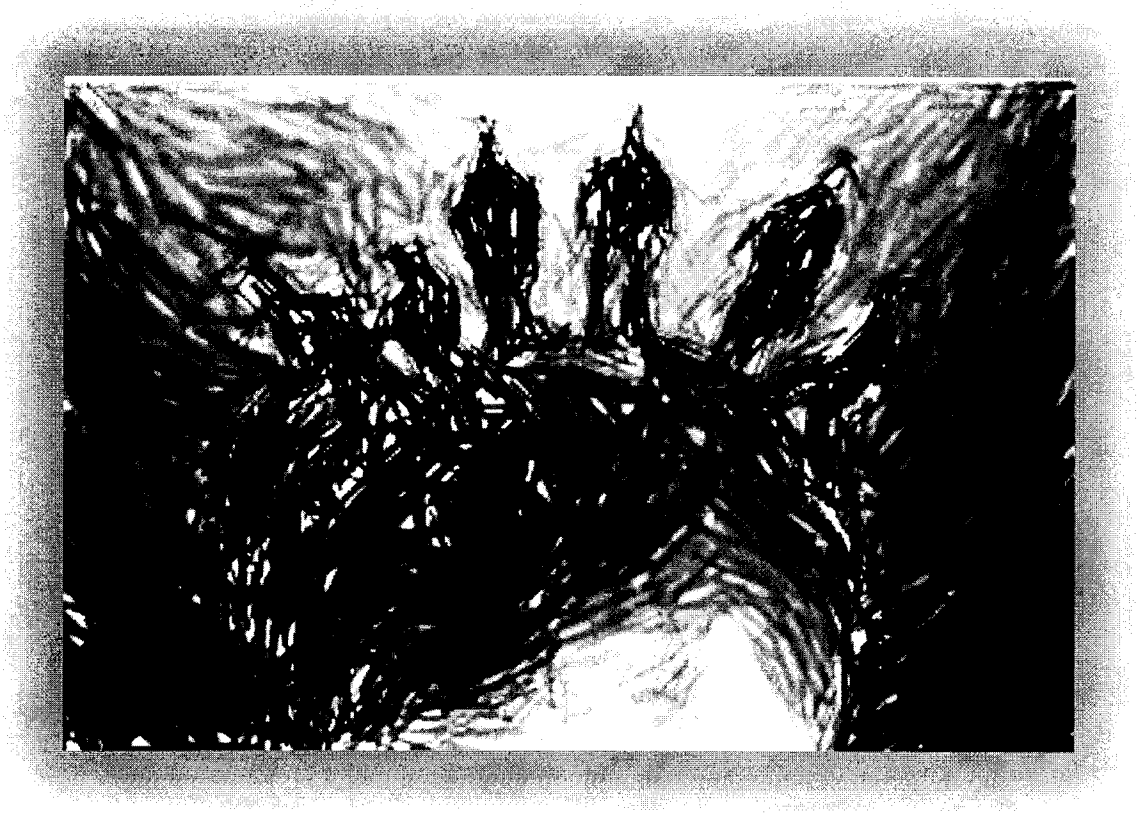
DATA PROTECTION AND MIGRATON:

BALANCING STATE INTERESTS AND INDIVIDUAL RIGHTS



Name: Ruzayda Martens

Student number: 521338

Supervisor: Jonathan Klaaren

DECLARATION

I, RUZAYDA MARTENS,

declare that this thesis is my own unaided work. It is submitted in fulfillment of the requirements of the degree of Master of Law by dissertation (LLM) in the Faculty of Commerce, Law and Management at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

SIGNATURE

521 338

STUDENT NUMBER

30 / 09 / 2014

DATE

DECLARATION

I, RUZAYDA MARTENS, declare that this dissertation is my own unaided work. It is submitted in the fulfilment of the requirements for the degree of Master of Laws by dissertation at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any other degree or examination in this or any other university.

Name: Ruzayda Martens

Student number: 521338

Date of Submission: 30 April 2014

ACKNOWLEDGEMENTS

Firstly, I would like to thank my husband, Jonathan Martens, for his patience, encouragement and continued support. Secondly, I would like to thank my mother, Latiefa Mansour, for teaching me the value of perseverance and hard work. Thirdly, I would like to thank my supervisor, Jonathan Klaaren, for his guidance and assistance. Last, but not least, I would like to thank the interviewees who informed my analysis of the key issues in this thesis.

Special appreciation is also due to the National Research Foundation (NRF) for the support received under the NRF grant "The Intersection of Rights and Regulation."

ABSTRACT

The globalization of irregular migration and its facilitation by transnational criminal groups, coupled with concerns of terrorism, has radically impacted the way in which States manage migration and national security. At the same time, the information age has placed the issue of privacy and confidentiality at the centre of public, legislative and media debates. While advanced technology facilitates migration management and data exchange, the emergent use of surveillance techniques to identify individuals and keep track of their movements is a growing concern. Advanced technology can help to protect and manage borders, but it can also threaten human rights and create vulnerabilities relating to data theft, data loss, inappropriate disclosure and misuse of personal data. In the absence of appropriate data protection safeguards, personal data can be used for reasons unrelated to its intended purpose, without the knowledge of the individuals concerned and contrary to their expectations. When applied to migrants, data protection has a cross-border dimension, and this gives rise to additional concerns related to unauthorized disclosure that could lead to a multitude of risks ranging from physical violence to profiling and discrimination.

This thesis seeks to outline the points of intersection between data protection and migration. In so doing, it points out the important consideration of the threat to human life and safety, a practical reality when collecting and processing personal data of vulnerable migrants. States have an obligation to protect the human rights afforded to all individuals, regardless of their nationality or immigration status. States also have the sovereign right to protect their borders and the duty to keep their citizens secure. While acknowledging the delicate exercise of having to balance between protecting State interests and respecting individual rights, this thesis emphasizes that the two are not mutually exclusive and it can be balanced, albeit a delicate balance. To ensure an appropriate balance, individual rights should not be diluted or subjugated by the interests of States. Instead any restrictions to privacy and data protection should be justified and proportional to the state interest. Further, the parameters for using advanced technology should be firmly embedded in the law. Finally, as technology is not infallible and cannot be seen in isolation, the human factor is a key consideration to take into account when developing and implementing the law governing the use of advanced technology that may impact on individual rights.

TABLE OF CONTENTS

8 Attachments:

Annexure A – Interview Questions

Annexure B – Key Terms Defined

Annexure C – Abbreviations

9 Bibliography

CHAPTER ONE

1. INTRODUCTION

> *'A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars.'*[1]

This introductory chapter outlines the purpose of this thesis which is to assess the legal framework for the protection of personal data in the context of migration.[2] To this end, it outlines the points of intersection between data protection and migration, introduces the use of advanced technology in migration management and humanitarian assistance, and highlights the consequent implication on privacy and other human rights. This thesis argues that although data protection stems from the right to privacy, it needs to be recognized as a separate right in light of advanced technology in the 21st century. Finally, by looking at the cross border dimension of migration and data protection from a regional perspective in Southern Africa and by examining the development of the data protection law and the criteria for balancing rights in the South Africa jurisprudence, it explores the line between State sovereignty and individual rights with the view to make recommendations for protecting the personal data of migrants.

---

[1] Cowen, Zelman 'The Private Man' The Boyer Lectures, Australian Broadcasting Commission (1969) in Malcolm Crompton, Federal Privacy Commissioner, *What is privacy?* Privacy and Security in the Information Age Conference, Melbourne, 16-17 August 2001 <http://www.docstoc.com/docs/2253786/What-is-privacy>

[2] For the purpose of this thesis, the word 'migration' refers to international migration and includes the process of non-nationals moving, either across an international border, or within the territory of a State. There is indeed a legal distinction between the terms 'internal migration' and 'international migration.' For the internationally accepted definition of these terms, see: Perruchoud, Richard and Redpath-Cross, Jillyanne eds. (2011) *International Migration Law: Glossary on Migration* 2nd Edition at 51, 52 and 62.

The information age

The information age has placed the issue of privacy and confidentiality at the centre of public, legislative and media debates. This is due to the widespread use of the Internet, increase in computer capacity and storage mechanisms, and the fact that data is easily accessible through social networking sites. Factors that affect privacy in the information age include 'the volume, magnitude, complexity, and persistence of information; the expanding number of ways to collect information; the number of people affected by information; and the geographic spread and reach of information technology.'[3] These factors are changing and expanding in scale with unprecedented speed and our ability to understand and contend with their implications often falls behind. In addition, 'the sheer quantity of information; the ability to collect information unobtrusively, aggregate, and analyze it; the ability to store it cheaply; the ubiquity of interconnectedness; and the magnitude and speed of all aspects of the way we think about, use, characterize, manipulate, and represent information are fundamentally and continuously changing.'[4]

Data protection

In the context of migration, advanced technology is being used as a tool to control borders, identify individuals, verify the authenticity of travel documents, and deliver

[3] Waldo, James; Lin, Herber S; and Millett Lynette I (2007) *Engaging Privacy and Information Technology in a Digital Age* at 27.

[4] Ibid, *Engaging Privacy and Information Technology in a Digital Age* at 30.

public services and humanitarian aid. There is, however, a growing concern that States are using surveillance techniques and biometric systems to keep track of the movement of individuals. Often the protection of personal data is absent in technology used to manage migration. If seen from a human rights perspective, that is, data protection stemming from the right to privacy, it becomes apparent that data protection includes the right to control personal data related to oneself. In recent years, privacy advocates have called for caution in the implementation of migration law and policy that focus on border control and overlook the human rights of migrants. While advanced technology facilitates migration management and data exchange, it also threatens human rights and creates vulnerabilities relating to data theft, data loss, inappropriate disclosure and misuse of personal data.[5] This has been exacerbated by globalization and the exercise of State sovereignty in the wake of terrorism.

Migration

The 2013 United Nations Global Migration Statistics reveal that '232 million people or 3.2 per cent of the world's population are international migrants when compared to the 175 million in 2000 and 154 million in 1990' and the 'forecast for the year 2050, four decades from now, is about 405 million migrants.'[6] This unprecedented increase in the number of migrants around the world has gained saliency in political debates and this has heightened the concern that weak migration management systems may

[5] Martens, Ruzayda (2011) *IOM Data Protection Manual* at 3.

[6] 'Number of international migrants rises above 232 million' UN News Centre, New York, 11 September 2013
<http://www.un.org/en/development/desa/news/population/number-of-international-migrants-rises.html>

encourage irregular migration and endanger the safety and security of nationals.[7] The 2011 World Migration Report projected at the time that there is around a billion migrants worldwide (215 million international migrants and 740 million domestic migrants) and this was 'expected to expand in size and complexity due to growing demographic disparities, new global and political dynamics, technological revolutions and social networks'.[8] 'The digital world we live in today demonstrates that almost 2 billion of the estimated 3 billion migrants are connected to the Internet, and while technology keeps people connected all over the world, it is not without risk to infringement of individual rights.'[9] The September 2011 attacks and subsequent terrorist threats have added to the complexity, resulting in automatic links between migration, security and terrorism.[10] Consequently, migration is perceived negatively and immigration officials often overlook the rights enjoyed by migrants. International agencies have stressed to governments that there is a need to shift the focus to the voice of the migrant and the positive contribution of migration.[11] This shift in focus will foster the development of national migration strategies and laws that aim to manage migratory flows without infringing upon human rights and it will help to alleviate social and economic pressures by eventually leading to the creation of opportunities for both migrants and nationals of a country.

---

[7] Redpath, Jillyanne (2005) *Biometrics and International Migration* at 5.

[8] Appave, Gervais; Laczko, Frank et al (2011) *World Migration Report 2011: Communicating Effectively about Migration* at 3.

[9] 'Interview with William Lacy Swing, 'Director General of the International Organization of Migration (IOM)' UN News Centre, New York, 6 December 2011 <http://www.un.org/apps/news/newsmakers.asp?NewsID=46>

[10] Op cit note 8, *World Migration Report 2011: Communicating Effectively about Migration.*

[11] See for example, Appave, Gervais and Laczko, Frank (2013) *The World Migration Report 2013: Migrant Well-Being and Development.*

The above-mentioned pertinent migration issues create diverse challenges linked to data protection, and as such, give rise to three interrelated questions. First, to what extent should States be allowed to intrude into the private sphere of the individual? Second, should advanced technology drive policy or should we rather adopt a cautionary approach and develop laws that are flexible in its reach? Third, where do migrants fall in the spectrum and is the current legal framework on data protection sufficient to address the rights of people on the move? This thesis will explore these questions in the area at the intersection between data protection and migration.

1.1 *Objectives*

This thesis covers two broad objectives. The primary objective is to identify gaps and loopholes in the current legal framework covering data protection and migration. The secondary objective is to look in detail at the challenge of having to balance between State interests and individual rights. The cross-border dimension of data protection will be highlighted to provide a better understanding of the nexus between data protection and migration, particularly in the context of humanitarian assistance and migration management where unwanted and inappropriate disclosure of personal data could result in a wide range of risks, including threat to life and safety. Moreover, a human rights based approach will be adopted to identify the gaps and help draw the line between balancing the exercise of State sovereignty and respecting the individual rights of people travelling within and across borders.

International migration law

In the absence of a defined body of law on international migration, States are increasingly exercising their sovereignty to address globalization, combat terrorism and deter irregular migration. In addition to privacy concerns, this has given rise to migrant profiling, discrimination and limitations on the freedom of movement and the right to family unity. In this context, the core minimum standards to be accorded to migrants will be outlined, as well as policy imperatives with an emphasis on the principle of proportionality and accountability, which is necessary to limit the discretionary power of immigration officials when using advanced technology. By supporting the 2009 Madrid Resolution,[12] which calls for a legally binding instrument at the international level, this thesis argues that a firm legal basis is needed to clearly define data protection as a universal legal right. This will, in turn, give rise to corresponding State obligations.

Data protection law

A global assessment indicates that national data protection laws are increasing.[13] Currie and Allan attribute this increase to the extraordinary influence of the EU

---

[12] The Madrid Resolution *International Standards on the Protection of Privacy and Data Protection* International Conference of Data Protection and Privacy Commissioners, 5 November 2009 <http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf>.

[13] See also op cit note 5, *IOM Data Protection Manual* at 107-108 which demonstrates at its date of publication that there were approximately 63 jurisdictions with specific laws on data protection, this number is in the increase with a number of draft laws in the making as seen in the recent global overview in DLA Piper (2013) *Data Protection Laws of the World.* <http://www.thelawyer.com/Journals/2013/03/20/t/b/l/Data_Protection_Laws_of_the_World_2013-414865.pdf>

Directive,[14] which require adequate data protection systems outside the European Union for trade reasons.[15] The increase is also due to proactive steps taken by legislators to close the gap between the growth in technology and the absence of laws regulating the processing of personal data. However, with the exception of the European context, and unless covered by bilateral agreements between States,[16] national laws are generally limited to the territory of one State. The law of one country is not binding on its neighbours, but there is a need to establish common legal standards when handing personal data of migrants travelling across borders.

Arguably, certain rights extend beyond geographical lines, but should data protection extend beyond borders if it is recognized as a legal right? In the European Union, the answer to this question is unequivocally – yes – data protection is explicitly recognized as a fundamental human right afforded to all individuals within the borders of the European Union.[17] The EU Directive, while covering data protection, has an underlying purpose to facilitate data exchange across borders and between member

[14] The official name of the EU Directive is the *Directive 95/46/EC on the protection of personal data and on the free movment of such data* which is the most comprehensive legal instrument on data protection.

[15] Currie, Iain and Allan, Kate (2007) 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator' at 572.

[16] With regard to data protection, there is for example, the Safe Harbor Agreement between the United States of America and the European Union which aims to regulate trade relations requiring the flow of personal data provided adequate safeguards are in place to protect personal data in line with the EU Directive. The implementation of this Agreement is questionable, but the legal basis does exist. For further detail on the Safe Harbor Agreement see: Anneliese (2009) 'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study', UNISA theses and dissertations at 144 <http://uir.unisa.ac.za/handle/10500/1463?show=full>

[17] Article 8 of the 2000 Charter of Fundamental Rights of the European Union states that: '(1) Everyone has the *right to the protection of personal data* concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority.'

states of the European Union. Nonetheless, the European regional legal instruments on data protection are comprehensive and it is constantly evolving to better protect individual rights.[18]

Regional and domestic law

This thesis will assess whether the European model can be translated to the Southern African Development Community (SADC) in light of the different social, economic and political realities experienced in the fifteen Southern African States.[19] Recommendations will be proposed to promote discussion on how to integrate data protection into the development of coherent migration strategies, law and policy in this region. Regardless of the region of focus, to protect individual rights effectively, it is important to continually monitor new developments and ask whether the balance between privacy and competing interests are right for today? This calls for a balanced approach, which on the one hand – recognizes the need to collect and process personal data to the benefit of both States and migrants, and on the other hand – respects the rights of people on the move. The criteria for this balancing test, which should be assessed on a case-by-case basis, will be established with reference to South African jurisprudence.

For ease of reference key terms used throughout this thesis are defined and

[18] See chapter 3.2 for discussion on the European data protection reform.

[19] Currently SADC has fifteen Member States, namely: Angola, Botswana, Democratic Republic of Congo (DRC), Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, United Republic of Tanzania, Zambia and Zimbabwe. For further detail see the SADC website <http://www.sadc.int/english/about-sadc/>

abbreviations are listed, in the attached Annexures B and C, respectively.

1.2 *Contribution to knowledge in the area of research*

The information age has given rise to increased debate on privacy issues and on protecting personal data from unauthorized and inappropriate disclosure. There is, however, little debate on the rights of migrants in this context. There are indeed several studies on privacy and increasingly on data protection, as well as extensive studies on migration. However, few studies have canvassed the intersection between data protection and migration. The right to privacy is protected as a universal right in numerous international instruments, but there is to date, no legally binding instrument on data protection. Nor is there an overarching legal instrument covering international migration. This thesis looks at the crossroad between data protection and migration and seeks to contribute to the academic knowledge and current developments in this field. It supports the 2009 Madrid Resolution calling for a legally binding instrument at international level because a firm legal basis will clearly define data protection as a legal right and give rise to corresponding State obligations. Moreover, by incorporating a human rights based approach into migration strategies, laws and policy; it will help States to draw the line between balancing the exercise of State sovereignty and respecting the rights of individuals travelling within and across their borders. The intention is to help legislators and policy-makers to urge States to proceed with promulgating a binding law on data protection that affords the legal right to all individuals including migrants while trying to achieve the objective of managing

their borders.

1.3 *Research Methodology*

The research was based on library and on-line resources. Primary and secondary materials on data protection and migration at the international and regional (Europe and SADC) levels and within the South African context were relied upon. In addition, human rights legal instruments, case law and academic commentaries on data protection and international migration law were reviewed, as well as available policies at international organizations. The methodology included the collection of qualitative data. Since this thesis focuses on the point of intersection between data protection and migration, interviews were conducted with academics and practitioners in both fields.

