leitch, Kellie et al. "Leveraging Information Technologies To Transform and Sustain British Columbia's Health Care Sector", online: Centre for Health Innovation and Leadership <http://sites.ivey.ca/healthinnovation/files/2010/10/BC-White-Paper-Final.pdf>.

Lemaire, Jeanine."Scaling up Mobile Health: Elements for the successful Scale-Up of mHealth in Developing Countries", online: K4Health <https://www.k4health.org/sites/default/files/ADA_mHealth%20White%20Paper.pdf>.

Lester, Richard T et al. "Effects of a mobile phone short message service on antiretroviral treatment adherence in Kenya (WelTel Kenya1): a randomized trial", online: (2010) The Lancet <http://www.pepfar.gov/documents/organization/161268.pdf>.

Lewis, Trevor *et al*."E-health in low- and middle-income countries: findings from the Center for Health Market Innovations", online: World Health Organization <http://www.who.int/bulletin/volumes/90/5/11-099820/en/>.

Locke,John. *Second Treatise of Government,*1690 at 6 cited in digitized form by David Gowan, "Second Treatise of Government by John Locke "online: Oregon state < http://oregonstate.edu/instruct/phl302/texts/locke/locke2/locke2nd-a.html>.

Macdonald, Ian."The Counsel of Elders", online: South Africa the Good News < http://www.sagoodnews.co.za/newsletters/773-the-counsel-of-elders.html>.

Mairiga, Abdulkarim et al."Sociocultural factors influencing decision-making related to fertility among the Kanuri tribe of north-eastern Nigeria" (2010) 2 African Journal of Primary Health Care & Family Medicine <http://www.phcfm.org/index.php/phcfm/article/view/94/85>.

McCann, Erin. "WHO credits mHealth app with helping Nigeria get rid of Ebola", *mHealth News* (24 October, 2014) online: mHealth News < http://www.mHealthnews.com/news/who-credits-mHealth-app-helping-nigeria-get-rid-ebola>.

Medical Business News. "What is eHealth?" cited in Hans Oh et al, "What Is eHealth (3): A Systematic Review of Published Definitions", Online: Journal of Medical Internet Research< https://tspace.library.utoronto.ca/html/1807/4733/jmir.html>.

"mHealth: New Horizons for Health through mobile technologies", online: World Health Organization <http://www.who.int/goe/publications/goe_mHealth_web.pdf>.

"Mobile Health and Fitness Apps: What Are the Privacy Risks?" online: Privacy Rights Clearing House < https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks>.

"Model Contracts for the transfer of personal data to third countries", online: European Union <http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm>.

MTN Nigeria. *Privacy policy*, online: MTNOnline<http://nextapps.mtnonline.com/index/page/id/24>.

Mxokoheli, Sive. "Controversies of gender and sexuality, heteronormativity and homosexuality in African contexts "online: Academia.edu <http://www.academia.edu/8753580/Controversies_of_gender_and_sexuality_heteronormativity_and_homosexuality_in_African_contexts>.

"New Public- Private Initiative Leverages Mobile Technologies to Save One Million Lives in Nigeria" (3 December 2012),online:UN Foundation <http://www.unfoundation.org/news-and-media/press-releases/2012/new-public-prive-partnership-mHealthalliance.html>.

Ndukwe, Ernest. "Country Experience in Telecom Market Reforms-Nigeria", online: Nigerian CommunicationsCommission<http://www.ncc.gov.ng/archive/speeches_presentations/EVC's%20Presentation/Country%20Experience%20with%20Market%20Reforms%20in%20Telecoms%20%20-%20060705..pdf>.

Nigerian Communications Commission. "Subscriber Statistics", online: Nigerian CommunicationsCommission<http://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125&Itemid=73>.

---. *Monthly Subscriber Day (May 2013-April 2014),* online: Nigerian CommunicationsCommissionhttp://www.ncc.gov.ng/index.php?option=com_content&view=article&id=125&Itemid=73.

"Nigerian Culture", online: Government of Nigeria, http://www.nigeria.gov.ng/2012-10-29-11-05-46/2012-11-05-09-51-17

"Nigerians living in poverty rise to nearly 61%", *BBC News Africa* (13 February 2012) online: BBC News<http://www.bbc.com/news/world-africa-17015873>.

Occupational Health and Safety Agency for Healthcare in British Columbia. "Technological Innovations in Occupational Health and Safety in the Healthcare Industry" online: Oregon Coalition for Healthcare Ergonomics <http://www.hcergo.org/136-id-technologicalinnovationsreport.pdf>.

Ogbebulu, Benjamin. "The Sorry State Of Nigeria's Health Sector and the Agitation For A 21st Century Comprehensive Health Care Delivery System In Nigeria", online: Gamji<http://www.gamji.com/article6000/NEWS7105.htm>.