The following interviews were conducted in South Africa and in Switzerland during the period January 2011 – August 2011:[20]

- Lawyers for Human Rights; Ramjathan-Keogh, Kaajal; Head of the Refugee and Migrant Rights Programme; 12 January 2011 at 11h30; LHR, 2nd Floor Braamfontein Centre, 23 Jorissen Street, cnr Jan Smuts Street, Johannesburg

[20] The interviews were informal and semi-structured. During January 2011 back-to-back interviews were carried out in Johannesburg with the practitioners and academics and between December 2011 to August 2011 interviews were carried out in Geneva with experts from the International Organization for Migration. Informal discussions were also held with a representative of the United Nations High Commissioner for Refugees; Beck, Alexander; Senior Legal Officer at the Department of International Protection UNCHR Headquarters and a representative of the International Committee of the Red Cross; Bircher, Romain; Head of Data Protection Unit ICRC Headquarters; and conducted in Brussels on 8 November 2012.

- University of Witwatersrand; Visser Cornelius; Lecturer, Privacy Expert; 12 January 2011 at 13h00; Wits, office 83, Oliver Schreiner, School of Law Building, West Campus, Johannesburg
- Human Rights Advocate; Bizos, George; Senior Advocate, Constitutional Litigation Unit; Legal Resources Centre; 12 January 2011 at 15h00; LRC Senate House, 20 Albert Street, Johannesburg
- African Centre for Migration and Society; Landau, Loren; Director of Forced Migration and Refugees Studies Programme; 12 January 2011 at 17h00, Wits, South West Engineering building, Johannesburg
- Legal Aid South Africa; Mayet, Achmed; Senior Litigation Impact Lawyer; 13 January 2011 at 14:30; 41 Fox Street Marshaltown, Johannesburg
- International Organization for Migration; Mariano, Bernardo; Regional Representative of East and Southern Africa; while on travel duty at the IOM Headquarters, 27 May 2011 at 10h30, 1st floor, Avenue des Morillons, Geneva
- International Organization for Migration; Martens, Jonathan; [21] Senior Specialist on Migrant Assistance; 24 July 2011 at 11h30, IOM Headquarters, 4th floor, Avenue des Morillons, Geneva
- International Organization for Migration; Perruchoud, Richard; Former Legal Advisor and Director of the Department of International Migration Law and Legal Affairs; 24 July 2011 at 14h30; IOM Headquarters, 1st floor, Avenue des Morillons, Geneva; and 4 August 2011 at 21h30 by email

Interview questions, as outlined in the attached Annexure A, where developed for the semi-structured interviews with experts to address policy level issues and the

[21] It should be noted that Martens, Jonathan is my husband and the interview was conducted in his professional capacity at the IOM offices.

challenge of implementing human rights in the context of migration. The informal interviews focused on legal/policy considerations including the practical realities when collecting and processing personal data of migrants. The expertise, experience, views and opinions of the interviewees were particularly useful in identifying important policy considerations and this informed the analysis in this thesis. It also helped to outline the practical challenges and good practices associated with protecting personal data of migrants. The outcome of the interviews is filtered throughout this thesis.

1.4 *Limitations*

This thesis provides a legal analysis from the international law perspective. However, due to the lack of directly applicable positive law on the specific topic, the focus turned to domestic law with the view to use the South African jurisprudence as a guide to illustrate criteria that could be applied at the meeting point between data protection and migration. Since data protection and migration are both cross-border issues, domestic law cannot be looked at in isolation, it is for this reason that materials available at the regional level in Europe were analysed with the view to explore whether the practice of European States can be replicated by States in the SADC region.

It should be noted that there were limited materials available on the nexus between data protection and migration and this resulted in an inference being drawn from resources in the data protection field on the one hand, and the migration field on the other hand. Further, in the absence of directly applicable positive law, the research turned to soft law at the international level and relied upon on-line resources and case law at the European and South African levels. The analysis of such materials, supplemented by expert interviews, helped to address the pertinent issues lying at the interface between data protection and migration.

CHAPTER TWO

2. NEXUS BETWEEN DATA PROTECTION AND MIGRATION

This chapter provides a background to the challenge of having to balance between States interests and individual rights and sets the stage for the remaining chapters. Specific examples in the context of humanitarian operations and migration management are used to provide a better understanding of the complexities arising at the nexus between and data protection and migration.

1.2 *Background*

The globalization of irregular migration and its facilitation by transnational criminal groups, coupled with concerns of terrorism, has radically impacted the way in which States manage migration and national security. As a result, the last decade has witnessed the increased use of advanced technology to manage large volumes of data and monitor migratory movements, but often without due regard to the impact on individuals and their human rights.

Normative approach

While migration management is a means by which to protect State borders, it should not be at the expense of individual rights, including the human rights enjoyed by migrants. As outlined in this thesis, any limitation to individual rights should be properly balanced against States interests and it should be necessary and proportionate.

This thesis focuses on a normative approach, which emphasizes migration and data protection from a human rights perspective. Waldo, Lin, Lynette link the 'formal normative basis for data protection laws to catalogues of international and regional treaties that expressly recognize the right to privacy as a human right' and emphasize that this is central to the rationale for protecting personal data.[22] Bygrave stresses the normative importance of data protection as it provides legal and ethical counter-weights to technological imperatives and says even though data protection instruments are not binding at the international level, the principles contained therein 'form a field of law and policy that has attained considerable maturity, spread and normative importance over the last four decades.'[23]

Human rights perspective

According to Cholewinsky, Perruchoud and McDonald international migration law exists as a source of law dispersed among already established areas of law and this gives rise to a normative approach to migration, which is comprised of two aspects. Firstly, principles and standards that derive from State sovereignty including protecting borders, conferring nationality, admission and expulsion, combatting human trafficking and smuggling, and safety of national security; and secondly, the

[22] Op cit note 3, *Engaging Privacy and Information Technology in a Digital Age* at 381 – 382.

[23] See: Bygrave, Lee A (2002) *Data Protection Law, Approaching its Rationale Logic and Limits* generally and,Bygrave, Lee A (2010) 'Privacy and data protection in an international perspective' at 166. Hornung, also recognizes privacy and data protection as fundamental human rights and cautions that the emergence of new technologies are an increased threat to privacy and data protection, for further detail see: Hornung, G (2013) 'Regulating Privacy Enhancing Technologies: Seizing the Opportunity of the Future European Data Protection Framework.'

human rights of those involved in migratory movements.[24] According to the United Nations Office of the High Commission for Human Rights (OHCHR), 'there is relatively little research from a human rights perspective into the reasons why migrants [as opposed to refugees] move.

There is a need to go beyond economic explanations of migration which focus on income poverty and focus also on human poverty, which takes into account the lack of health care, food, education, and inequality of opportunity, discrimination, etc. If seen in this way, the link between poverty and human rights is clear.'[25] The distinction between economic migrants and vulnerable migrants are sometimes blurred and this calls for greater caution when handling personal data of migrants in general. For example, migrants who leave their home to seek better economic opportunities may be subject to human trafficking during their migratory route and are vulnerable to traffickers who may exploit them to make a profit through the sale of human lives. Although migrants may move for economic reasons, migrants should not be viewed as commodities themselves.[26] They should be seen as individuals who are entitled to the full enjoyment of their human rights, regardless of the root cause of their movements. Privacy, on the other hand, can sometimes be seen as a commodity when private facts and information are shared across borders and it is used for trade purposes. Cavoukian notes that privacy remains a fundamental human right even if a degree of control is

---

[24] Cholewinski, Ryszard; Perruchoud, Richard and MacDonald, Euan (2007) *International Migration Law: Developing Paradyms and Key Challenges at* ix.

[25] United Nations Office of the High Commission for Human Rights (OHCHR) 'Migration and Development: A Human Rights Approach' at 2 <http://www2.ohchr.org/english/bodies/cmw/docs/HLMigration/MigrationDevelopmentHC'spaper.pdf>

[26] Ibid, OHCHR 'Migration and Development: A Human Rights Approach.'

lost once it becomes a commodity.[27] Similarly, human dignity is intrinsic to individuals and this remains intact regardless of whether an individual travels in a regular or irregular manner.

Human rights for migrants

At the international level there is a shift towards focusing on the human rights of migrants as evidenced by the establishment of human rights mechanisms in this area, namely, the Special Rapporteur on the Human Rights of Migrants and the Committee on Migrant Workers, both of which have been clear in stating that 'although countries have a sovereign right to determine conditions of entry and stay in their territories, they also have an obligation to respect, protect and fulfill the human rights of all individuals under their jurisdiction, regardless of their nationality or origin and regardless of their immigration status.'[28] The OHCHR goes further to argue that the 'human rights of migrants are central and not ancillary because the effect of respecting human rights has far reaching impacts on society as it goes beyond the individual migrant'.[29] Xenophobia, for example, not only affects migrants negatively but it also threatens the very principle of a free and open democracy built on the recognition that all individuals have dignity and are equal in society. Moreover, with globalization

---

[27] Cavoukian, Ann (1999) *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation.* Anneliese Roos, also acknowledges that personal data has become a commodity for both the State and the private sector, for further detail see: Roos, Anneliese (2000) 'Data Protection for South Africa: Expectations Created by the Open Democracy Bill' at 41.

[28] See United Nations Office of the High Commissioner for Human Rights (OHCHR) 'Migration and Human Rights'

<http://www.ohchr.org/EN/Issues/Migration/Pages/MigrationAndHumanRightsIndex.aspx >

[29] Op cit note 25, OHCHR 'Migration and Development' at 2. <http://www2.ohchr.org/english/bodies/cmw/docs/HLMigration/MigrationDevelopmentHC'spaper.pdf>

one's society extends beyond borders and it can no longer be limited to a geographical line.

The United Nations Secretary-General also recently urged States to achieve policy coherence at the national, regional and international levels regarding the various issues associated with migration in order to protect the human rights of migrants.[30] 'Ensuring that all migrants, regardless of their immigration status, enjoy their internationally recognized human rights at all stages of the migratory processes in countries of origin, transit and destination should be the guiding principle of migration governance.'[31] Cholewinski emphasized, as early as 1997, that 'the right to equality and non-discrimination are all encompassing with reference to race colour, sex, language, religion, political or other opinion, nationality or social origin and it applies equally to migrants because international human rights law in principle applies to all persons regardless of nationality and immigration status.'[32]

State obligations

States have rights and obligations under international law. This includes the right to sovereignty and the duty to protect and keep its citizens secure within its borders. A

---

[30] United Nations 'Promotion and Protection of Human Rights, Including Ways and Means to Promote the Human Rights of Migrants' *Report of the Secretary-General* (A/64/156), 21 July 2010 <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/459/22/PDF/N1045922.pdf?OpenElement>

[31] Bustamante, Jorge A. 'Human Rights of Migrants' *Report of the Special Rapporteur on the Human Rights of Migrants* (A/65/222) 3 August 2010 <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/474/88/PDF/N1047488.pdf?OpenElement>

[32] Cholewinski, Ryszard (1999) *Migrant Workers in International Human Rights Law: Their Protection in Countries of Employment* at 48.

challenge, however, arises when States have to strike a balance and take progressive steps to equally protect the rights of individuals, including the rights of non-nationals travelling within and across its borders. It is indeed a delicate exercise to balance State sovereign rights and individual rights in the context of migration. Notwithstanding this challenge, when it comes to data protection, it is important to consider the bounds of privacy, especially in a world where information technology continues to grow. This thesis does not look into the philosophical aspect of privacy or the classical theories related to this concept. Instead, it views privacy as a fundamental human right as recognized in the Universal Declaration of Human Rights (1948) and related international treaties such as the International Covenant on Civil and Political Rights (1966).[33] As outlined by Cavoukian, 'privacy is a core human value that goes to the very heart of preserving human dignity and autonomy,'[34] and as a fundamental right, it is equally afforded to all migrants.[35]

Migration law

According to the statistics of the OHCHR, 'there is an estimated 214 million people who currently live outside their country of origin, many having moved for a variety of reasons in which the search for protection and the search for opportunity are inextricably entwined.'[36] Despite this large number, there is no overarching international law covering the movement of migrants, nor are migrants referred to as a specific group in one international legal binding instrument. Instead, the rights of

[33] See chapter 3 for further detail.

[34] Op cit note 27, *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation* at 4 includes a detailed discussion on privacy as a human right.

[35] See chapter 3.1 for a further discussion on privacy.

[36] For further detail, see op cit note 28, OHCHR 'Migration and Human Rights.'

migrants are dispersed across various branches of international law, including human rights law, criminal law, labour law, humanitarian law, refugee law, nationality law and the law of the sea. While State sovereignty envisages the right to protect borders and to determine conditions for admission, stay and removal; once non-nationals are in their territory, States are bound by their international obligations to protect, respect and enforce human rights without discrimination.

The importance of the human rights of migrants is evidenced by the appointment of the Special Rapporteur on Human Right of Migrants[37] and by the High-level Dialogue on International Migration and Development (HLD) held in 2006 and most recently the HLD held in October 2013. The High-Level Dialogue brings together all Member States of the United Nations for policy discussions at the General Assembly and as emphasized by the current Special Rapporteur on the Human Rights of Migrants, François Crépeau, 'this High-level Dialogue should affirm that migration, human rights and development are interdependent and mutually reinforcing.'[38] The HLD did affirm this through the promulgation of the 2013 Declaration on the High-Level Dialogue adopted by the UN member states at the HLD, and this fruitful outcome 'recognizes that international migration is a multidimensional and a crosscutting phenomenon that should be addressed in a coherent, comprehensive and balanced

[37] The mandate of the Special Rapporteur on the Human Rights of Migrants was created in 1999 pursuant to the Commission on Human Rights Resolution 999/44. See: United Nations Office of the High Commission for Human Rights: (OHCHR) 'Special Rapporteur on the Human Rights of Migrants' <http://www.ohchr.org/EN/Issues/Migration/SRMigrants/Pages/SRMigrantsIndex.aspx>

[38] 'Preparing for the 2013 High-level Dialogue: A Human Rights Perspective' *Presentation by Professor François Crépeau Special Rapporteur on Human Rights of Migrants* Tenth Coordination Meeting on International Migration, New York, 9-10 February 2012. See:

<http://www.un.org/esa/population/meetings/tenthcoord2012/SRM%20Final%20statement.pdf>

manner, integrating development with due regard for social, economic and environmental dimensions and respecting human rights; confirms the need to protect human rights of migrants; condemns discrimination and xenophobia; and recognizes that international cooperation is needed to address the challenge of irregular migration with full respect for human rights.'[39] To further underscore the importance of the human rights of migrants, the United Nations proclaimed 18 December as 'International Migrants Day'.[40]

Privacy and data protection

Even though the expression of the right to privacy differs across national jurisdictions, there is consensus that the sanctity of the private sphere should be protected from arbitrary interference. Moreover, the right to privacy includes information privacy, which is often seen to be synonymous to data protection. In this thesis the terms 'data protection', 'information privacy' and 'data privacy' are used interchangeably. States and humanitarian organizations inevitably engage in the collection and processing of personal data, whether to manage the flow of migrants within and across borders or to provide humanitarian assistance to individuals in need. It is, thus, important to ensure that data protection is recognized as an integral part of the development and implementation of migration law and policy that focus on the use of technology for the purpose of facilitating migratory movements.

[39] United Nations General Assembly 'Declaration of the High-Level Dialogue on International Migration and Development' (A/86/L.5) 1 October 2013.

[40] United Nations General Assembly 'Proclamation of 18 December as International Migrants Day' (A/RES/55/93) 28 February 2001.

Vulnerabilities in migration

It should be noted that vulnerable migrant groups such as refugees and asylum-seekers, trafficked persons, smuggled persons, unaccompanied minors and irregular migrants[41] are particularly susceptible to the consequences of unwanted or inappropriate disclosure of their personal data as they often lack effective protection from their State and have little legal recourse. While national migration law and policy creates protection for different categories of migrants, State obligations toward individuals who travel in an irregular manner are often unclear. Consequently, decisions are left to immigration officials and law enforcement authorities who sometimes make arbitrary decisions. Such decisions are made through the immigration lens and without due recognition of the human rights afforded to all individuals. Even though irregular migration impedes the legitimate functioning of government initiatives to regulate conditions of entry and stay, the contravention of national immigration laws should not detract from the State's human rights obligations.[42] This thesis emphasises that data protection is not restricted to nationals of a particular country; it applies to migrants as well, whether they travel in a regular or irregular manner.

Nowadays, vulnerable migrant groups who need special protection often travel alongside economic migrants using the same migratory routes and crossing the same

[41] Op cit note 30. The Secretary General of the United Nations states that 'the term "illegal migrant" is broadly used in the context of the criminalization of irregular migration. It is however not recognized in international law [...] "irregular" or "non-documented" migrant, as defined by Article 5 of the International Convention on the Rights of All Migrant Workers and Members of Their Families (1990) are internationally accepted terms to describe the situation of not having, or having lost, the proper documents that allow migrants either to reside in a given territory or to work there.'

[42] Op cit note 8, *World Migration Report 2011: Communicating Effectively about Migration* at 104.

borders without the requisite documentation. This increase in mixed migration[43] has blurred the distinction between the root causes of migration. Travelling without documentation creates a space for human smugglers and human traffickers and this facilitates irregular migration. As stated by the Global Migration Group: 'Irregular migrants often face prolonged detention or ill-treatment, and in some cases enslavement, rape or even murder. They are more likely to be targeted by xenophobes and racists, victimized by unscrupulous employers and sexual predators, and can easily fall prey to criminal traffickers and smugglers. Too often, States have addressed irregular migration solely through the lens of sovereignty, border security or law enforcement, sometimes driven by hostile domestic constituencies [...]. Although States have legitimate interests in securing their borders and exercising immigration controls, such concerns cannot, and indeed, as a matter of international law do not, trump the obligations of the State to respect the internationally guaranteed rights of all persons [...].'[44]

In the context of mixed migration, States and international organizations also collect, or attempt to gain access to, personal data of migrants in order to assess the protection needs of individuals travelling within mixed flows and to address the issue of deterring irregular migration. Having access to personal data is indeed a necessary component of assessing the needs of individuals and the protection interventions required, however, the collection and processing of personal data needs to be regulated to ensure that the

[43] Mixed migration is defined as 'the mixed flow of migrants, that is, complex migratory population movements including refugees, asylum seekers, economic migrants and other migrants as opposed to migratory population movements that consists entirely of one category of migrants.' See op cit note 2, *International Migration Law: Glossary on Migration* 2nd Edition at 63.

[44] 'Landmark Statement on Protecting the Human Rights of Migrants' Global Migration Group, 30 September 2010 <http://www.ohchr.org/EN/NewsEvents/Pages/MigrantsInIrregularSituation.aspx>

use thereof does not infringe upon individual rights or result in identification that could harm vulnerable migrants in particular.

Data protection law

The 1990 United Nations Guidelines for the Regulation of Computerized Personal Data Files (UN Guidelines) draw from the commonly accepted data protection principles as set out in the Council of Europe and European Union legal instruments and the Guidelines of the Organization for Economic Co-operation and Development (OECD),[45] but it fails to oblige States to enforce data protection as a legal right. As evidenced by the 31st International Conference on Data Protection and Privacy Commissioners, there is a need to strengthen the international character of data protection through the adoption of a universal and binding international instrument.[46] This thesis supports the *Joint Proposal for Setting International Standards on Privacy and Personal Data Protection* adopted at this Conference and has a closer look to determine if it sufficiently addresses data protection issues in the migration context.

Generally, data protection concerns include, *inter alia*, unlawful and unfair collection without the consent of the person, lack of data quality, collection of excessive categories of data, unclear purposes which are not communicated to the person at the time of collection or disclosure, inadequate confidentiality obligations, unsafe data storage, lack of data security mechanisms, inappropriate and improper disclosure, and

[45] See chapter 3.2 for futher detail.

[46] Op cit note 12, '*The Madrid Resolution International Standards on the Protection of Privacy and Data Protection.*'

unauthorized use for purposes unrelated to the specified purpose for collecting the personal data in the first place. In the context of migration, if data protection safeguards are absent, the life and safety of individuals can also be threated.

Data protection practice

Ideally protection standards should be pre-empted by law, however, sometimes practice goes further than law and in the absence of a legally binding international instrument one has to look at the practice at international level. The United Nations agencies and other intergovernmental organizations[47] generally adhere to the standards set out in the UN Guidelines, albeit non-binding. Some agencies simply follow the UN Guidelines but do not have comprehensive institutional policies, while others who may have internal policies in the making are still indecisive whether they should be made publicly available. Recently, at the 4th International Data Protection Workshop, the International Criminal Police Organization (Interpol) presented their data protection policies on protecting personal data in the context of prosecutions and investigations.[48] In addition, the International Organization for Migration published its Data Protection

[47] Relevant agencies operating in the migration context include the United Nations High Commissioner for Refugees (UNHCR), the United Nations Office of the High Commissioner for Human Rights (OHCHR), the United Nations Children's Fund (UNICEF), the United Nations Office for the Coordination of Humanitarian Affairs (OCHA), the International Labour Organization (ILO), the International Organization for Migration (IOM), International Committee of the Red Cross (ICRC), and the World Health Organization (WHO) amongst others.

[48] The 4th International Data Protection Workshop was organized by the European Data Protection Supervisor and the World Customs Organization, 8-9 November 2012, Brussels, Belgium. Participants included representatives from 50 international and European agencies specializing in privacy and data protection.

Manual in 2010 and this provides guidance focused on protecting personal data of migrants.[49]

It should be mentioned that while available policies and guidelines are indeed useful, there are new arising issues such as crises mapping that are yet to be addressed by international organizations.[50] This issue of crises mapping will be discussed in the next section.

2.2 *Points of Intersection*

This section aims to illustrate the meeting point between data protection and migration in the context of humanitarian assistance and migration management. It highlights the concern for protecting the life and security of the individual and the need to address human rights implications prior to using advanced technology, and discusses the emerging issue of crisis mapping and third party requests to access personal information collected during humanitarian operations. It emphasizes that migration management efforts require engagement in case specific sensitivity assessments and application of the proportionality test when using technology such as biometric

[49] The IOM Data Protection Manual was published to coincide with International Data Protection Day, see: 'IOM Publishes Data Protection Manual' IOM Press Briefing, Geneva, Switzerland, 27 January 2012<http://www.iom.int/jahia/Jahia/media/press-briefing-notes/pbnEU/cache/offonce?entryId=31191>

[50] Crisis Mapping can be described as the combination of information collection, visualization and analysis within the context of a dynamic interactive map. See Patrick Meier, 'What is Crisis Mapping? An Update on the Field and Looking Ahead' iRevolution, 20 January 2011 < http://irevolution.net/2011/01/20/what-is-crisis-mapping/> and Patrick Meier's overview of the IOM Data Protection Manual with reference to crises mapping in his article 'On Crowdsourcing, Crisis Mapping and Data Protection Standards' iRevolution, 5 February 2012 < http://irevolution.net/2012/02/05/iom-data-protection/>

systems to ensure that adequate data protection safeguards are applied after weighing the benefits and risks to individual rights. It also highlights means by which to reduce the risks to data protection with reference to privacy impact assessments and inclusion of 'privacy by design' into the technology itself, coupled with human intervention and complaints mechanisms, to address inherent fallibilities in the system. In addition, it supports the view that if migration is addressed from a human rights based approach it can help States to address migration issues more coherently.

i) *Humanitarian Assistance*

> '*Data collection in conflict zones is extremely sensitive as it may put people at risk, or distort reality in a way that may invoke harm.*'[51]

The collection and processing of personal data is an integral part of humanitarian operations. Often data collection is necessary to assess the target group and to identify the specific needs of women, children, elderly and persons with Human Immunodeficiency virus/Acquired Immune Deficiency Syndrome (HIV/AIDS).[52] It is also needed to ensure that individuals are registered to receive international protection, emergency relief items such as food, shelter and medical treatment, and where necessary, to effect evacuation to safe-havens. In conflict situations, improper use and

[51] Ibid, 'On Crowdsourcing, Crisis Mapping and Data Protection Standards' at 3.

[52] United Nations Population Fund (2010) *Guidelines on Data Issues in Humanitarian Crisis Situations* at 34.

unauthorized disclosure of personal data could result in a multitude of risks, ranging from physical violence to discrimination and social marginalization.[53]

Conflict situations

To date, the Rwandan Genocide and civil war of 1994 was one of the world's worst humanitarian crises.[54] The personal data of Rwandan nationals in the context of the crisis was particularly sensitive, their names revealed their ethnicity, and any disclosure to the opposition ethnic group placed them in harms way. Amidst the catastrophic incidents, which resulted in the death of an insurmountable number of Rwandan nationals massacred because of their Hutu or Tutsi ethnicity, United Nations aid officials were also killed.[55] During the humanitarian assistance provided by the United Nations Development Program (UNDP), one of its employees allegedly disclosed privileged and confidential information including the names, contact lists, safe-havens and whereabouts of UNDP beneficiaries and humanitarian aid workers, as well as the evacuation points at border posts. According to news reports, the UNDP employee was a computer technician who could have had access to the personnel records of staff and beneficiaries; alternatively, the confidential information could have been inadvertently revealed by one of his colleagues who viewed him as a trusted colleague.[56] Regardless of the manner in which he obtained access to the confidential

---

[53] Op cit note 5, *IOM Data Protection Manual* at 13. See also 'Data Collection in Humanitarian Response: A Guide for incorporating Protection', Inter-Action Protection Working Group <http://www.jointokyo.org/images/cms/Data_Collection_in_Humanitarian_Response.pdf>

[54] Of similar magnitude is the Darfur crisis and the current Syrian crisis.

[55] 'UN Worker Arrested Over Genocide' Reuters, 13 April 2001 <http://tvnz.co.nz/view/page/425822/36358>

[56] See: Stein, Ginny 'Rwanda – Questions of Murder' SBS Dateline, 21 February 2007 <http://www.sbs.com.au/dateline/story/transcript/id/130743/n/Rwanda-Questions-of-Murder>.

information, the method was clearly deceptive and the disclosure resulted in the death of the persons identified on the contact lists.

Rwanda case

It is alleged that this UNDP employee was complicit in, or even, directly involved in killing 32 Rwandan beneficiaries and 27 UNDP staff. In 2009 the International Criminal Tribunal for Rwanda (ICTR) failed to sign an indictment against the alleged UNDP employee on the basis of insufficient evidence of genocide to warrant prosecution before the ICTR. However, he was arrested in Paris following a warrant issued by the International Criminal Court (ICC) for allegedly killing the 32 Rwandans based on their ethnicity and for identifying UNDP staff to be killed.[57] In January 2011 France extradited him to the ICC for war crimes and crimes against humanity, but in December 2011 the ICC dismissed the case on the grounds of insufficient evidence.[58] Although the allegations remain unresolved after several United Nations and international criminal investigations, this case illustrates the potential dangers that are present when collecting personal data in the context of humanitarian assistance. Harm or threat to the life is a concern for both humanitarian aid workers and the beneficiaries they seek to assist.

[57] See: 'ICC - France Arrests Rwandan Rebel Leader Callixte Mbarushimana in Paris for War Crimes Committed in DR Congo's Kivu Province in 2009' Congo Watch, 31 October 2010 <http://congowatch.blogspot.com/2010/10/icc-france-arrests-rwandan-rebel-leader.html?m=1>

[58] See: 'Callixte Mbarushimana is Released from Custody' ICC Press Release, 23 December 2011 <http://www.icc-cpi.int/NR/exeres/4D4FA434-3060-4EF7-8E5C-AD5C53540E64.htm>

Risk assessments

It is, thus, of great importance to take extra care in situations of conflict and to ensure that personal data is kept strictly confidential. In addition, strict access controls to information technology systems and adequate data security measures are necessary to limit access to only authorized persons and to prevent it from falling into the hands of unscrupulous individuals with malicious intent. The International Organization for Migration (IOM) recommends conducting a risk assessment prior to data collection and throughout the data processing process to ensure that adequate data protection safeguards are in place. This means weighing the probability of harm against the potential risks and ensuring that the benefits significantly outweigh the risks.[59]

Technology in emergencies

International organizations are increasingly looking into advanced technology as an added value in preparation of their emergency response operations. One such method is crisis mapping, which is not new to the humanitarian field. Crisis mapping can be defined as the use of population census maps, and most recently, satellite images through Internet access points as a tool to plan humanitarian intervention in crises situations.[60] In the past it has been used as a pre-emptive activity to ensure effective and efficient rollout of medical assistance and emergency relief items at the right time and at the right place. However, it is fast evolving with advanced surveillance technology that has added the dimension of virtual interaction in real time as well as

[59] Op cit note 5, *IOM Data Protection Manual* at 16 -17.

[60] See also op cit note 50 for an explanation of crisis mapping.

live mapping. In addition, crisis mapping is complemented with geolocation[61] tools such as mobile phones and Internet access points that allow individuals in need to communicate with the international community for help.

Humanitarian emergencies have been at a peak lately with the Arab spring starting in January 2011, the consequent political crises in Syria, Mali, South Sudan and the Central African Republic, as well as many other ongoing internal conflicts and territorial wars that have resulted in forced migration. When coupled with population movements resulting from national disasters such as the January 2010 earthquakes in Haiti, the Pakistani floods in July 2010, and the Japanese tsunami, earthquake and nuclear meltdown in March 2011,[62] it is clear that humanitarian actors need more effective methods to ensure timely intervention. Indeed, crisis mapping can be an effective emergency preparedness tool and advanced technology can help to gather data more comprehensively and speedily. During the crises in Libya, for example, a crisis map was developed for the United Nations Office for Coordination of Humanitarian Affairs (OCHA), thereby facilitating insight into conflict areas which helped to identify points of access to provide humanitarian assistance where needed.[63]

In addition, surveillance technology can facilitate access to a humanitarian crisis when

---

[61] Wikipedia defines 'geolocation' as the identification of the real-world geographic location of an object, such as a radar, mobile phone or Internet-connected computer terminal.

[62] David, Anne-Sophie 'Le nouvelles technologies au service del'aide humanitaire' French weekly Le Novel Economiste, 12 April 2012.

[63] See: Searle, Louise and Wynn-Pope, Phoebe 'Crisis Mapping, Humanitarian Principles and the application of Protection Standards: A Dialogue between Crisis Mappers and Operational Humanitarian Agencies,' Meeting Record, 17 November 2011, Geneva <http://irevolution.files.wordpress.com/2012/02/world-vision-geneva-report.pdf>

infrastructures are destroyed and communication to the outside world is cut off. Telecoms Without Borders is active in this area and it facilitates satellite links when it is impossible for United Nations aid workers to be physically present on the ground. As part of the Emergency Telecommunications Cluster it provides technical means to other non-governmental organizations and United Nations agencies within 30 days of a crisis and facilitates virtual connection in less than 24 hours.[64] Since humanitarian presence is shrinking in certain countries due to *inter alia* terrorist abductions of humanitarian workers, more international agencies are looking into the use of such surveillance techniques.

Sensitivities

Indeed, the use of this advanced technology in humanitarian crises is far reaching, but it is not without risks. 'Do no harm' is a universal principle that permeates the collection of data in humanitarian interventions.[65] It is equally important to ensure that sharing of personal data, where necessary to meet the specified purpose of delivering humanitarian aid, does not result in backlash to individuals in their communities.[66] Disclosure of HIV/AIDS status is, for example, very sensitive and the power to decide how, when, to whom, and to what extent such personal medical data can be shared vests with the individual. While there are legal and ethical reasons of disclosure that could be justified, those living with HIV/AIDS often suffer discrimination related to the unauthorized disclosure of their HIV/AIDS status. For example, if the HIV/AIDs

[64] Ibid, 'Crisis Mapping, Humanitarian Principles and the application of Protection Standards: A Dialogue between Crisis Mappers and Operational Humanitarian'.

[65] Op cit note 53, *Guidelines on Data Issues in Humanitarian Crisis Situations* at 44.

[66] Ibid, *Guidelines on Data Issues in Humanitarian Crisis Situations.*

status of an individual is inadvertently revealed in a community where it is seen as taboo, it could result in discrimination, or even in physical violence.[67] Yet, this sensitive personal medical data is necessary to ensure that proper medical treatment is delivered to those migrants living with HIV/AIDS. Inaccurate recording of personal data could also have a negative impact on service delivery. The personal medical data of a migrant might, for example, be a determinant factor for his/her resettlement to another country; therefore if the medical data incorrectly indicates that the migrant is HIV positive, it could hamper the migrant's resettlement application if the country restricts entry based on medical grounds.[68]

Data collection

Data collection through crisis mapping has the potential to result in the development of data centres with large storage capacities. When Telecoms Without Borders set up satellite communication centres during the Libyan crisis and provided estimates and data analysis to the United Nations,[69] it greatly enhanced the rollout of emergency relief items as it allowed humanitarian aid workers to project the movement of migrant groups, enabled registration and identification of their specific needs, and improved response times to service delivery. The establishment of data centres does, however, have the potential to jeopardize the safety of the very people they seek to protect.

---

[67] Op cit note 49, 'IOM Publishes Data Protection Manual'

[68] This is often under the guise of protecting the public health of nationals. For example, the United States of America used to have an entry ban on medical grounds and migrants with HIV/AIDS applying for resettlement would not qualify for the resettlement programme. This ban was, however, lifted in 2009. Today HIV/AIDs can be treated and concerns for public safety are no longer warranted. See: Peston, Julia 'Obama Lifts a Ban on Entry into US by HIV Positive People' The New York Times, 30 October 2009 <http://www.nytimes.com/2009/10/31/us/politics/31travel.html>

[69] Op cit note 63, 'Crisis Mapping, Humanitarian Principles and the application of Protection Standards: A Dialogue between Crisis Mappers and Operational Humanitarian Agencies.'

Since it stores large volumes of valuable and sensitive data, including personal data, it is of utmost importance to protect the location of the data centre, even if the location is in a remote area.

Data security

Data centres need a high level of security with controlled access to the physical location. In addition, high levels of data security mechanisms need to be in place to protect the computer technology from being accessed remotely by hackers. Any unauthorized access to databases used during humanitarian assistance, or inappropriate disclosure of personal data and sensitive information stored therein, could result in harm or threat to life especially in the context of volatile situations. Of utmost importance is that tools aiming to assist in a humanitarian crisis should not end up in the wrong hands as it can help persecutors to trace the whereabouts of individuals, and in the worst case scenario, facilitate ethnic cleansing as seen in the Rwandan case.

Thus, humanitarian actors should ensure that safety precautions and data protection safeguards are embedded into strategies that envisage the use of crisis mapping and geolocation tools. In particular, it is paramount to ensure that the location of data centres are kept strictly secure and the location details must be privileged to those authorized individuals who require access for the specified purpose of the humanitarian operation.

Restricted data access

Another issue that arises in humanitarian interventions is third party access requests to the valuable information captured by different agencies. In the Libya crises, for example, the Office of the High Commissioner for Human Rights (OHCHR) requested access to databases in order to verify human rights abuses. The International Criminal Court also tried to gain information in support of international criminal law investigations.[70] Humanitarian actors such as international organization, and governmental and non-governmental entities operating in humanitarian interventions should be careful not to take up an 'information sharing role,' even under conditions of confidentiality, as this could compromise, *inter alia*, the humanitarian principles of impartiality, neutrality and independence.[71] It may also negatively impact on humanitarian operations where there is limited access to certain areas and it could jeopardize the safety of humanitarian aid workers and beneficiaries of the aid.

While it is often necessary to share information with humanitarian partner agencies for a specified purpose related to the humanitarian operation, a prior assessment is needed to ensure that the safety of individuals are protected. In the migration context, the sensitivity of the personal data should be assessed on a case-by-case basis and it is important to balance between the benefit of data collection and the risk of unauthorized disclosure, bearing in mind that the benefits should always outweigh the

[70] Ibid, 'Crisis Mapping, Humanitarian Principles and the application of Protection Standards: A Dialogue between Crisis Mappers and Operational Humanitarian Agencies.'

[71] Op cit note 53, *Guidelines on Data Issues in Humanitarian Crisis Situations* provides detail on the importance of upholding these humanitarian principles.

risks.[72]

Determining factors in the balancing test

Any limitation to the rights and interests of data subjects in the migration context 'should always be proportional to, or appropriately balanced with, the benefits gained when intending to derogate' from applying data protection safeguards. The test is one of 'reasonableness and the derogation must be sufficiently justified' to avoid an arbitrary decision.[73] The IOM Data Protection Manual draws from humanitarian principles and in the application of the IOM policy also puts forward factors to consider when weighing competing rights against data protection, these include the nature of the personal data, prevailing circumstances, whether there is a pressing need to derogate from the commonly accepted data protection principles, the purpose achieved by the derogation, the nature and extent of the derogation, the relationship between the derogation and the specified purpose for which the personal data was collected, the proportionality between the extent of the derogation and the purpose of the derogation, and ensuring minimal impairment on the rights and interests of the individual by considering alternative measures to achieve the desired goal. The benefit to, and impact on, the data subject and the target population is an equally important consideration and the threat to the life, health and safety of individuals and humanitarian aid workers in the migration context is paramount.[74]

---

[72] Op cit note 5, *IOM Data Protection Manual* at 16-17.

[73] Ibid, *IOM Data Protection Manual* at 42.

[74] Ibid, *IOM Data Protection Manual* at 103.

ii) *Migration Management*

> *'If a regime of "migration management" is to be effective, not only must it be credible to States, but it must also be credible to migrants.'*[75]

States are increasingly using biometric systems as a migration management tool in order to manage large volumes of migrant data and to verify travel documents, but if it is used inappropriately and without adequate safeguards, it can have implications on individual rights.[76] This section examines the use of advanced technology in migration management, in particular biometric systems.

Biometrics systems

Biometric systems are defined as 'applications that use biometric technologies, which allow the automatic identification, and/or authentication/verification of a person. It is used to capture biometric data and this changes the relation between the body and identity because characteristics of the human body become machine-readable and easily accessible.'[77] Since biometric data is derived from the human body, it is unique in identifying an individual. This unique character relates to the integrity of the body,

---

[75] Amnesty International (2006) *Living in the Shadows: A Premier on the Human Rights of Migrants* <http://www.amnesty.ch/it/doc/temi/asilo-e-migrazione/fatti-e-cifre/en-savoir-plus>

[76] See similar arguments by Redpath, Jillyanne op cit note 7, *Biometrics and International Migration* at 10-17 and Thomas, Rebekah (2005) *Biometrics, International Migration and Human Rights* at 378.

[77] For definition and further discussion, see: The Working Party on the Protection of Individuals with regard to the Protection of Personal (Data Protection Working Party) 'Opinion 3/2012 on Developments in Biometric Technologies' (WP193), 27 April 2012 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

and thus, has the potential to interfere with human dignity.[78] Other implications on human rights include disrespecting the right to privacy and data protection, violating the undertaking to keep biometric data confidential, and limiting the right to move around freely and lawfully. For example, if the biometric data of a migrant does not match the record in the system, notwithstanding the fact that the migrant is travelling legally and with the requisite documentation, immigration officials can and often do impede the migrant's movement at the border and this could result in the migrant being detained for unjustified reasons due to the biometric system failure.