Ogundele, Solomon O. "Unbridled bribery and corruption in the Nigerian communications commission (NCC): Dr. Hamadoun Touré, Secretary-General of ITU, guilty by association", Letter to the Editor, *Sahara Reporters* (16 March 2010)

<http://saharareporters.com/2010/03/16/unbridled-bribery-and-corruption-nigerian-communications-commission-ncc-dr-hhamadoun>.

Okuboyejo, Senanu & Omatseyin Eyesan. "mHealth: Using Mobile Technology to Support Healthcare", online :(2014) Journal of Public Health and Informatics 5 < http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3959917/pdf/ojphi-05-e233.pdf>.

Olupohunda, Bayo. "The burden of illiteracy in Nigeria", *Punch Newspapers* (24 September 2012) online :< http://www.punchng.com/opinion/the-burden-of-illiteracy-in-nigeria/ >.

One World, "Learning about Living – Using cross-media technology to empower young people with reproductive health and life skills"online: OneWorld< http://oneworld.org/2014/08/21/learning-about-living-using-cross-media-technology-to-empower-young-people-with-reproductive-health-and-life-skills/> .

Onukwube, Bonnie. "Why SIM Card Registration Exercise Needs to Succeed", *Daily Trust* (25 June 2012) online: allafrica.com<http://allafrica.com/stories/201206250697.html>.

Onwuemele, Andrew. "Impact of Mobile Phones on Rural Livelihoods Assets in Rural Nigeria: A Case study of Ovia North East Local Government Area "online :(2011)9:2 African Journals Online <http://www.transcampus.org/JORINDV9Dec2011/Jorind%20Vol9%20No2%20Dec%20Chapter30.pdf>.

Otieno, Gabriel et al."The feasibility, patterns of use and acceptability of using mobile phone text messaging to improve treatment adherence and post-treatment review of children with uncomplicated malaria in western Kenya"(2014) 13:44 Malaria Journal < http://www.malariajournal.com/content/pdf/1475-2875-13-44.pdf>.

Oyedele, Damilola. "Nigeria Accounts for 13% Global Maternal Mortality Rates", *This Day* (12 July 2014) online: This Day <http://www.thisdaylive.com/articles/nigeria-accounts-for-13-global-maternal-mortality-rates/183394/>.

Oyediran, Kola A & Ayodele F Odusola. "Poverty and the Dynamics of Women's Participation in Household Decision-Making in Nigeria", online :(2004)19 African Population Studies<http://www.bioline.org.br/pdf?ep04023>.

Pai, Aditi. "23 health and wellness apps that connect to Apple's Health Kit",online:Mobi Health News <http://mobihealthnews.com/36870/23-health-and-wellness-apps-that-connect-to-apples-healthkit/ >.

Parliamentary Monitoring Group (PMG), "Protection of Personal Information Bill [B9-2009] briefing"(6 October 2009)online: Parliamentary Monitoring Group <http://www.pmg.org.za/report/20091006-protection-personal-information-bill-b9-2009-briefing>.

Pear, Robert."Tighter Medical Privacy Rules Sought"*The New York Times* (22 August 2010)online:The New York Times <http://www.nytimes.com/2010/08/23/health/policy/23privacy.html?_r=0>.

"PF using details of SIM registration to campaign, distributing cash", *Zambian Watchdog* (20 February 2013) online: Zambian Watchdog <https://www.zambianwatchdog.com/pf-using-details-of-sin-registrion-to-campaign/>.

"PIPEDA Report of Findings #2014-001:Report of Findings Use of sensitive health information for targeting of Google ads raises privacy concerns", online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/cf-dc/2014/2014_001_0114_e.asp>.

"Pocket Guide to South Africa 2011/12: South Africa's People"online: Government of South Africa<http://www.gcis.gov.za/sites/default/files/docs/resourcecentre/pocketguide/004_saspeople.pdf>.

Podesta,John. "Findings of the Big Data and Privacy Working Group Review (1 May 2014) online: The White House Blog <http://www.whitehouse.gov/blog/2014/05/01/findings-big-data-and-privacy-working-group-review>.

Pritts, Joy L." The Importance and Value of Protecting the Privacy of Health Information: The Roles of the HIPAA Privacy Rule and the Common Rule in Health Research" online: Institute of Medicine <http://www.iom.edu/~/media/Files/Activity%20Files/Research/HIPAAandResearch/PrittsPrivacyFinalDraftweb.pdf>.

Pyramid Research.*The Impact of Mobile Services in Nigeria: How Mobile Technologies are Transforming Economic and Social Activities,* online: Pyramid Research <http://www.pyramidresearch.com/documents/IMPACTofMobileServicesInNIGERIA.pdf >.