Advantages of biometrics

The process of globalization has dramatically increased the number of migrants travelling across borders. Consequently, States are faced with the challenge of handling an increase in migratory flows while maintaining a sufficient level of security, and at the same time, respecting individual rights. In response, States have introduced extensive application of biometrics systems as a migration management tool.[79] This started in the Europe and has spread globally even to countries that do not have the technological infrastructure needed to support biometric systems. Due to the constant evolution of technology, research shows that biometrics data do not only include traditional fingerprints, iris scans, facial image, hand geometry, voice recognition and signature verification; it now also includes multimodal identifiers such

[78] Directorate General of Human Rights and Legal Affairs 'Progress Report on the Applications of the Principles of Convention 108 to the Collection and Processing of Biometric Data' (2005) at 82 - 84 in *Data Protection: Compilation of Council of Europe Texts*, Strasbourg, November 2010 <http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompli_en.pdf>

[79] Gromovs, Juris (2008) *A Compendium of Legal Instruments of the European Union and the Council of Europe concerning the Use of Security Features and Biometric Identifiers in Passport and Travel Documents, Residence Permits and Short-term Visas* at 279.

as vein prints.[80] However, the most frequently used and commonly known biometric feature is still the fingerprint.[81]

The International Civil Aviation Organization (ICAO) sets the international standards on the use and functionality of biometrics in passports to control cross border movements through secure methods[82] and concludes that the face is in fact the most suited for travel documents, with fingerprints and iris scans as a second choice.[83] Coats confirms that the ICAO has set the standard for passports to include biometrics and this will drive the legislative requirement for biometric passports domestically and internationally for all passports.[84] Since biometric data is unique to each individual, it can guarantee the authenticity of identification documents indicating that a photograph or fingerprint represents who the person purports to be. This is an advantage for States because it helps to reduce document fraud and it assists with preventing the use of multiple identities, the latter believed to be used by terrorists.[85] It is therefore increasingly being used as a tool for screening individuals against watch lists and for

---

[80] Op cit note 76, see *Biometrics, International Migration and Human Rights* at 383-384.

[81] Ibid, *Biometrics, International Migration and Human Rights* at 7. See also: International Civil Aviation Organization 'Accelerating a Worldwide Approach to Biometric Identity Confirmation in MRTD's as the Key Token of Entitlement for Simplified Passenger Travel' Twelfth Report, Cairo, Egypt, 22 March 2004 to 2 April 2004 <http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12ip007_en.pdf>

[82] Coats, William Sloan et. Al. (2007) *The Practitioner's Guide to Biometrics* at 198.

[83] The ICAO standards introduce interoperable global standard of biometrics in Machine Readable Travel Documents. For the latest developments, see: Knopjes, Fons 'Total Identity: Latest Developments ICAO' ID Management Centre <http://www.idmanagement-centre.com/>

[84] Op cit note 82, *The Practitioner's Guide to Biometrics*.

[85] Op cit note 78, 'Progress Report on the Applications of the Principles of Convention 108 to the Collection and Processing of Biometric Data' at 83.

managing illicit movements. To note, though, that the European Data Protection Supervisor in looking specifically at biometrics has warned that the use of biometrics systems indirectly develops a category of *male fide* travellers and this could lead to a migration system based on suspicion instead of the good faith of travellers.[86] What is useful is that biometric systems allow for an audit trail in the issuance of travel documents and it can also assist in the delivery of services to migrant populations.[87]

Technological flaws

Notwithstanding the above-mentioned positive aspects, biometric systems have inherent flaws embedded in the technology. Weather conditions can result in failure to read biometric data correctly and the realities of different groups of migrants such as amputee refugees who lack fingerprints are likely not be accommodated by this technology. Therefore the possibility of alternative mechanisms for vulnerable groups such as disabled persons and persons with ethnic or cultural identifying characteristics on their faces or hands, as well as children and elderly, need to be taken into account to ensure that individuals are not discriminated upon by the use of technology that does do not cater for special needs and natural change in biometric features due to age.

---

[86] See: European Data Protection Supervisor 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on Migration' (2012/C 34/02), 9 July 2011, Official Journal of the European Union at 25 <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:034:0018:0026:EN:PDF>

[87] Op cit note 7, *Biometrics and International Migration* at 8.

To address inherent technical flaws and human error when using biometric systems, the technology should be kept up to date and stored in places where the weather will not affect it. In addition, biometric systems should include features to cope with bodily differences and provide alternative mechanisms for vulnerable groups such as children, elderly, disabled persons, and persons with ethnic, cultural or religious identifying characteristics.[88]

Human alternatives

Training of border officials is essential to avoid infringement of human rights. To ensure that individual rights are adequately protected, measures should be taken to ensure that border officials are equipped to handle exceptions such as failure of the technology in reading the biometric data, improper functioning or damage of the storage medium and tampering with documents. There should be procedures for exceptional circumstances to ensure that individuals are allowed to travel by either accepting alternative biometric features or allowing for a different method of identification. This would also help to avoid discrimination against an individual based on physical features such as ethnic markings that interfere with biometric readings.

The Data Protection Working Group in Europe goes further to emphasize that an impact assessment should be employed given the potential harmful effects on the

[88] See: Homeland Security, Biometric Identification & Personal Detection Ethics (HIDE) 'Project Report on Policy Forum on Body Issues' <http://www.hideproject.org/downloads/deliverables/D4.2aPolicy_Forum_Report_on_Body_Issues.pdf >

human dignity, privacy and data protection of vulnerable persons resulting from the application of technology, in particular, and 'for the sake of the person's dignity and to ensure reliability of the procedure – the collection and processing of fingerprints should be restricted for children and for elderly people and the age limit should be consistent with the age limits used large EU biometric databases (as per enacted regulations).' In the event that such individuals are unable to complete an enrolment in the biometric system due to certain physical characteristics or change in fingerprints resulting from skin development or deterioration, specific alternatives with appropriate safeguards need to be in place to guard against the risks of stigmatization or discrimination of those individuals either because of their age or because of the inability to enroll their biometric data.[89]

Functional creep

Equally important when using biometrics is preventing what is called a 'functional creep,' that is, biometric data that is used for purposes contrary to the specified purpose and without the consent of the individual.[90] For example, the collection of biometric data for immigration purposes should not be used for discriminatory practices such as racial and ethnic profiling at airports. Another concern is that the collection of biometric data may divulge additional information that is not needed to meet the specified purpose of the data collection. For example, iris scanning can detect health conditions and the collection of such information is not related to identification

[89] Op cit note 77, 'Data Protection Working Party in Opinion 3/2012 on developments in biometric technologies' at 15.

[90] Op cit note 78, 'Progress report on the applications of the principles of Convention 108 to the collection and processing of biometric data'. The concern of 'functional creep' was also raised by the European Data Protection Supervisor in its Opinion 3/2012 when discussing the introduction of large IT systems at border posts in Europe.

of individuals for immigration purposes. Moreover, creating large databases to store biometric data may enable governments to match data and engage in clandestine tracking to secretly monitor the movement of individuals within their borders. While the right of sovereignty enable States to control the movement of individuals by establishing entry and exit conditions, this big brother approach of surveillance monitoring is not compatible in a democratic society.[91] This deepens the gap between the usefulness of biometric systems and the threat of using it for incompatible purposes.[92]

Misuse of personal data

A further danger lies in the potential misuse if biometric data is retained for unlimited periods. Thomas notes that there are a number of data security concerns related to the storage medium, this includes the 'risk of disclosing personal information (including through private agencies) to unauthorized persons and the lack of security measures to ensure appropriate protection against abuse, misuse and malfunction.'[93] Biometric data is vulnerable to unauthorized use if no access controls are in place and data security concerns such as hacking is increased if large volumes of data are stored in a shared database at border posts. Interoperability at the international level, that is, absence of common standards may also lead to incompatible biometric systems.[94]

---

[91] Op cit note 1, 'The Private Man.'

[92] Op cit note 77, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data at 85.

[93] Op cit note 76, see *Biometrics, International Migration and Human Rights* at 395.

[94] Op cit note 7, see *Biometrics and International Migration* at 11.

Balancing right and interests

Data security, global exchange of information, interoperability, migrant profiling, arbitrary decisions based on incorrect biometric reading, as well as technological flaws and human error may impede the right to move around freely and lawfully within and across borders. Thus, an objective balance is needed, particularly because of the imbalance between the power of the State and the power of individuals to assert their rights. The collection of biometric data must be necessary to achieve the purpose of the national security and intrusions to privacy should be at a minimum. When looking into the balancing test it is important to ensure that national security issues are proportional to the intrusion on individual human rights and that data protection standards are not diluted when using advanced technology to protect the security interests of States.

Proportionality

The UN Guidelines recommend proportionality as a means to reduce the risks of impeding on individual rights and this can be applied directly to biometrics, which lies at the intersection between data protection and migration. Article 3 of the UN Guidelines defines the principle of proportionality as 'an assessment of the risks for the protection of fundamental rights and freedoms of individuals and notably whether or not the intended purpose could be achieved in a less intrusive way.' This is usually seen in light of prevailing circumstances and the analysis of proportionality should commence prior to rolling out the use of biometric systems.

According to the Data Protection Working Party in Europe,[95] an analysis of the proportionality of using biometric data involves four important considerations. 'First, the proposed biometric system must be necessary to meet an identified need and this means it should be essential to meet the need rather than merely being a matter of convenience or cost effectiveness. Second, for the biometric system to be effective and meet the need, specific characteristics of the technology proposed must be taken into account. Third, when weighing whether the resulting loss of privacy will be proportional to any anticipated benefit, the benefit must not be relatively minor because then the loss of privacy is inappropriate and likely not proportional (for example an increase in convenience or a slight cost saving is not a proportional intrusion on the right to privacy). Fourth, the adequacy of the biometric system must be assessed by considering whether less privacy intrusive means could achieve the desired need.'[96]

The Working Party warns that the use of biometric data in central databases is risky because of the potential impacts on human dignity and the implications on the individuals' right to privacy and data protection. In line with case law of the European Court on Human Rights, it emphasizes that 'any interference with the right to data protection is only to be allowed on condition that it is in accordance with the law and that it is necessary, in a democratic society, to protect an important public interest which has a clearly specified purpose. If there is a legal basis, the collection and

[95] The Data Protection Working Party was set up under Article 29 of Directive 95/46/EC/. It is an independent European Advisory Body on Data Protection and Privacy, see: <http://ec.europa.eu/justice/data-protection/index_en.htm>.

[96] Op cit note 77, 'Data Protection Working Party Opinion 3/2012 on Developments in Biometric Technologies' at 8.

processing must also be adequate, relevant and not excessive in relation to that purpose. In addition, the limited categories of personal data to be collected and processed to meet the specified purpose should be kept to a minimum and security measures must be adequate and effective.'[97] In referencing case law at the European Court of Human Rights and the European Court of Justice, the European Data Protection Supervisor pointed out that 'any interference with the right to private life must comply with the principle of proportionality and it must meet the standard of being necessary'. Moreover, 'necessity' is a higher burden of proof than just being 'useful' and proof of necessity could be demonstrated by a privacy impact assessment based on sufficient evidence (statistics and estimates of irregular migration are not sufficient to invade privacy).'[98]

Privacy by design

Of relevance to migration management is the concept of 'privacy by design' as introduced by the European Data Protection Supervisor (EDPS). Accordingly, The EDPS introduces 'privacy by design' as a technical necessity that should be built into large information technology systems gathering personal data at borders as this would mitigate the impact on privacy rights, restrict data collection to a minimum, limit retention periods and make the technological process generally more privacy friendly. The Data Protection Working Party in Europe also recommends 'privacy by design' as a high level of technical protection for the processing of biometric data because it

[97] Ibid, 'Data Protection Working Party Opinion 3/2012 on Developments in Biometric Technologies' at 9.

[98] Ibid, Data Protection Working Party Opinion 3/2012 on Developments in Biometric Technologies.'

involves embedding privacy proactively into the technology itself.[99]

If biometric systems are introduced at border posts, it should not only be a matter of convenience, it must be accompanied by stringent data security safeguards, it has to be reliable and accurate and there needs to be a fall back procedure to allow for alternatives in the event of system failure.[100] In addition, as a positive aspect, biometrics can also be used as a security mechanism to ensure that access to a database is limited to only authorized persons with unique identifying biometric data. Thus, biometrics can be used as a privacy-enhancing tool that monitors access to restricted data.

Privacy impact assessment

The Data Protection Working Party in Europe strongly recommends carrying out a Privacy Impact Assessment (PIA) in order to evaluate risks associated with processing personal data and designing additional measures to mitigate these risks before employing the use of biometric systems. Moreover, defining the purpose and the means of executing the PIA should be viewed as an integral part of the design phase of the biometric systems. It outlines the following factors to be taken into account when conducting the PIA: the nature of the personal data needed, the purpose of the data collection, the accuracy of the biometric system, the legal basis and legal compliance

[99] Ibid, 'Data Protection Working Party Opinion 3/2012 on Developments in Biometric Technologies' at 71.

[100] Op cit note 86, 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on Migration' at 20- 23.

requirements, whether consent is required, the access and internal and external sharing of information that is necessary, security techniques and procedures to protect personal data from unauthorized access, whether there are less privacy-invasive measures available to the use of biometric systems, the timeline for retaining and deleting the personal data, and most importantly, protecting the rights of the individual. Finally, the PIA should not only focus on identifying the risks, it should also provide adequate data protection measures and appropriate solutions to mitigate the data protection risks that are identified through the PIA.

Consent for legitimate purpose

It should be highlighted that consent is a core data protection principle and it is often the legal basis for collecting and processing personal data. Consent is, however, tricky to establish in the context of the use of biometrics, but the Working Group recommends that the option of providing alternatives to biometric systems as a lesser intrusive measure indicates free consent if individuals choose the proposed biometric system, moreover, consent is deemed valid only if sufficient information on the use of biometric data is given to the individuals.[101] National legislation can set out a legitimate purpose of rolling out the use of biometric systems in the absence of consent, but the fairness principle still applies and requires that the data subject be informed and be made aware of the purpose of the data collection and the identity of the data controller.[102] In addition, the purpose of the data collection still needs to meet

[101] Op cit note 76, 'Data Protection Working Party Opinion 3/2012 on Developments in Biometric Technologies' at 10.

[102] Op cit note 77, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' at 87.

the principle of proportionality and intrusion on the right to privacy and data protection should be limited to what is necessary to meet the specified purpose of using the biometric data.

If processing biometric data without consent is an exception embedded in the law, at a minimum, individuals should be fully aware of the manner in which their biometric data will be used and they should be ensured of the confidential treatment of their data and the application of appropriate data security measures to protect their data from unauthorized and unwanted disclosure. In practice, the enrolment of the biometric data involves personal contact with the individual; this is the point at which the requirement of informing individuals can be met to ensure fairness in line with the principle of collecting and processing personal data for a lawful and fair purpose.[103] Equally important is general public acceptance to the introduction of biometric systems; this could be achieved through consultations prior to enacting any laws incorporating the use of biometric systems.[104]

Law and use of technology

In Europe the use of biometrics in passports and visas has given rise to the rapid expansion of regional laws.[105] Inherently problematic in this approach is the fact that

[103] Op cit note 77, 'Data Protection Working Party Opinion 3/2012 on Developments in Biometric Technologies.'

[104] Op cit note 76, 'Data Protection Working Party Opinion 3/2012 on Developments in Biometric Technologies' at 28 – 29.

[105] Op cit note 79, *A Compendium of Legal Instruments of the European Union and the Council of Europe concerning the Use of Security Features and Biometric Identifiers in Passport and Travel*

the cross-border dimension of data protection seems to have been an after thought. Laws were developed in response to the use of biometric systems, and have until recently, not taken data protection concerns into account. Redpath emphasises that technology should not be driving law and policy because this creates a risk to impacting on the individual rights of both nationals and non-nationals as seen in government responses to the September 11 attacks. Accordingly, if it is not governed by a legal framework there will be no limitation to the use of such technology which is rapidly expanding based on government demand for reasons of State security and border control.[106] Thus, policy makers/legislators need to take the lead to ensure that there is a legal basis to process biometric data in accordance with adequate data protection safeguards.

Alternative measures

It is equally important to ensure that biometric systems are not used in isolation and that alternative measures are made available to cater for system failure. For example, a biometric system can fail to accurately read biometric data due temperature in the storage area and the system may reject matching the individual with his/her biometric data. 'In order to protect the individual's right not to be subject to a decision affecting him/her based solely on mistaken processing of data by automated means, appropriate safeguards must be introduced such as human interventions, remedies or mechanisms

---

Documents, Residence Permits and Short-term Visas at 277 – 256. It includes a compendium of legal instruments in the European Union, legislative proposals, communications of the European Commission and Instrument on Personal Data Protection relevant to the use of biometric identifiers.

[106] Op cit note 7, see *Biometrics and International Migration* at 14.

allowing the data subject to put (forward) his/her point of view.'[107] This involves both human inspection of travel documents and technical comparison of biometric data stored in databases, as well as appropriate channels to report complaints. Having access to a human being to provide an immediate remedy in the event of system failure is essential and the procedure for recourse to the data subject should not be disproportionately burdensome for the data subject, for example, if a person has a physical disability and their hands are missing the system should not even be applied to that person if the system relies on fingerprints.[108]

Secondary inspection and review

Redpath recommends that secondary inspections and the right to review and appeal decisions that deny entry and movement in a country could help to strike the balance between individual rights and the security interests of the State. It will also guarantee procedural fairness for migrants in decisions that affect them and reinforce accountability of decision-makers.[109] This is needed because biometric systems lack the human factor that provide for alternative immediate remedies and does not allow for review and appeal procedures in the event that the technology fails and reads the biometric data incorrectly.

---

[107] Op cit note 77, 'Data Protection Working Party Opinion 3/2012 on developments in Biometric Technologies' at 10.

[108] Op cit note 78 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' at 90.

[109] Op cit note 7, *Biometrics and International Migration* at 17.

Interoperability

Thomas argues that the 'elevated costs of biometric scanning and reading equipment will perpetuate the inequality between the more technologically advanced countries, and the less developed ones, leaving the latter more exposed (insofar as there exist less efficient border controls), while making the borders of the north ever more impenetrable.'[110] Without taking a particular view on this issue, the counter-argument is that developing countries tend to implement new biometrics systems, whereas the developed countries have to ensure compatibility of new biometric systems with their existing systems and this is sometimes more costly and it often results in additional technical flaws that cannot be remedied due to interoperability. What is clear is that the added costs of new biometric travel documents can be a deterrent for migrants wishing to travel, whether in the north or elsewhere.

Impact on human rights

The motivation by States to use biometric systems is primarily driven by heightened security concerns arising from the growth of transnational crime, irregular migration and terrorism,[111] and it is seen as a key tactic to effective border control. However, the collection and processing of biometric data has the potential to infringe upon the right to privacy and data protection if it is not regulated and used within the parameters of the law. It can also result in migrant profiling and discriminatory treatment if biometric data is read incorrectly and this could lead further to limitations on the

[110] Op cit note 76, *Biometrics, International Migration and Human Rights* at 390.

[111] Ibid, *Biometrics, International Migration and Human Rights* at 377-378. Thomas argues further that the future of biometrics is not restricted exclusively to travel and identification documents. It will inevitably extend into the commercial and private sectors.

freedom of movement and family unity. For example, refugee families can be separated at airports if one of them encounters a problem with their biometric reading, thereby resulting in the unnecessary legal and financial burden of unifying the family in the resettlement country which could take months or even years. Hence, policy-makers/legislators should ensure that the use of biometric systems are regulated and that they do not adversely affect human rights, and any limitation to recognized individual rights has to be appropriately balanced to ensure that it is legitimate and proportional to meet a justifiable purpose.[112]

As stated by Thomas, 'if biometric measures present a risk to an individual's private life, or are considered illegitimate or disproportionate to the ends sought, it will be a clear breach of the specified purpose principle.[113] In the European Data Protection Supervisor Opinion of 7 July 2011 it was highlighted that respect for the fundamental rights of migrants and refugees, including their right to data protection, should be part of comprehensive migration initiatives that envisage the use of technology and surveillance systems at borders, particularly because these groups often find themselves in vulnerable positions.[114]

[112] In the Constitution of South Africa, 1996 this is written in the limitation clause in section 36 of the Bill of Rights. See chapter 5 for further detail.

[113] Op cit note 76, *Biometrics, International Migrants and Human Rights* at 390.

[114] Op cit note 86, 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on Migration.'

Biometric collection and processing

Biometrics is a complex issue that is currently in discussion among European member states and in other international fora, such as the Organisation for Economic Co-operation and Development (OECD) and the International Civil Aviation Organisation (ICAO).[115] Humanitarian aid agencies are consequently receiving requests from its member states to start using biometrics, while others are taking the initiative to introduce it into their programmes, for example, UNHCR and IOM collect biometrics to ensure equal distribution of emergencies supplies to asylum seekers and refugees. Similarly ICRC also uses biometrics in their operations when tracing family members of displaced persons.[116]

Even though there are risks to using biometric systems, State security interests and the right to privacy and data protection may not necessarily be incompatible, and the development of such technology can operate within a context that reconciles the needs and rights of both States and individuals. To do so, the use of biometric systems must be proportional to the limitation on individual rights and the consequent restrictions placed on freedom of movement. Thomson emphasizes that there is a need to approach immigration reform and anti-terrorism as two separate and distinct issues because there is no evidence that the use of biometrics deters terrorism.[117] This mistaken belief,

---

[115] Op cit note 78, 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' at 81.

[116] Informal interview with Perruchoud, Richard, former Legal Adivisor of the Departement of Legal Affairs and International Migration at IOM Headquarters conducted in Geneva, and informal discussions with Beck, Alexander, Senior Legal Advisor at the Department of International Protection, UNHCR Headquarters; and Bircher, Romain, Head of the Data Protection Unit at the ICRC Headquarters conducted in Brussels.

[117] Op cit note 76, *Biometrics, International Migration and Human Rights* at 398.

she says, detracts from the positive aspects of biometrics.

Regulation of biometric systems

The purpose of collecting biometric data and limitations on data sharing, as well as safeguards for ensuring confidentiality and data security needs to be clear if the use of biometric systems is to become a global trend. Moreover, addressing migration issues coherently at national level from a human rights based approach can help States to achieve the objective of managing the movement of individuals more effectively through the use of biometric systems. Although States look to the ICAO standards on the use and functionality of biometrics in passports, there is no legally binding international instrument that includes data protection safeguards for the use and exchange of biometric data. There is arguably no need for a separate international legal instrument on biometric data. The standard internationally accepted Data Protection Principles are flexible in that they allow for adapting to technological advancements through the introduction of code-specific rules/regulations, and biometrics could be elaborated in such a code that would have mandatory force.[118]

The regularization of biometric data is already being developed at the national level as legislators are inserting definitions of biometric data into data protection laws to ensure that it falls within the framework of the this law, but this needs further elaboration through regulations or codes given the complexities surrounding the use of

[118] Op cit note 77, see 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometrics Data' discussing the flexibility and use of a regulatory system which relies on the core data protection principles.

biometric data in pursuit of State interests.

To ensure a standardized approach by States, ICAO standards that take account of data protection could apply in the framework of a universally binding instrument on data protection instrument following the *Joint Proposal for Setting International Standards on Privacy and Personal Data Protection.* The proposal for a binding legal instrument on data protection will be discussed in next chapter 3 following arguments that privacy and data protection should be recognized as a fundamental right alongside other human rights.

CHAPTER THREE

3. PRIVACY AND DATA PROTECTION AS HUMAN RIGHTS

This chapter covers the right to privacy and argues that this fundamental human right forms the basis for establishing a separate right to data protection. In so doing, it adopts a human rights based approach to privacy, which in turn, invites the adoption of uniform and universal rules for protecting informational privacy.'[119] It emphasizes that the right to privacy alone is insufficient to address the myriad of issues arising out of the advanced technology in the 21st century and argues that unless the right to data protection is firmly embedded in the law and accepted as a human right, State interests will continue to trump individual rights without appropriate checks and balances. While privacy can be viewed as a commodity to benefit State interests, if an individual provides consent to the use of personal data, it does not result in complete loss of autonomy; instead there is a need for continued protection against arbitrary infringement and for preventing the misuse of personal data particularly for reasons unrelated to the purpose for which it was disclosed. The discussion then turns to an analysis of existing data protection laws and provides an overview of State obligations under the international legal instruments on human rights.

3.1 *Human Rights Based Approach*

> *'The right to privacy and the concomitant right to protect the content of our lives and move freely is what separates democratic societies from*

[119] Op cit note 27, *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation.*

autocracies and overbearing States.'[120]

Privacy is a fundamental human right as it is given expression in human rights law and the bill of rights or freedom charters the world over.[121] Rotenberg reiterates that the right to privacy is indeed a fundamental human right and warns that in the 21st century it may become one of the most critical human rights of all.[122] Even though national privacy laws may differ, the right to protect private facts from arbitrary interference is echoed in all privacy laws. It is clear in the legal texts that the right to privacy is twofold: it includes the right to positively assert one's right to privacy and the right to protect privacy from arbitrary infringement. This stems from Article 14 of the 1948 Universal Declaration of Human Rights: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*"

Fundamental rights

Since privacy supports the development of individual dignity and autonomy, it has been argued by Cavoukian, among others, that 'privacy is considered to be a fundamental human right, a moral and social "good," and it is recognized as such in

---

[120] February, Judith 'Border Controls May Cross Boundaries' The Cape Times, 29 July 2003 <http://www.queensu.ca/samp/sampresources/migrationdocuments/commentaries/2003/cross.htm>

[121] This argument is supported by Waldo et. al. and Bygrave, op cit note 3 and 23 respectively.

[122] Rotenberg, Marc 'Data Protection Day: Joint High Level Meeting From European to International Standards on Data Protection' Remarks of Marc Rotenberg, President EPIC, Council of Europe and the European Commission Charlemagne Building, Brussels, Belgium, 28 January 2011.

numerous international covenants and declarations.[123] Cavoukian argues correctly that privacy is not an absolute right, instead 'a balance must usually be struck somewhere along the continuum between an absolutist position of total privacy and complete anonymity versus one that denies or negates all privacy rights. While this view recognizes that personal privacy is valued as a fundamental right, deserving of the highest protection; it also recognized that at times, personal information is used in ways that may be considered comparable to a commodity.' The latin proverb *scientia potentia est*, i.e. knowledge is power, is most relevant in the information age, particularly when personal data is seen as a commodity.[124]

Privacy as a commodity

The value of privacy as a commodity is often seen from the perspective of the State or private entities and the individual usually has little power to negotiate the boundaries of information privacy/data protection. Even though individuals may, for example, have little choice but to give photographs and fingerprints for the purpose of obtaining travel documents as prescribed by immigration laws, there should also be laws in place to ensure data protection and respect for privacy when handling personal data to meet the State's interest of managing migration and controlling its borders. Of course an individual can refuse to provide personal data to the State, but this would limit his or her ability to travel. Similarly, in order to receive a government benefit, individuals are required to give detailed personal information including their personal income and

[123] Op cit note 27, *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation.*

[124] Ibid, *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation* at i-iv.

living conditions.[125] Since privacy is not absolute, for privacy advocates, the pertinent issue is for the State to ensure that individuals are fully informed and understand the different approaches to protecting the privacy of their uniquely identifiable information and to contribute to finding effective solutions that can truly enhance people's ability to exercise control.[126]

Freedom to choose

Cavoukian states that 'privacy protection and economic interests should not be seen as an either / or - to varying degrees it can encompass both - provided the individual has a final choice' and that choice has to be made freely and voluntary.[127] The notion of consent is central to data protection and this is seen as the core principle amongst the commonly accepted Data Protection Principles, and since it forms part of the international and European legal instruments and is embedded in national data protection laws outside Europe, it can be seen as an international standard.[128] Consent ensures fair processing of personal data, minimal intrusion and limitations to the use of such data according to the conditions set by the individual.[129] Even though privacy may become a commodity when one loses a measure of control, the limitations on privacy does not mean that no safeguards are needed to protect the handling of

---

[125] Ibid, *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation* at 13.

[126] Ibid, *Privacy as a Fundamental Huma Right vs. An Economic Right: An Attempt at Conciliation* at 27.

[127] Ibid, *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation* at 28.

[128] See the commonly accepted Data Protection Principles in the Madrid Declaration as set out in Chapter 3.2.

[129] Warren, A et al (2001) *Sources of Literature on Data Protection and Human Rights*

personal data. Regulation by law would give the State a firm legal basis for processing personal data and it would help to ensure an appropriate balance between the pursuit of State interests and adequate protection of the individual's right to privacy and data protection.

Notions of privacy (and data protection)

Waldo, et al emphasize that attitudes toward privacy is context based and it depends on who is processing the personal information and for what purposes. In their view what is needed for data protection is a 'deep, comprehensive and multidisciplinary examination of privacy in the information age, and this suggested approach involves assessing privacy in a manner that accounts for implications of technology, law, economics, business, social science and ethics.'[130] Even though privacy is contextual, it is deserving of protection because the loss of privacy often results in harm to individuals, to groups, and even to society as a whole. They agree that a balancing test is needed and emphasize that the test should account for context and nuance.[131]

Current legislative debate involves a discussion about whether data protection should be viewed as a separate individual right to solidify the safeguards needed to protect personal data or whether data protection should be interpreted as a part of the right to privacy. Banisar and Davies suggest that privacy can be divided into four separate, but

[130] Op cit note 3, see *Engaging Privacy and Information Technology in a Digital Age* at 3 – 14.

[131] Op cit note 3, see *Engaging Privacy and Information Technology in a Digital Age* at 12-14.

related concepts; *one: information privacy which involves rules for the handling of personal data through mechanisms of choice and consent*; two: bodily privacy which protects our physical selves against invasive procedure, this includes assault laws and searching procedures; three: privacy of communications which involves security of mail and telephone conversations; and four: territorial privacy which sets limits on the intrusion of one's property rights.[132]

Protecting the privacy of information about oneself does indeed stem from the right to privacy and this falls neatly into the first category of Banisar and Davies's theory on privacy, but data protection is somewhat broader and should not be limited only to the notion of privacy. This is because it covers the handling of personal data notwithstanding consent and focuses on legal parameters to avoid potential infringement on a number of other human rights (e.g. privacy, non-discrimination, freedom of movement); to ensure that personal data is kept secure and used for lawful, fair and clearly defined purposes; to prevent the pursuit of wide unlimited and unknown State interests that do not respect the individual's choice, consent and access and rectification rights, as well as confidentiality requirements; to ensure extra safeguards for special categories of sensitive personal data; and to avail the right to recourse to individuals in the event of unlawful data processing. Data protection extends to the right of an individual to choose under what circumstances to disclose personal data that is private and uniquely identifiable to that individual. Moreover, it

[132] Banisar, D and Davies, S (2000) 'Privacy and Human Rights: An International Survey of Privacy Laws and Developments.'

not only includes protecting privacy of the information after consenting to disclosure, it also involves setting conditions, safeguards and limitations for handling the information from the moment it is collected until it is erased or destroyed.[133] Kuner confirms that the concepts of 'data protection and privacy are twins but not identical. He says data protection law goes further as it seeks to give rights to individuals in how data identifying or pertaining to themselves are processed and to subject such processing to a defined set of safeguards.'[134]

Data protection defined

Data protection is a developing area of law, which stems from the right to privacy, but what exactly is data protection? Given the lack of a binding legal instrument on data protection, there is no international legal definition of data protection, nor is there a definition in the soft law instruments. In the Glossary on Migration it is defined in the migration context as 'the systematic application of a set of institutional, technical and physical safeguards that preserves the right to privacy with respect to the collection, storage, use and disclosure of personal data.'[135] This recognizes the right to privacy and goes further to include the different phases of handling personal data that equally require protection. Therefore, it can be described as an all-encompassing term that is used to describe the handling of personal data under safe parameters, thereby recognizing the need to collect and process personal data, while equally protecting the rights and interests of individuals.

---

[133] Op cit note 129, *Sources of Literature on Data Protection and Human Rights.*

[134] Kuner, Christopher (2009) 'An International Legal Framework for Data Protection: Issues and Prospects' at 4.

[135] Op cit note 2, *International Migration Law: Glossary on Migration* 2nd Edition at 25.

The Joint United Nations Programme on HIV and AIDS (UNAIDS) emphasize that data protection is not only about the right to privacy. It involves three interrelated concepts: 'First, *privacy* that is both a legal and an ethical concept. The legal concept refers to the legal protection that has been accorded to an individual to control both access to and use of personal information and provides the overall framework within which both confidentiality and security are implemented. Second, *confidentiality* that relates to the right of individuals to protection of their personal data during storage, transfer, and use, in order to prevent unauthorized disclosure to third parties. Third, *security* that is a collection of technical approaches addressing issues covering physical, electronic, and procedural aspects of protecting information collected.'[136] According to the South African Law Commission, data protection entails the legal protection of the data subject with regard to the processing of data concerning him, her or itself by another person or institution.[137]

Kuner says 'data protection can be regarded as a specific aspect of privacy that gives rights to individuals in how data identifying them or pertaining to them are processed, and subjects such processing to a defined set of safeguards.'[138] Thus, data protection can be seen as the handling of personal information that is uniquely identifiable to an

[136] Joint United Nations Programme on HIV/AIDS (UNAIDS) (2007) 'Guidelines on Protecting the Confidentiality and Security of HIV Information' at 22, Proceedings from a Workshop, 15-17 May 2006 Geneva.

[137] South African Law Reform Commission (2005) 'Privacy and Data Protection: Discussion Paper 109' at 1-4 and 24 <http://www.doj.gov.za/salrc/dpapers.htm>. The Discussion Paper followed an earlier Issue Paper on the same topic (SA Law Reform Commission *Privacy and Data Protection* (Issue Paper 24 August 2003)..

[138] Kuner, Christopher (2010) 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' at 12 <http://ssrn.com/abstract=1689483 or http://dx.doi.org/10.2139/ssrn.1689483>

individual and deemed confidential, and as stated by Cavoukian, 'it provides a baseline protection, particularly in terms of restricting secondary use of personal data, providing individuals with access rights and ensuring a mechanism for enforcement.'[139]

Data protection as a separate legal right

Additional legal safeguards are needed to cover the following data protection concerns, *inter alia*, unlawful and unfair collection without the consent of the person, lack of data quality, collection of excessive categories of data, unclear purposes which are not communicated to the person at the time of collection or disclosure, inadequate confidentiality requirements, unsafe data storage and data security mechanisms, inappropriate and improper disclosure, and unauthorized use and access for purposes unrelated to the specified purpose. Thus, data protection needs to be a distinct right on its own as it goes further than the right to privacy as evidenced in the Charter on Fundamental Rights of the European Union (EU Charter). Article 8 sets out the right to data protection as follows:

Protection of personal data:

> 1. **Everyone has the right to the protection of personal data concerning him or her.**
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which

[139] Op cit note 27, *Privacy as a Fundamental Human Right vs. An Economic Right: An Attempt at Conciliation* at 27.

has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.[140]

The European Court of Human Rights has held that Article 8 is a fundamental human right. For example in *Rotaru v. Romania* the Court stated that 'Article 8 extends to confidential matters, such as medical and health data, sexual activity and orientation, family kinship and, possibly, professional and business relations and other intimate areas in which public intrusion would be an unwarranted encroachment on the natural barriers of self. Public activism in public political parties has little in common with the ratio which elevates the protection of privacy into a fundamental human right.'[141]

The European Charter is the only existing international legal instrument that explicitly recognizes data protection as a fundamental human right. While data protection may not yet be recognized as such at the international level, data protection itself encompasses the right to privacy which is recognized already as a fundamental human right and is accepted by many countries as echoed in their constitutions or freedom charters. Just as in Europe, international law needs to develop to keep up with the rapid growth of technology because this has a direct impact on individual rights. To give effect to data protection as a legal right, legislation needs to be enacted to give it

[140] Charter on Fundamental Rights of the European Union, 2000.

[141] European Court of Human Rights, *Case of Rotaru v. Romania* (Application no. 2834/95) Judgement, Strasbourg, 4 May 2000 at 6.

force as a statutory right as seen in the growing body of national data protection laws. Since States are recognizing the need for data protection laws, it is an opportune time to establish a binding legal instrument at the international level as recommended by the 31st International Conference on Data Protection and International Commissioners.[142] Commentary on the Resolution resulting from the international conference is covered in the next section.

Countries are increasingly enacting laws to give effect to their international obligations under the International Covenant on Civil and Political Rights (1966) amongst others and this includes protecting the right to privacy, but they need to go further at the international level, to establish adequate legal regimes confirming the legal right to data protection and facilitating the transborder flow of information in line with the EU Directive. What is clear is that the information age has placed us at a crossroads because personal data is now easily transferable and the right to privacy and data protection in national legislations can no longer be confined to geographical borders.

3.2 *Data Protection Laws*

> *'Data protection law is an important part of preserving personal privacy rights, which otherwise could be easily overwhelmed by the power of*

[142] Op cit note 12, *The Madrid Resolution International Standards on the Protection of Privacy and Data Protection.*

government agencies and corporations that hold information about individuals'.[143]

This section examines the international legal instruments on privacy and data protection rights and highlights the cross-border dimension of data protection with reference to the core Data Protection Principles governing the collection, use, disclosure, storage and disposal of personal data. It should be noted that this section, to some extent, overlaps with the preceding section which sets the theoretical argument for protecting data protection as a human right.

Soft law on data protection

The United Nations Guidelines for the Regulation of Computerized Personal Data Files (1990)[144] sets the international standards on data protection, albeit without legal force. The UN Guidelines, draws on the Data Protection Principles as set out in the Council of Europe and European Union legal instruments, the OECD Guidelines, but it fails to oblige States to enforce data protection as a legal right due to its non-binding nature. While it encourages the UN member states as well as governmental, intergovernmental and non-governmental organizations to respect the Guidelines when carrying out activities within their field of competence, it has carried little weight because it does not create any obligations to follow the Guidelines. In its overview of the existing data protection instruments around the world, the South African Law

[143] Open Rights Group 'Data Protection' <https://www.openrightsgroup.org/issues/data-protection>

[144] Guidelines Concerning Computerised Personal Data Files adopted by the UN General Assembly on 14 December 1990, Doc E/CN.4/1990/72 20.2.1990.