Raab, Charles D, et al. "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", online :European Commission <http://ec.europa.eu/justice/dataprotection/document/studies/files/19980901_adequacy_methodology_en.pdf>.

Ratti, Carlo, et al. "Mobile Landscapes: Using Location Data from Cell Phones for Urban Analysis"online:SENSEable<http://senseable.mit.edu/papers/pdf/RattiPulselliWilliamsFrenchman2005E&PB.pdf>.

"Religion in Nigeria" online: Wikipedia <http://en.wikipedia.org/wiki/Religion_in_Nigeria>.

Rozenberg, Norman. "Big data: Benefits, drawbacks in addressing Ebola" (20 August 2014) online: Tech Page One<http://techpageone.dell.com/technology/big-data-benefits-drawbacks-in-addressing ebola/#.VBwl1PldVps>.

Smith, Richard. "The future of medical education: speculation and possible implications", online: BMJ Talks<www.bmj.com/talks>.

"Special Report: A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector" (30 April 2014), online: Office of the Information and Privacy Commissioner for British Columbia <https://www.oipc.bc.ca/special-reports/1634>.

Stephens, Joe. "Panel Faults Pfizer in '96 Clinical Trial In Nigeria", *The Washington Post* (7 May 2006) online: The Washington Post<http://www.washingtonpost.com/wpdyn/content/article/2006/05/06/AR2006050601338.html>.

Striata, "POPI - to Act or not to Act? That is the question..." (2 March 2015),online:WebTech Forumhttp://www.itweb.co.za/index.php?option=com_content&view=article&id=141547:POPI-to-Act-or-not-to-Act-That-is-the-question-&catid=355#prcontacts.

Teyras, Kristel. "SMS innovation and dynamic mobile content drives mHealth initiatives in Africa",*Gemalto's Blog*(16July 2014)online:Gemalto.com<http://blog.gemalto.com/blog/2014/07/16/sms-innovation-and-dynamic-mobile-content-drives-mHealth-initiatives-in-africa/#sthash.ZfgwXzGp.dpuf>.

The Earth Institute Colombia University. "Barriers and Gaps Affecting mHealth in Low and Middle Income Countries: A Policy White Paper" (May 2010), online: mHealth Alliance < http://mHealthalliance.org/media-a-resources/publications>.

"The future of healthcare in Europe" *The Economist*, online: The Economist<http://www.economistinsights.com/sites/default/files/downloads/EIUJanssen_HealthcareAfrica_Report_Web.pdf >.

The Location Forum."Location Data Privacy: Guidelines, Assessments and Recommendations *"Privacy Association* (1 May 2013) online: Privacy Association <https://privacyassociation.org/media/pdf/resource_center/LocationDataPrivacyGuidelines_v2.pdf>.

The World Bank. "2012 Information and Communications Development: Maximizing Mobile", online:

TheWorldBank<http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/IC4D-2012-Report.pdf.>

"The World in 2014, ICT Facts and Figures", online:ICThttp://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf>.

Thien, Madeleine. "Freedom of Thought Requires Privacy, Not State Scrutiny", *Huffington Post* (23 December 2013) online: Huffington Post <http://www.huffingtonpost.ca/madeleine-thien/freedom-of-thought-requires-privacy_b_4495244.html>.

Thomas, Karl W, Charles S Dayton & Michael W Peterson. "Evaluation of Internet-Based Clinical Decision Support Systems", online:(1999)Journal of Medical Internet Research<http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761710/>.

"Traffic Data", online: UK Information Commissioner's Office < https://ico.org.uk/for-organisations/guide-to-pecr/traffic-data/>.

United Nations Foundation, "Assessing the Enabling Environment for ICTs for Health in Nigeria: A Landscape and Inventory", online: UN Foundation< http://www.unfoundation.org/assets/pdf/nigeria-landscape-report.pdf>.

USAID. *A DIV-funded start-up becomes a leading solution for mobile health,* online: USAIDhttp://www.usaid.gov/div/commcare>.

US Department of Commerce. "U.S. - EU Safe Harbor Framework A Guide to Self-Certification", Online: US Department of Commerce<http://trade.gov/media/publications/pdf/safeharbor-selfcert2009.pdf>.

"Vitalité Health refers doctor privacy breach to RCMP" *CBCNews* (23 September 2014)online: CBCNews <http://www.cbc.ca/news/canada/new-brunswick/vitalit%C3%A9-health-refers-doctor-privacy-breach-to-rcmp-1.2775290>.

Walczuch, Rita M, Snajay Singh & Todd Palmer, "An analysis of the cultural motivations for Transborder data flow legislation", online: ProQuest<http://search.proquest.com/docview/222414212/ED5A89FFD085437DPQ/3?accountid=10406>.