Commission stated that the UN Guidelines has had much less influence on data protection regimes than the other instruments even though its intention was to influence States to enact data protection laws.[145]

International trends of humanitarian actors

The United Nations agencies and other international organizations[146] generally adhere to the standards set in the UN Guidelines. International intergovernmental organizations are not subject to national laws due to their privileges and immunities accorded to it by its member states. Instead, they establish their own policies that form part of their internal laws. According to Amerasinghe 'international organizations have as a characteristic that with respect to their internal organization and functioning they are outside the jurisdiction of national law. Their life is governed by a set of rules and principles, which constitute their internal law.'[147] In establishing their internal laws, international organizations look to both hard and soft law at the international level.

From informal discussions at the 4th International Data Protection Workshop it seems that there are a number of agencies contemplating developing specific internal policies on data protection because more detail is required than provided in the UN

[145] Op cit note 137, 'Privacy and Data Protection: Discussion Paper 109' 6-12.

[146] Relevant agencies operating in migration context include the United Nations High Commissioner for Refugees (UNHCR), the United Nations Office of the High Commissioner for Human Rights (OHCHR), the United Nations Children's Fund (UNICEF), the United Nations Office for the Coordination of Humanitarian Affairs (OCHA), the International Labour Organization, the International Organization for Migration, the International Committee of the Red Cross (ICRC), the World Health Organization (WHO) and the World Intellectual Property Organization (WIPO).

[147] Amerasinghe, C F (2005) *Principles of the Institutional Law of International Organizations* at 272.

Guidelines.[148] It is surprising that UN agencies have taken 20 years, following the incident that occurred during the Rwanda Genocide as mentioned in chapter 1.3 above, to place data protection on their agendas and to establish internal rules that govern the handling of personal data collected and processed within the scope of their mandates. Nonetheless, it is a welcomed initiative because once established it would help shape the international legal framework on data protection through capacity building initiatives, and this would in turn, encourage States to place data protection on their legislative agendas.

The United Nations High Commissioner for Refugees (UNHCR) has an internal policy generally covering confidentiality of refugee information which refers to the UN Guidelines, but they are still in the process of developing a specific policy on data protection, most likely to be in force only in the latter part of 2014.[149] This incentive stems from the UNHCR ExCom Conclusion No. 91 (LII) (2001) on Registration of Refugees and Asylum-Seekers which stresses the 'confidential nature of personal data and the need to protect confidentiality whilst recognizing that the appropriate sharing of some personal data in line with data protection principles can assist States to combat fraud, to address irregular movements of refugees and asylum-seekers, and further to identify those not entitled to protection under the 1951 Convention and/or 1967 Protocol on refugee protection.'[150] Similarly, even though the International

[148] The 4th International Data Protection Workshop organized by the European Data Protection Supervisor and the World Customs Organization, Brussels, 8-9 November 2012.

[149] Informal discussions with Beck, Alexander, Senior Legal Officer at the Department of International Protection, UNCHR Headquarters conducted in Brussels on 8 November 2012.

[150] United Nations High Commission for Refugees (2003) 'Comments on the Source Country Information Systems (SCIS) of the International Centre for Migration Policy Development (ICMPD).'

Committee for the Red Cross (ICRC) has a dedicated department to data protection, they are still in the process of developing a comprehensive policy covering beneficiary data.[151]

The Joint United Nations Programme on HIV and AIDS (UNAIDS) has Guidelines on Protecting the Confidentiality and Security of HIV Information which emphasize that data protection involves three interrelated concepts, namely privacy, confidentiality and security, all of which have an impact on the development and implementation of the protections available for securing sensitive personal data. In the scope of their work the 'public health goal of safeguarding the health of communities through the collection, analysis, dissemination, and use of health data, has to be carefully balanced with the individual's right to privacy and confidentiality and there is a need to have specific guidelines in place that are based on human rights principles.[152] In addition, the balancing test in the HIV context requires maximizing of benefits of data collection and protection from harm that can result from either malicious or inadvertent and inappropriate release of individually identifiable data.'[153]

The International Organization for Migration (IOM) has a policy as well as detailed guidelines, which are available publically in the IOM Data Protection Manual. The manual is comprehensive in providing guidance to organizations collecting and

[151] Informal discussions with Bircher, Romain, Head of Data Protection Unit, ICRC Headquarters conducted in Brussels on 8 November 2012.

[152] Op cit note 136, 'Guidelines on Protecting the Confidentiality and Security of HIV Information' at 2.

[153] Ibid, 'Guidelines on Protecting the Confidentiality and Security of HIV Information' at 6-10.

processing personal data of migrants and IOM has been active in advising governments when strengthening their data protection laws to apply it equally to migrants.[154] The manual recommends that a risk-benefit assessment be conducted prior to data collection taking all surrounding circumstances into account, including *inter alia*, the prevailing social, cultural and religious attitudes of the target population group or individual data subject.[155] This means weighing the probability of harm against the anticipated benefits and ensuring that the latter significantly outweighs the potential risks. It also recommends conducting a sensitivity assessment to identify the categories of personal data needed for the specified purpose and to determine whether stricter data protection safeguards should be applied throughout the lifecycle of the data processing. The manual also states that data controllers should always put themselves in the shoes of the data subject and consider 'How would a reasonable person, in the position of that data subject, react to the data collection and data processing practices?'[156] While the guidelines in this manual are indeed useful, as illustrated in chapter 2, there are new issues arising from advance technology such as crisis mapping that pose a threat to the protection of migrant data.[157]

The International Criminal Police Organization-Interpol has published Rules on the Processing of Data adopted by its member states in 2011. The Rules aim to ensure international cooperation between criminal police authorities with due respect for the

---

[154] Informal interview with Perruchoud, Richard, former Legal Advisor at the Legal Affairs and International Migration Department, IOM Headquarters conducted in Geneva.

[155] Op cit note 5, *IOM Data Protection Manual* at 16.

[156] Ibid, *IOM Data Protection Manual* at 16-18.

[157] For an analysis of the IOM Data Protection Manual, see: Meier, Patrick 'On Crowdsourcing, Crisis Mapping and Data Protection Standards, iRevolution, February 2012 <http://irevolution.net/2012/02/05/iom-data-protection/>

basic rights of individuals afforded under the 1948 Universal Declaration of Human Rights. A concerning issue with this policy is that the consent principle is absent and it allows for exchange of data among Interpol's member states with further disclosures to national central bureaus who are allowed access to the Interpol Information System to use personal data for broad police purposes.[158] Nonetheless, the Interpol Information System is an impressive data security tool and the confidentiality requirement, which is a fundamental rule, is underscored by a risk analysis and classification of categories of confidentiality. The absence of the consent principle is problematic because migrants would have no opportunity to decide whether or not they would want their personal data that have been collected by Interpol to be accessed by their governments who are member states to Interpol.

Model regional data protection law

Data protection as a legal right is rooted primarily in the European jurisdiction. The European data protection model has the most comprehensive legal framework that developed as a response to the challenge of exchanging personal data across borders. Most recently on 22 October 2013, the European Parliament voted in favour of the European Commission's Data Protection Reform which aims at strengthening, *inter alia*, privacy and data protection rights to ensure that such rights are not eroded by the ever increasing interests of the State and private entities.[159] This turns the focus to the legal instruments in Europe.

---

[158] De Villenfagne, Florence and Gayrel, Claire (2011) 'Data Protection at ICPO-Interpol: Assessments, Issues and Outlook,' at 11.

[159] European Commission 'LIBE Committee vote backs new EU data protection rules' European Commission Press Release, 22 October 2013 <http://europa.eu/rapid/press-release_IP-12-46_en.htm>

Article 8 of the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms[160] states that: '(1) Everyone has the right to respect for his private and family life, his home and his correspondence, and (2) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.' The 1950 Convention created the European Commission of Human Rights and the European Court of Human Rights to oversee the enforcement of rights. Both have been particularly active in the enforcement of privacy rights and have consistently viewed protections in Article 8 expansively and the restrictions narrowly.[161]

EU Directive

The 1995 European Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (EU Directive) aims to facilitate data exchange in Europe and the 1981 Council of Europe Convention aims to facilitate the trans-border flow of information while also protecting privacy rights; the latter is the only legally binding document at

[160] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950.

[161] Privacy International 'Privacy & Human Rights' 28 May 2007.
<http://www.privacyinternational.org >

supranational level and the former obliges European Union member states to transpose the EU Directive into national law in each country.[162] The EU Directive was the legal instrument that regulated data protection for the first time under European Union law and it is by far the most comprehensive and leading legal instrument on data protection.

The EU Directive has been developed for the dual purpose of introducing parameters for the lawful and fair collection of personal data and for the sharing and free flow of such data across borders. It aims to harmonize data protection laws in the European Union by regulating the processing of personal data under conditions of transparency, legitimacy and proportionality.[163] Moreover, advisory bodies called 'Data Protection Authorities' have been established to ensure that laws are implemented properly. Necessary data protection safeguards that are introduced through the law include the common Data Protection Principles which aim to ensure that personal data is collected lawfully and fairly with the consent of the individual and used confidentially for a specified purpose under the guarantee of applying safe data security measures, even if transferred across borders. It serves as a model for good practice both within and outside Europe, and to date inspired over 70 countries to develop its own data protection laws that conform to the European and international standards, and this number is steadily increasing.[164] While examining conflicts of the proprietary right of

[162] See the objectives of the Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data and the EU Directive.

[163] See overview of the EU Directive: <http://en.wikipedia.org/wiki/Data_Protection_Directive>

[164] Op cit note 5, *IOM Data Protection Manual* at 196-107 for a global overview of national data protection laws in force at its date of publication. This number has increased and there are a number of countries at a similar stage as South Africa where comprehensive data protection laws are looming. See

data and the right to privacy, Campbell and Bàn highlight the need for harmonization of national policies to encourage the flow of information. Bygrave examines the rationale, logic and limits of data protection law and questions the interests that this law purports to protect. He says most of the laws are general broad framework laws, and 'instead of stipulating in casuistic fashion detailed provisions for regulating the processing of personal information, they set down rather diffusely formulated general rules for such processing, thereby allowing for the subsequent development of more detailed regulatory norms as the need arises in the form of codes or regulations.[165]

Data protection is a well-developed area of law in Europe dating back to the 1980s and 1990s. The Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data and the Council of Europe's Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981) established the modern parameters for the principle-based regulation and security of personal data.[166] The most comprehensive piece of legislation on data protection, however, remains the EU Directive. At the time of its promulgation, the main objective of the EU Directive was to create a legal basis to facilitate the transborder flow of personal data without impeding on existing individual rights. Protection of

---

also op cite note 13, *Data Protection Laws of the World* for an assessment of countries and their legal developments with to respect data protection laws.

[165] Bygrave, Lee A 'An International Data Protection Stocktake at 2000: Part 1: Regulatory Trends' (2000) 6 *Privacy Law & Policy Reporter* 129 at 130.

[166] Knoppers, Bartha Maria (2000) 'Confidentiality of Health Information: International Comparative Approaches' in *Protecting Data Privacy in Health Services Research* National Academy of Sciences, Washington DC < http://www.nap.edu/openbook.php?record_id=9952&page=173 >

personal data was a by-product of the data transfer objective and introducing an obligation for States to have adequate laws in force to protect personal data reinforced this secondary data protection objective. The requirement to ensure that adequate laws are in place prior to transfer is what has caused the growth of laws outside Europe in line with the EU Directive. Currie and Allan say that 'adequacy can be taken to mean equivalence. This means that EU member states need to be satisfied that personal data can safely be transferred to a third state provided it provides legal protection that is roughly the equivalent of the EU regime. In addition, the level of adequacy of protection is assessed in light of all the circumstances surrounding a data transfer or set of data transfer operations and particular considerations are given to the nature of the data; the purpose and duration of the proposed processing operation or operations; the country of origin and country of final destination; the rules of law, both general and sectorial, in force in the third country in question; as well as and the professional rules and security measures which are complied with in that country.'[167]

EU data protection reform

Even though it is currently the global model on data protection, the European Commission recently proposed a revision of the EU Directive, calling for stronger provisions on individual rights in light of rapid technological change.[168] After a review of the current legislative framework, the European Commission confirmed that the

[167] Op cit note 15, 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa' at 572.

[168] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions on Migration 'A Comprehensive Approach on Personal Data Protection in the European Union' COM (2010) 609 final 9, Brussels, 4 November 2010 <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf>

existing Data Protection Principles are still valid and that its technologically neutral character should be preserved. However, an increase in legal clarity is needed to make data controllers aware of the implications of advanced technology on individual rights and to ensure that the Data Protection Principles are enforced effectively.[169]

The focus of the EU data protection reform is to enhance data protection rights, particularly since the EU Directive was initially developed with the objective of facilitating the trans-border flow of personal data at a time when the internet was at its infancy.[170] There is now strong support among EU countries to strengthen the protection of personal data relating to individuals, increase transparency and awareness of rights for data subjects, enhance notions of privacy through data protection impact assessments and using technology to protect privacy, re-examine categories of sensitive personal data and its prohibitions, protect the 'right to be forgotten' (i.e. to have no trace to the individual online) and the right of portability (i.e. to allow individuals to transfer personal data among service providers) and reinforce the power of Data Protection Authorities by reallocating resources to ensure effective provision of remedies and sanctions.[171] It aims at creating one single set of rules to be applicable to all countries across Europe as well as to European companies outside Europe. It also introduces a 'notification obligation' for companies to notify the Data Protection Supervisory Body within 24 hours of any breach or infringement on the rights of individuals and strengthens the role of the Data Protection Supervisors

[169] Ibid, 'A comprehensive approach on personal data protection in the European Union'

[170] See the European Commission website for the latest updates on the EU data protection reform <http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm>

[171] Op cit note 168 'A Comprehensive Approach on Personal Data Protection in the European Union' at 7-14.

appointed throughout Europe.[172] This lends itself to a human rights based approach with an objective to elevate respecting individual rights to the same level as facilitating the interests of State bodies and private companies. This objective of balancing the rights of individuals and interests of States can be achieved by ensuring legal protections for both.

Data protection a sui generis right

The European Court of Human Rights has given strong recognition to the Data Protection Principles and data protection is increasingly seen as a *sui generis* right, given its expression in the EU Charter of Fundamental Rights of the European Union.[173] The EU data protection model finds its strength in the explicit provision in Article 8 of the Charter of Fundamental Rights of the European Union (2000) (EU Charter) that provides for the right to data protection.[174] This confirms that data protection is a fundamental human right available to all individuals in the European Union and it confers an obligation on all EU member states to uphold the right. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) (CoE Convention) builds on Article 12 of the Universal Declaration of Human Rights, which sets out the simple premise that privacy is a

[172] European Commission 'Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of their Data and to Cut Costs for Businesses' European Commission Press Release, 25 January 2013 <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en>

[173] Hammarberg, Thomas 'Protecting the Right to Privacy in the Fight against Terrorism', Council of Europe Commissioner for Human Rights, Strasbourg, CommDH/IssuePaper (2008) 3 at 5. <https://wcd.coe.int/ViewDoc.jsp?id=1469161>

[174] Article 8 states that: '(1) Everyone has the right to the protection of personal data concerning him or her, (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified, and (3) Compliance with these rules shall be subject to control by an independent authority.

fundamental human right entitled to protection under the law and it gives effect to Article 8 of the EU Charter.[175] The European Commission recognizes that the CoE Convention is currently the sole international treaty with a binding character and it has as a result opened it to non-EU member states for signature. However, this has not been as successful and even though it is binding on 27 EU member states and the three member countries in the European Economic Area, it is unlikely that the CoE Convention will become *the* global binding international instruments on data protection.[176]

Need for global harmonization

The UN Guidelines were promulgated because it was difficult to reach international consensus to create a binding law due to existing data protection laws around the world that either follow the EU Directive or the 1980 OECD Guidelines and the APEC Privacy Framework, thereby creating problems for global harmonization. Kuner argues that it is this very disparity that calls for a global legal instrument and this is what led to the Madrid Resolution.[177] National laws around the world that don't follow the EU model, draw on the OECD Guidelines and APEC Privacy Framework which focus more on a regulatory framework and provides a non-binding set of principles that member states may enact. The emphasis is still on 'achieving acceptance of certain minimum standards of privacy and personal data protection, and of eliminating, as far as possible, factors which might induce countries to restrict

[175] Op cit note 122, 'Data Protection Day: Joint High Level Meeting From European to International Standards on Data Protection, Remarks of Marc Rotenberg'.

[176] Op cit note 138, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' at 16-18.

[177] Ibid, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' at 25.

transborder data flows for reasons associated with such flows.[178] The Council of Europe Commissioner for Human Rights stressed that 'the Data Protection Principles in the EU Directive must be construed as fundamental, constitutional human rights principles, and applied in accordance with the case law of the European Court of Human Rights which interprets data protection as a fundamental human right.[179] Since Europe has vast knowledge in this area, the drafters of an international legal instrument could draw from the European data protection model for guidance.

A known concern with the EU data protection model is that it has been difficult to enforce compliance with the law because of jurisdictional boundaries. Even though a global legal instrument will not cure this, it will create harmony by imposing legally binding obligations and requiring the transposition of data protection safeguards into national laws worldwide. This is also relevant to migrants who travel across borders. It is therefore important that the provision allowing recourse to Data Protection Supervisory Authorities are applied without distinction and that it applies equally to persons within the territory who will have equal protection before the law, regardless of their nationality or immigration status.

Kruner states that one of the arguments for the EU Directive requirement of adequate laws prior to data transfer was the concern for creating data havens, that is, transferring personal data outside the protective framework in the European Union to

[178] Ibid, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' at 16.

[179] Op cit note 173, 'Protecting the Right to Privacy in the Fight against Terrorism' at 6.

third countries to circumvent legal protections. However, there has been little evidence that data havens are a reality and with the increase of national laws this is less of a concern.[180] The creation of a global legal instrument will further do away with this concern because there would be a minimum standard that all States would have to comply with, whether or not, national data protection laws are already developed. Kuner warns that international harmony will depend on international cooperation and the need for countries not to extend their reach across borders as this will result in friction. This, he says, can be avoided if data protection is viewed as a human right and not merely as a commodity.[181] What governments need to realize to reach international consensus is that data transfer is an advantage to a globalized economy and promoting data protection as a right can facilitate this. Kuner argues further that 'the economic, legal, and social importance of data protection is a niche area of interest to only data protection and privacy specialists, and it is not adequately recognized by the governments. Ministers and government officials at the highest levels need to grant international data flows the same attention as they do to international flows of capital and international trade.'[182] Indeed, this will help to put data protection on the political, policy and legislative table.

Madrid Resolution

The Madrid Resolution includes the commonly accepted Data Protection Principles

[180] Op cit note 138, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' at 31.

[181] Ibid, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' at 43.

[182] Ibid, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' at 8 – 9.

and the appointment of Data Protection Supervisory Bodies with the power to set conditions for allowing data transfer to countries with existing data protection laws or on the basis of industry codes or contractual clauses. Since this is much in line with the EU data protection model, which recognizes data protection as a fundament human right, a global law could similarly have the quality of a legally binding human rights instrument.[183] Moreover, the shift toward focusing on responsibilities of the data controller as seen in Europe is compatible with viewing data protection as a human right because it allows remedies to individuals in the event of breach. Thus, creating a data protection law in the human rights framework will make it more difficult for States and private companies to circumvent the rights of individuals at the expense of State interests and economic interests.

Even though there will be an inevitable tension between States since most existing laws are based on territorial needs and national legal frameworks, the Madrid Resolution proposes to codify the already commonly accepted Data Protection Principles and make them universal. It also provides useful guidance to create harmonization across borders by defining the form of the legal framework on data protection to be introduced by States, the standards on which it would be based and the scope thereof, and agreement on the appointment of international organization to assist in implementation.[184] Kuner says that since data transfer involves both benefits and risks it is important that the following measures be implemented to avoid inherent

[183] Ibid,'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' at 27.

[184] Ibid, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' at 35- 39.

threats to privacy and data protection: ensuring pro-active compliance with the law (such as the promotion of privacy audits), granting sufficient resources and enhanced enforcement powers to Data Protection Authorities, and enacting rules to ensure the legal accountability of the parties involved in transferring personal data.[185]

Rotenberg emphasizes that the Madrid Declaration resulted from discussions on the need for an international framework on data protection with the 'full participation of civil society, based on the rule of law, respect for fundamental human rights and democratic debate.'[186] However, the problem is that States and legislators where not at the table for this discussion which leaves a big gap.[187] The International Conference of Data Protection and Privacy Commissioners involved data protection stakeholders in Europe Canada, Latin America, Australia, New Zealand, Hong Kong, Japan and other jurisdictions in the Asia-Pacific region, mostly privacy experts and the Data Protection Authorities or the equivalent bodies responsible for guaranteeing data protection and privacy.[188] The Department of Privacy Office and the Staff of the United States Federal Trade Commissioner noted that international conventions typically cover a narrow issue with broad consensus while the Madrid Resolution covers an extremely broad array of issues with which there is narrow consensus, yet it is a good starting

[185] Ibid, 'Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future' at 41.

[186] Op cit note 122, 'Data Protection Day: Joint High Level Meeting From European to International Standards on Data Protection, Remarks of Marc Rotenberg'.

[187] Department of Homeland and Security (DHS) (2010) 'Comments by the DHS Privacy Office and the Staff of the U.S. Federal Trade Commissioner on the Joint Proposal for International Standards on the Protection of Privacy with regard to the Processing of Personal Data' at 4.

[188] The Madrid Resolution 'International Standards on the Protection of Personal data and Privacy' the International Conference of Data Protection and Privacy Commissioners, 5 November 2009 < http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/24464/20091.pdf>

point for discussions on the feasibility of a global legal instrument.[189] Indeed a comprehensive approach involving dialogue between all stakeholders from both the private and public sector is necessary to ensure global consensus.

Draft international law on data protection

As evidenced by the 31st International Conference on Data Protection and Privacy Commissioners, there is a need to strengthen the international character of data protection through the adoption of a universal and binding international instrument. At this conference, a resolution was adopted on a *Joint Proposal for Setting International Standards on Privacy and Personal Data Protection.*[190] The objectives of allowing for the cross border flow of information and establishing Data Protection Supervisory Bodies to monitor data protection practices, while at the same time protecting privacy, confidentiality of personal data and anonymity of individuals is echoed in national laws that do exist and there is no reason why this dual objective cannot remain in a legally binding instrument at international level. To ensure a uniformed approach the Draft Law identifies the core Data Protection Principles that has already received international consensus together with rights, obligations and procedures that should become legally binding. Accordingly, personal data should be processed:

> a. fairly, lawfully and in a proportionate manner in relation to specific, explicit and legitimate purposes;

[189] Op cit note 187, 'Comments by the DHS Privacy Office and the Staff of the U.S. Federal Trade Commissioner on the Joint Proposal for International Standards on the Protection of Privacy with regard to the Processing of Personal Data' at 2 - 3.

[190] Op cit note 12, *The Madrid Resolution International Standards on the Protection of Privacy and Data Protection.*

b. on the basis of transparent policies, informing adequately the data subjects and without any arbitrary discrimination against them;

c. ensuring the accuracy, the confidentiality and the security of the data as well as the legitimacy of the processing, and the rights of data subjects to access, rectification, erasure of data and to object against their processing;

d. implementing the principles of accountability and liability, even if the processing operations are carried out by service providers on behalf of the controller;

e. offering more appropriate guarantees where the data are sensitive;

f. ensuring that personal data transferred internationally benefits from the level of protection provided by the above-mentioned set of standards,

g. subject to the monitoring of independent and impartial supervisory authorities provided with adequate powers and resources also in connection with their duty to cooperate among themselves;

h. in a new and modern framework of proactive measures, such as those oriented in particular to prevent and detect breaches and based on the appointment of privacy officers as well as on efficient audits and privacy impact assessments.[191]

The Draft Law seeks to reflect the many approaches to data protection by integrating legislations from five continents with the view to create one binding legal instrument. The purpose is two fold: firstly, to define a set of principles and rights guaranteeing the effective and internationally uniform protection of privacy with regard to the processing of personal data; and secondly, to facilitate flow of personal data needed in a globalized world. It would be useful if the first purpose could be narrowed to data protection specifically because privacy definitions differ in various jurisdictions, whereas most States would welcome a universal definition of the right to data

[191] Ibid, *The Madrid Resolution International Standards on the Protection of Privacy and Data Protection* at 31.

protection. Kuner agrees that since 'privacy is a broader concept than data protection, it would seem more practical to limit the scope of a legal instrument to data protection.'[192]

It is clear that a human rights approach is included in the text of the draft because unlike existing data protection laws, the emphasis is on creating uniform protection of personal data as the primary objective and facilitating of personal data as the secondary purpose. In addition, States are given the freedom to supplement the minimum level of protection with additional measures to better guarantee data protection. Restrictions are allowed in the interests of national security, public safety, for the protection of public health, or for the protection of the rights and freedoms of others, provided such restrictions are necessary in a democratic society and it is outlined in national legislation to appropriately guarantee and preserve the rights of the data subjects.

The Department of Privacy Office and the Staff of the United States Federal Trade Commissioner rightfully point out that the provision relating to national security is problematic because it will lead to inconsistent exceptions due to differing legal frameworks and cultural differences.[193] This is because different jurisdictions may make different determinations as to whether there is a credible risk to national

[192] Kuner, Christopher (2009) 'An International Legal Framework for Data Protection: Issues and Prospects' at 6.

[193] Op cit note 187, 'Comments by the DHS Privacy Office and the Staff of the U.S. Federal Trade Commissioner on the Joint Proposal for International Standards on the Protection of Privacy with regard to the Processing of Personal Data' at 4 - 8.

security. To cure this, clear criteria for the exceptions should be embedded in the law to ensure uniformity. A safeguard embedded in the law is the principle of proportionality which provides that: '1) The processing of personal data should be limited to such processing as is adequate, relevant and not excessive in relation to the purposes, and 2) The responsible person should make reasonable efforts to limit the processed personal data to the minimum necessary. Interestingly, it has a provision for a 'processing service provider' defined 'as any natural person or organization, other than the responsible person that carries out processing of personal data on behalf of such responsible person.' This makes it clear that outsourcing of State obligations to private companies would, for example, not detract from the obligations that will be applicable to those companies acting as *de facto* State agents. A right to object by the data subject based on the particular personal situation of the person is introduced as well as an explicit duty of confidentiality that extends beyond expiration of the legal relationship between the data subject and the data controller.

To cover countries that lack existing data protection laws, contractual clauses in the form of bilateral agreements are allowed and cooperation agreements between appointed Data Protection Supervisory Bodies are encouraged to ensure effective application of the law. There are also proactive measure for compliance and provisions for liability and remedies; however, this should be carefully applied because it should not give rise to double damages if remedies are available in national laws. As per the explanatory notes to the Draft Law, 'the conference correctly considered the rights to data protection and privacy as fundamental rights of individuals, *irrespective of their nationality or residence*, while noting that the persisting data protection and privacy

disparities in the world, in particular due to the fact that many States have not yet passed adequate laws, harm the exchange of personal information and the implementation of effective global data protection.'[194] It is therefore clear that the drafters intended to have the law applicable to migrants crossing borders.

To date the task to develop an international treaty has indeed been challenging. The *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data* is a big step that brings the international community closer to achieving this goal. The regulation of cross border data protection issues is an area of law where international cooperation and coordination can come together to address these issues from a global private international law perspective.[195] However, it is not limited to international private law, data protection is a mixture of various legal areas, such as human rights law, public law, private law, amongst others.[196] If seen in this way, it also caters for the intersection with migration. It is understandable that drafters require time, but the societal needs today are far too great to lag behind and legislators need to act in hast to keep up with the growth in advanced technology that are impacting on existing individual rights. Back in 2009 Kuner was of the opinion that a legally binding instrument on data protection was premature and suggested alternative harmonizing

[194] Op cit note 12, *The Madrid Resolution International Standards on the Protection of Privacy and Data Protection* at 33.

[195] See Permanent Bureau (2010) 'Cross-border Data Flows and Protection of Privacy' Note submitted by the Permanent Bureau, Hague Conference on Private International Law <http://www.hcch.net/upload/wop/genaff2010pd13e.pdf>

[196] Op cit note 192, 'An International Legal Framework for Data Protection: Issues and Prospects' at 26.

instruments including a model or uniform law that States can enact into their national law.[197]

A model law is worth pursuing as good practice guidance, but what we need is legally binding obligations to ensure that such a model is transposed into national laws. Soft laws at international level are no longer sufficient and if States agree to international law obligations it can apply in the interim while country-specific laws are developed to take account of the complexities and legal regimes in different countries. Since States are increasingly interested in migrant data, it is important that data protection for migrants form part of the legislative process. This leads to a discussion on human rights framework and its extension to migrants.

3.3 *International Legal Instruments on Human Rights*

> '*We stand today at the threshold of a great event, both in the life of the United Nations and in the life of mankind. The UDHR may well become the International Magna Carta of all men everywhere.*' [198]

This section provides an overview of the legal instruments on human rights, following

[197] Ibid, 'An International Legal Framework for Data Protection: Issues and Prospects' at 9-12.

[198] Rooseveld, Eleanor 'Address to the United Nations General Assembly on the adoption of the Universal Declaration of Human Right' Paris, 9 December 1984 in Rehman, Javaid *International Human Rights Law* (2010) at 75.

the argument in the preceding section that data protection as an established legal right should find itself within the framework of this body of law, and emphasizes that States are obligated to ensure respect for the human rights of all migrants.

Customary law

Even though the 1948 United Declaration of Human Rights (UDHR) is a declaration with soft law force, over time, its substantive provisions have become customary law. To be considered customary law, the two key elements of: (1) State practice and (2) belief that such practice is binding amounts to law (*opinio juris*) must be proven.[199] Rehman and others confirm that most international lawyers agree that these two elements have been met, firstly it is widely accepted that the rights in the UDHR are acknowledged by most States as international norms, and secondly, the *opinion juris* is overwhelmingly evident in the text and *travaux prepatoires* of the United Nations (UN) Charter.[200] The preamble of the UN Charter 'reaffirms faith in fundamental human rights and in the equal rights of men and women' and Article 1(3) states that 'one of the purposes of the UN is to achieve international cooperation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction.' The incorporation of the UDHR into the UN Charter and its recognition by the 193 countries as member states to the UN demonstrates that the Charter is the leading international treaty recognizing the universal protection of human rights. It is also evident in the preambles of regional legally binding

[199] Rehman, Javaid (2010) *International Human Rights Law* at 79 – 80.

[200] Ibid, *International Human Rights Law* at 79.

instruments throughout the world, further replicated in national constitutions, and treated as binding in court jurisprudence at national, regional, and international level.[201]

Steiner says 'no one document received the same moral and rhetoric force, or has exerted as much influence on the human rights movement throughout history. It is the parent of the International Conventions and the grandfather to many specialized treaties.'[202] International human rights law is *sui generis* (of a unique character) in that it focuses on legal order based on the good towards all individuals within the jurisdiction of a State.[203] A human rights based approach is therefore an affirmation of the basic and fundamental human rights and principles as embodied in the UDHR where the individuals are the right holders and the State is the duty bearer.[204] In 1985 the member states to the UN adopted the *Declaration on the Human Rights of Individuals who are Not Nationals in the Countries in which they live*[205] which aims to, *inter* alia, reaffirm the purposes and principles of the UN Charter, and recognize that the protection of human rights and fundamental freedoms provided for in international instruments should also be ensured for individuals who are not nationals

---

[201] Ibid, *International Human Rights Law* at 81.

[202] Steiner 'Securing Human Rights: The First Half Century of the UNDH' Harvard Magazine, September – October 1998 in op cit note 132 *International Human Rights Law* at 83.

[203] Op cit note 199, *International Human Rights Law* at 14.

[204] Action Research on AIDS and Mobility, Global Alliance against Traffic in Women and International Women's Rights Action 'Report on Roundtable on using CEDAW to Protect the Rights of Women Migrant Workers and Trafficked Women in South and Southeast Asia' Kuala Lumpur, Malaysia, 6-9 May 2009

<http://www.iwraw-ap.org/publications/doc/Roundtable_on_Migration_and_Trafficking_report.pdf>

[205] Declaration on the Human Rights of Individuals who are Not Nationals in the Countries in which they live, (A/RES/40/144), 13 December 1985 <http://www.un.org/documents/ga/res/40/a40r144.htm>

of the country in which they live. Although this is a Declaration, it does signify the intention and commitment of the signatory States to afford human rights equally to all migrants. The UDHR outlines a wide range of rights which are traditionally classified into three generations of rights, namely: (1) civil and political first generation rights; (2) social, economic and cultural second generation rights, and (3) group/peoples third generation rights.[206] The right to privacy falls under the first generation rights focusing on the autonomous individual and protection from interventions by the State.[207] Human rights are indivisible and inherent to the dignity of every individual and therefore all human rights have equal status without any hierarchy.[208] Thus, the right to privacy, which encompasses data protection, should have equal respect to other guaranteed rights.

Positive law

Article 12 of the UDHR and Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR) guarantees the 'right to *everyone* to have their privacy, family, home or correspondence protected from arbitrary interference.' Similarly, Article 5 (1) (b) of the *Declaration on the Human Rights of Individuals who are Not Nationals in the Countries in which they live* states that 'Aliens shall enjoy, in accordance with domestic law and subject to the relevant international obligations of the State in which they are present, the right to protection against arbitrary or unlawful

[206] Op cit note 199, *International Human Rights Law* at 77.

[207] Sehmer, Carolin 'Report of the Parallel Event 'Third Generation Human Rights-Reflections on the Collective Dimension of Human Rights' Palais des Nations, Geneva, 22 March 2007 <http://www.academia.edu/1140272/_Third_Generation_Human_Rights>

[208] Op cit note 204, 'Report on Roundtable on using CEDAW to Protect the Rights of Women Migrant Workers and Trafficked Women in South and Southeast Asia.'

interference with privacy, family, home or correspondence.' Article 2 of the UDHR states further that '*everyone* is entitled to all the rights and freedoms, *without distinction of any kind.*' This is reiterated in Article 26 of the ICCPR which 'protects all persons from *discrimination on any ground* such as race, colour, sex, language, religion, political or other opinion, *national* or social origin, property, birth or *other status.*' Emphasis is added to the preceding provisions to illustrate that the right to privacy is a universal fundamental right afforded to all individuals, regardless of nationality or immigration status, and it extends to all migrants whether in a regular or irregular situation.[209]

The ICCPR is binding on the international community and even though some countries like South Africa have not ratified it, signing the Convention signifies its commitment to uphold the spirit and purpose of the provisions contained therein. Specific reference to privacy as a right can also be found in Article 14 of the International Convention on the Protection of All Migrant Workers and Members of their Families (1990) (MWA) affording the right to privacy to all migrant workers; in Article 10 of the Convention on the Rights of the Child (1989) (CRC) ensuring that the child has an equal right to privacy as an adult, and this is coupled with Article 12 which states that the views and opinions of the child should be given due weight according to the age and maturity of the child; and in Article 22 of the Convention on the Rights of Persons with Disabilities (2006) (CRPD) the right to privacy is

[209] Op cit note 32, *Migrant Workers in International Human Rights Law: Their Protection in Countries of Employment* and op cit note 5, *IOM Data Protection Manual* at 13.

guaranteed to persons with disabilities.[210] These international legal instruments essentially echo the right to privacy as stated in Article 12 of UDHR, without any difference in substance, except that Article 17 of the ICCPR adds the criteria of 'unlawful interference' to emphasize that any limitation to the right to privacy must be legitimate and embedded in the law.

The Human Rights Committee stresses, in General Comment No. 16 (1988), the importance of the right to privacy by stating that 'compliance with Article 17 (of the ICCPR) requires that the integrity and confidentiality of correspondence should be guaranteed *de jure* and *de facto*.'[211] As a result, States are obligated to adopt legislative and other measures to give effect to the prohibition against arbitrary interferences with the right to privacy and any interference by States have to be on the basis of an enacted law. In addition, the concept of 'arbitrariness' and 'unlawful interference' means that such interference should not only be provided by law, but it must be reasonable in the particular circumstance.[212] Specifically, 'the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or entities, must be regulated by law. To this end, effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not

[210] Even though South African only ratified some of the international treaties giving legal effect to the right to privacy, it signed all of them and is therefore obliged to act according to its spirit and intention. See chapter 5 below for further detail on the right to privacy in South African law.

[211] United Nations Human Rights Committee 'General Comment No. 16: *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Article 17), 04/08/1988, CCPR General Comment No. 16 (General Comments)*' Office of the High Commissioner for Human Rights <http://hria.equalit.ie/pdf/en/5/GC%2016%20-%20privacy%20EN.pdf>

[212] Ibid, 'General Comment No.16' at 4-8.

authorized by law to receive, process and use it, and that it is never used for purposes incompatible with the Covenant (i.e. ICCPR).'[213] This clearly supports the view that data protection is included in the right to privacy and it is also line with Banisar's argument in chapter 2.1 that data protection is one facet of the right to privacy.[214] Moreover, since human rights are afforded to all individuals without distinction, it also applies to migrants and thus privacy and data protection as fundamental human rights should be afforded equally to migrants.

Limitation on rights

Even though human rights are afforded to everyone, some rights are derogable and may result in different treatment between nationals and non-nationals. Any derogation from fundamental rights should, however, be based on reasonable and objective criteria and should be proportionate to meet a legitimate and justifiable need. The international human rights instruments state that the principle of necessity allows for limitations to rights, but this is not defined. Consequently, it has been given various interpretations, but in all interpretations it emphasizes the proportionate relationship between the right that needs to be protected and the importance of the objective to be achieved by limiting the right in question.[215] This proportionality between the right and the objective of the limitation stresses that measures taken pursuant to a derogation of a right must be taken 'to the extent strictly required by the exigencies of the situation,'

[213] Ibid, 'General Comment No.16 at 10,

[214] Op cit note 132, 'Privacy and Human Rights: An International Survey of Privacy Laws and Developments.'