Walton, David J. "Big Data raises big legal issues As the laws and regulations within the United States evolve, companies must be extremely attentive", online: Inside Counsel<http://www.insidecounsel.com/2014/03/28/big-data-raises-big-legal-issues>.

"Where Profits and Lives Hang in Balance: Finding an Abundance of Subjects and Lack of Oversight Abroad, Big Drug Companies Test Offshore to Speed Products to Market", *The Washington Post* (17 December 2000)online: The Washington Post <http://www.washingtonpost.com/wpdyn/content/article/2007/07/02/AR2007070201255_pf.html>.

Whiting, Alex. "Middle-income countries leave their poorest behind – report" *Thomson Reuters Foundation* (7 December 2011), online: Thomson Reuters Foundation <http://www.trust.org/item/?map=middle-income-countries-leave-their-poorest-behind-report>.

"Women & Mobile: A Global Opportunity A study on the mobile phone gender gap in low and middle-income countries", online: GSMA<http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/01/GSMA_Women_and_Mobile-A_Global_Opportunity.pdf>.

"World Bank report on poverty in Nigeria", Editorial, *The Daily Independent* [nd] online: The Daily Independent<http://dailyindependentnig.com/2014/05/world-bank-report-poverty-nigeria/>.

World Health Organization. "mHealth: New Horizons for health through mobile technologies", online: World Health Organization<http://www.who.int/goe/publications/goe_mHealth_web.pdf>.

—. "Nigeria: Country Profile", online: World Health Organization <http://www.who.int/countries/nga/en/>.

—. *Legal Frameworks for eHealth: Based on the Findings of the Second Global Survey on eHealth,* online: Global Observatory for eHealth <http://www.who.int/goe/publications/ehealth_series_vol5/en/>.

Worldmark Encyclopedia of Nations. "Nigeria", online: <http://www.encyclopedia.com/topic/Nigeria.aspx>.

Wyatt, JC & JLY Liu. "Basic concepts in medical informatics", online: (2002) 56 Journal of Epidemiology and Community Health 11< http://jech.bmj.com/content/56/11/808.full>.

UNPUBLISHED THESIS

Matemba, Reyneck Thokozani. *Judicial Activism: Usurpation of Parliament's and Executive's legislature functions, or A Quest for Justice and Social Transformation* (LLM Thesis, Institute of Advanced Legal Studies,University of London, 2010) [Unpublished].

Singhatey, Peter Joseph. *Peacekeeping in Africa: The Vital Role of a Regional Hegemon* (M A Thesis, Dublin City University, 2008) [Unpublished].

INTERNATIONAL CONVENTIONS

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981.

OTHER MATERIALS

Asiyanbola, Abidemi R. "Patriarchy, male dominance, the role and women empowerment in Nigeria"(Paper delivered at the International Union for the Scientific study of Populations Conference, Tours, France,21 July 2005),[unpublished].

Brey, Philip, Frances Grodzinsky & Lucas Introna. *Western Privacy and Ubuntu: Influences in the forthcoming data privacy bill: Proceedings of the Sixth International Conference of Computer Ethics, Enschede,The Netherlands, 2005*.

Council of Europe. PA,3rd Sess,*Working Document on the processing of personal data relating to health in electronic health records (EHR*), (2007).

De Silva, Harsha & Ayesha Zainudeen, eds. *Teleuse on a Shoestring: Poverty Reduction Through Telecom Access at the 'Bottom of the Pyramid': Annual Symposium on Poverty Research for the Centre for Poverty Analysis, Colombo, 2007.*

EC, Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number (2000)2441), [2000] OJ,L215.

Kpamor, Dr Sipporah. " Nigeria's Health Statistics and Trends" (Presentation delivered at the Woodrow Wilson International Center for Scholars Environmental Change and Security Program, Global Health Initiative, 25 April 2012).

Motamarri, Saradhi et al. "mHealth, a better alternative for healthcare in developing countries" (Paper delivered at the Pacific Asia Conference on Information Systems (PACIS), Vietnam, July 2012), [Unpublished].

Recommendations To Identify and Combat Privacy Problems in the Commonwealth: Hearing on H.R. 351 Before the H. Select Comm. on Info. Sec., 2005 Gen. Assemb., 189th Sess. (Pa. 2005).

Showell, Chris & Christian Nohr. *How Should We Define eHealth, and Does the Definition Matter: Proceedings of the European Medical Informatics Conference, Pisa, 2012* (IOS Press, 2012).

The Bible New International Version (Colorado Springs: Biblica, 2011).

World Health Organization, WHA Res 58.28, WHO, 114th Sess, UN Doc A58/21 (2005) at 108.

WHO, 58th Sess, UN Doc WHA58/2005/REC/1 (2005).