[215] Op cit note 7, *Biometrics and International Migration* at 12.

which sets a strict standard of being absolute necessity.'[216] The rationale for this proportionality test is that any derogation cannot affect the essence of the right. This is evident in the Article 5 of the ICCPR which provides that: 'Nothing in the Covenant may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms recognized herein.' Higgens states that 'derogation does not mean an abolition of a right because while the State has leeway to derogate a right, the derogation clauses do not suspend the rule of law, instead they regulate the relationship between the rule and the exception.'[217]

Privacy not an absolute right

Giving effect to human rights through the enforcement of national laws stems from international obligations of States under international human rights law. As a result, the right to privacy is legally protected in many national jurisdictions, but it is not an absolute right. Individual privacy competes alongside other recognized rights and can be limited by the legitimate interests of States provided it is proportional, justified and necessary to meet a legitimate purpose.[218] The collection and processing of personal data, without the appropriate safeguards, can lead to a number of risks including, *inter alia*, infringement of the right to privacy and privacy, violation of confidentiality

---

[216] United Nations Human Rights Committee 'General Comment No 29: *States of Emergency (Article 4)*' U.N.Doc CCPR/C/21/Rev.1/Add.11 (2001), Office of the High Commissioner for Human Rights <http://www1.umn.edu/humanrts/gencomm/hrc29.html>

[217] Higgins, Rosalyn (1978) 'Derogations under Human Rights Treaties.'

[218] See chapter 5 for a detailed discussion on justifiable limitations to rights in the South African context.

requirements, migrant profiling and discriminatory treatment. It can also lead to limitations on freedom of movement and family unity, the right to seek asylum or contravention to the universal principle of *non-refoulement.*[219] If, for example, confidentiality of personal data of refugees is not adequately protected, it could impact on the right to seek asylum due to fear of reprisals and it could also jeopardize the asylum process because asylum seekers may be reluctant to disclose necessary information due to lack of confidence and trust. Therefore, policy-makers/legislators should ensure that migration law and policy giving effect to State sovereignty do not adversely affect human rights including the right not to be *refouled.* Accordingly, any derogation to the right of privacy and data protection for the purpose of the national security of the State 'must be necessary and proportionate to the exigencies of the situation and must not involve discrimination in their application.'[220]

Domestic data protection laws

Some States have taken steps to give expression to privacy and data protection through enactment of specific data protection laws. In the absence of any regional laws and due to the non-binding nature of the 1990 UN Guidelines for the Regulation of Computerized Personal Data Files, African countries like most countries look to the European data protection laws for guidance.[221] One might think that the Americas

[219] The principle of *non-refoulement* is in included in Article 33 (1) of the 1951 Geneva Convention relating to Status of Refugees which states that 'no Contracting States shall expel or return ("*refouler*") a refugee in any manner whatsoever to the frontiers of territories where his life or freedom would be threatened on account of his race, regional, nationality, membership of a particular social group or political opinion.'

[220] Op cit note 7, *Biometrics and International Migration* at 12.

[221] See further discussion on developments of data protection in the African context in chapter 5.

would have a regional legal instrument comparable to the CoE Convention and the EU Directive, but as stated by Thomas 'the United States, as a modern democracy, has the weakest laws in terms of data protection. The Supreme Court of the United States has found that its Constitution contains 'penumbras' that implicitly grant a right to privacy against government intrusion.[222] Although the United States is a signatory to the OECD Guidelines, which is non-binding, it has not implemented a data protection law at federal-level. Instead, data protection laws have developed on an ad-hoc basis through industry-specific codes of practice governed by a mix of legislation, regulation, and self-regulation.'[223]

Asian countries adopt similar practices to the United States by focusing on self-regulation that follows a set of guidelines. States mostly follow the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and 2005 Asia-Pacific Economic Cooperation (APEC) Privacy Framework, both non-binding in nature. More recently, the 2009 ASEAN Human Rights Declaration recognizes an explicit right to the protection of personal data in Article 21 which states that: 'Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence *including personal data*, or to attacks upon

[222] For example see *Griswold v. Connecticut* 381 U.S. 479 (1965).

[223] Op cit note 76, *Biometrics, International Migration and Human Rights* at 391. For a detailed overview of the legal regime on privacy and data protection in the United States, see also: Anneliese (2009) 'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study,' UNISA theses and dissertations at 27 - 150 <http://uir.unisa.ac.za/handle/10500/1463?show=full>

that person's honour and reputation. Every person has the right to the protection of the law against such interference or attacks.' However, this Declaration is not binding and has not yet had much influence in the development of data protection laws in the region. Canada and Australia like other countries have independent data protection laws in place echoing the principles in the OECD Guidelines and drawing on the EU Directive. In Latin America, the law centres around the concept '*habeus data*' literally translated it means 'you should have data.' There is a constitutional right to *habeas data* to protect data that is private and it is predominant in many national laws in the region.[224]

Other countries without Constitutions have specific laws protecting data protection and privacy, such as the United Kingdom's Data Protection Act of 1998. The European model is the most comprehensive regional law and the European Union requires all its member states to legislate so as to ensure that citizens have a right to data protection. The African Union, or perhaps more specifically, the Southern African Development Community (SADC) should use the European model as a basis to develop a regional legally binding instrument on data protection that is suitable to the Southern African context. Whether or not the European model can be replicated in Southern African Development Community will be discussed in chapter 5. Before looking at the regional context, the international legal framework on cross border migration will be canvassed. The next chapter provides a legal analysis of existing international migration law from a human rights perspective.

[224] Salazar, Luis (2008) 'E-Commerce Best Practices: Online Privacy (Ten Keys to Latin American Data Privacy), Standford, Standford Law School.

CHAPTER FOUR

4. THE LEGAL FRAMEWORK ON CROSS BORDER MIGRATION

The chapter aims to provide a human rights based analysis of the existing legal framework on cross border migration with reference to rights and obligations of States under international law as well as best practice approaches which can help to shape the development of national laws. By looking at the exercise of State sovereignty rights in pursuit of national security interests it identifies gaps and highlights the importance of upholding State obligations toward individuals as guaranteed under international migration law. In so doing, it provides an insight into the meeting point and challenges at the interface between migration and data protection and argues that State interests and individual rights are not mutually exclusive; instead they can be balanced, albeit a delicate balance.

4.1 *International Migration Law*

> '*International Migration law, which is the international legal framework governing migration, is not covered by any one legal instrument or norm. Instead, it is an umbrella term covering a variety of principles and rules that together regulate the international obligations of States with regards to migrants.*[225]

[225] The International Organization for Migration 'What is International Migration Law?' < http://www.iom.int/cms/en/sites/iom/home/what-we-do/migration-law.html>

This section covers State responsibility and reviews the international framework for the protection of the rights of migrants. The following excerpts of rights and freedoms, which is customary law or find expression in international conventions, are amongst others relevant to the interface between data protection and migration:

Right to integrity, non-discrimination and equality:

- 'All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.' (Article 1 of the UDHR)
- 'Everyone is entitled to all the rights and freedoms set forth in this Declaration, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, *birth or other status*. Furthermore, no distinction shall be made on the basis of the political, jurisdictional or international status of the country or territory to which a person belongs, whether it be independent, trust, non-self-governing or under any other limitation of sovereignty. (Article 2 of the UDHR)
- 'All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.' (Article 7 of the UDHR)

Protection of privacy:

- 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks' (Article 12 of the UDHR)
- 'No one shall be subjected to arbitrary and unlawful interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.' (Article 17 of the ICCPR)

Right to family unity:

- 'The family is the natural and fundamental group unit of society and is entitled to protection by society and the State.' (Article 16 (3) of the UDHR).

Freedom of movement:

- 'Everyone has the right to freedom of movement and residence within the borders of each state.' (Article 13 of the UDHR)
- 'Everyone lawfully within the territory of a State shall, within that territory, have the right to liberty of movement and freedom to choose his residence.' (Article 12 of the ICCPR)

Right to seek asylum and non-refoulement:

- 'Everyone has the right to seek and to enjoy in other countries asylum from persecution.' (Article 14 (1) of the UDHR)
- No Contracting State shall expel or return ('refouler') a refugee in any manner whatsoever to the frontiers of territories where his life or freedom would be threatened on account of his race, religion, nationality, membership of a particular social or political opinion" (Article 33(1) of the 1951 Convention relating to Status of Refugees)

The rights of trafficked persons:

- In appropriate cases and to the extent possible under its domestic law, each State Party shall protect the privacy and identity of victims of trafficking in persons, including, inter alia, by making legal proceedings relating to such trafficking confidential (Article 6 (1) of the 2000 Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially women and children, supplementing the United Nations Convention against Transnational Organized Crime)

The rights of the child:

- No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honour and reputation. The child has the right to the protection of the law

against such interference or attacks (Article 16 of the CRC)

- States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child (Article 12 of the CRC)

The rights of migrant workers:

- States Parties undertake, in accordance with the international instruments concerning human rights, to respect and to ensure to all migrant workers and members of their families within their territory or subject to their jurisdiction the rights provided for in the present Convention without distinction of any kind such as to sex, race, colour, language, religion or conviction, political or other opinion, national, ethnic or social origin, nationality, age, economic position, property, marital status, birth or other status (Article 7 of the MWC)

- No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks (Article 14 of MWC)

State obligations stem from various sources

The obligation of States to protect the rights of migrants stem from the Universal Declaration of Human Rights (1948) and a number of international human rights treaties such as the International Covenant on Civil and Political Rights (1966), the International Covenant on Economic, Social and Cultural Rights (1966), the International Convention on the Elimination of All Forms of Racial Discrimination

(1965), the Convention on the Rights of the Child (1989), the Convention on the Elimination of All forms of Discrimination against Women (1979). All of these legal instruments extend to migrants because the rights embedded therein are not limited to nationals of the signatory States. The United Nations Human Rights Committee has emphatically stated that the enjoyment of these rights are not limited to nationals and that it 'must also be available to all individuals, regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers and other persons, who may find themselves in the territory or who are subject to the jurisdiction of the State Party.'[226] In addition, entering into a country in contravention to the immigration laws and travelling without documents 'do not deprive migrants of fundamental human rights provided in the human rights instruments, nor does it affect the obligation of States to protect migrants in an irregular situation.'[227]

The fact that all countries who are party to the United Nations have ratified at least one treaty that guarantees the right to non-discrimination to everyone demonstrates that this is a fundamental right that runs across all international human rights legal instruments.[228] Similarly, the concomitant right to equality is an integral and indivisible part of such legal instruments and it is in essence the foundation of all human rights, including the right to privacy, which is applicable to all people around

[226] United Nations Human Rights Committee 'The Nature of the General Legal Obligation Imposed on States Parties', General Comment No. 31, paragraph 10 at 3.

[227] Global Commission for International Migration (2005) 'Migrating in an Interconnected World: new directions for action' at 55.

[228] See: OHCHR website <http://www.ohchr.org/EN/Issues/Migration/Pages/HumanRightsFramework.aspx>

the world irrespective of their nationality or immigration status.[229]

The International Convention for the Protection of the Rights of All Migrant Workers and Members of their Families (1990) (MWC) is a core human rights treaty and is the only legal instrument dedicated to migrant rights. Even though it focuses on the rights of migrants with residence permits in the workplace and their neglected family members, it does recognize the specific vulnerabilities of migrants.[230] The 1951 Convention Relating to the Status of Refugees and its 1967 Protocol Relating to the Status of Refugees, and the Convention against Transnational Organised Crime 2000 and its supplementary Protocols on Trafficking in Persons and Smuggling covers particularly vulnerable groups of migrants. The Convention on the Rights of the Child (1989) (CRC) is near universal ratification and the theme that pervades the language of the Convention is the 'best interest of the child.' Article 1 provides guarantees to all children under the age of eighteen, regardless of their nationality.[231]

Article 16 of the Convention of the Rights of the Child emphasizes that children have a right to privacy and that the law should protect them from attacks against their way of life, their good name, their families and their homes that includes the right to equality and non-discrimination, and more specifically the right to privacy. Article 3 states that 'Every child shall be entitled to the enjoyment of the rights and freedoms

---

[229] United Nations (2003) *Human Rights in the Administration of Justice: A Manual on Human Rights for Judges, Prosecutors and Lawyers* at 640.

[230] Op cite note 228, OHCHR website.

[231] South Africa ratified the Convention on the Rights of the Child in 1995.

recognized and guaranteed in this Charter irrespective of the child's or his/her parents' or legal guardians' race, ethnic group, colour, sex, language, religion, political or other opinion, national and social origin, fortune, birth or other status.' Moreover, Article 10 states that 'No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.' Article 12 of the CRC requests that due consideration be given to the views of the child in accordance with the age and maturity of the child. While States have prerogative to limit certain rights to citizens, when it comes to children, no such limitation is allowed as migrant children should be treated equally and they must have equal access to all protections given to children who are citizens.

As seen above, the obligation of States toward migrants stem from various sources that are dispersed across different branches of international law, including human rights law, criminal law, labour law and humanitarian law refugee law. In the absence of a defined body of law on international migration, there continues to be a number of gaps and grey areas. Goulboune examines the limitations of the law protecting non-nationals and the conflict between human rights and the principle of sovereignty, which give States the power to control the entry to their borders. He argues that the lack of an adequate legal framework to take account of the intricacies of migration is

due to a global failure that goes beyond traditions legal norms.[232] This is, for example, evident from the slow ratification of the MWC. Harzig and Hoerder survey the history of migration and note that the classic theories of migration are being challenged by the global phenomenon of migration. Indeed migration in today's world is a dynamic concept and States are grappling with the challenges that it presents. Castles and Miller argue that the 9/11 September terrorist attacks transformed security dilemmas in States, but it did not bring about fundamental changes in the age of migration which faces the rapid growth of labour migration and an increase in asylum-seekers as a result of violence linked to migration.

Nexus between migration and human rights

Even though national migration laws are important to regulate movements across borders and to protect State interests, the fundamental principle of international law is that it prevails over national law if it conflicts with human rights standards to which State are bound. The increased recognition of the nexus between migration and human rights has also been made evident through the establishment of the Special Rapporteur on the Human Rights of Migrants as mentioned earlier in chapter 1.[233] The High Commissioner for Human Rights, Navi Pillay, has called on States to promote and protect the human rights of all migrants and has made this a priority of the work of her office (OHCHR) stating that 'the protection of migrants is an urgent and growing

[232] Goulboune, S (1998) *Law and Migration.*

[233] The mandate of the Special Rapporteur on the Human Rights of Migrants was created in 1999 by the Commission on Human Rights, pursuant to Resolution 1999/44 <http://www2.ohchr.org/english/issues/migration/rapporteur/>

human rights challenge.'[234] According to Loren Landau, 'legal status of migrants only matters in terms of legal identity, for example, refugees have different rights compared to undocumented migrants,'[235] but they are all individuals who should be afforded equal application of human rights. Cholewinski argues that the 'last decade has witnessed an awareness of the difficulties migrants face in accessing the full panoply of rights during migration with the result that migrants' rights today are more clearly recognizable as human rights.'[236]

Migration governance

Since there is no one body of law governing migration, States are left with discretion, and they often turn to migration strategies to regulate migration management. Migration is a politically sensitive issue, particularly in light of States' obligation to protect its citizens from threat or danger and the need to manage migration flows and reduce irregular movements. This political and economic approach to migration has the tendency to undermine the human rights dimension of migration. Cholewinsky emphasizes that when it comes to migration management and the protection of human rights, it is important to focus on the migrants themselves and not only on the migration process.[237]

---

[234] Op cit note 28, OHCHR 'Migration and Human Rights.'

[235] Informal interview with Landau, Loren, Director of the African Centre for Migration and Society, University of Witwatersrand conducted in Johannesburg.

[236] Cholewinski, Ryszard (2010) 'Human Rights of Migrants: The Dawn of a New Era' at 614.

[237] Cholewinsky, Ryszard (2005) *Study on Obstacles to Effective Access of Irregular Migrants: Access to Minimum Social Rights* at 18.

Xenophobia

Migration strategies are usually premised on State interests to protect its own nationals, but sometimes this lends to xenophobic attitudes and unequal treatment of migrants. As mentioned in chapter 2, migrants include both economic and forcibly displaced persons as well as vulnerable migrant groups that use the same migratory routes when searching for legal recourse to human rights abuses. The vulnerability of migrants is compounded by the fact that they live beyond the reach of the legal protection of their country of origin. They are frequently unfamiliar with the language and laws of the host country or transit country, and may not have the support of social networks in the community. This can impair their ability to assert their rights and to access available remedies.[238] In the South African context, as in many other countries, there are additional sentiments of xenophobia that are echoed in comments by high profile ministers[239] and this may eventually finds its way into the law because political agendas tend to drive the development of the law. On the positive side, political drive will provide a legal basis to enact much needed laws; but on the negative side, political agendas can also be fuelled by xenophobic attitudes toward migrants.

Migrant profiling

Migrants are also being treated with more suspicion and are often seen, unjustifiably, as potential enemies. The pretext for migrant profiling is often national security, but

---

[238] See: Statement by Simonovic, Ivan *Report of the United Nations High Commissioner for Human Rights to the ECOSOC General Segment 2010, Item 14(g)* Assistant Secretary-General for Human Rights, 22 July 2010 <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=10231&LangID=E>

[239] Informal interview with Landau, Loren, Director of the African Centre for Migration and Society, University of Witwatersrand conducted in Johannesburg.

the reality is that decisions are being made arbitrarily on discriminatory grounds. Data collection during screening processes and migrant profiling at borders, without adequate safeguards, can be used as a tool to fuel discriminatory practices, as well as ethnic and religious categorization, which are contrary to human rights standards.[240] The Special Rapporteur on the Human Rights of Migrants recently found that migrant profiling is widespread, and in some instances, law enforcement officials routinely use generalization about ethnicity, religion, race, colour of the skin, or national origin in deciding who to target for identity checks, stops, search and sometimes arrest, rather than utilizing objective evidence as the basis for making decisions.[241] This is clearly in contrast with the principle of human dignity and the prohibition of discrimination.

Balancing rights and interests

It is important to ensure that policy imperatives regulate the use of migration management tools that could potentially impede individual rights. An appropriate balance is necessary and this should find its way into the law by clearly outlining the legal justification for limiting rights if it is the only means by which to achieve a justifiable State purpose. This will involve taking account of political agendas and also ensuring that new laws will pass constitutional muster. Legislators need to be impartial when developing law and they are in a unique position to ensure an appropriate balance between the pursuit of States interests and legal safeguards that are needed to protect individual rights. The criteria for balancing State sovereignty and individual rights from the perspective of the South African law will be discussed in chapter 5.

---

[240] Op cit note 31, '*Report of the Special Rapporteur on the Human Rights of Migrants.*'

[241] Ibid, '*Report of the Special Rapporteur on the Human Rights of Migrants.*'

The next section looks in detail at the sovereignty rights and national security and its impact on human rights.

4.2 *State Sovereignty Rights and National Security*

> *'One of the biggest challenges faced by most States is that of striking the delicate balance between maintaining national sovereignty on migration issues and engaging in a whole spectrum of supranational initiatives, ranging from informal dialogues to international legal instruments.'*[242]

The principle of State sovereignty derives from Article 2 of the 1948 United Nations Charter. This right to sovereignty is conferred upon States to give them legal personality, that is, the capacity to enter into a legal relationship with other States and to enjoy rights and corresponding obligations. State sovereignty is about control over territory as well as control over people within the territory. While States have the power to determine the conditions of admission, residence and removal from their territory, this power is not without limits and cannot be to the detriment of individual rights. The human rights and humanitarian laws including refugee law places limits on the exercise of this sovereign power and the distinction between nationals and non-nationals can only be justified if they serve a legitimate State objective and if the distinction is proportional to the achievement of that objective.[243] As stated by former

[242] Op cit note 8, *World Migration Report 2011: Communicating Effectively about Migration.*

[243] Perruchoud, Richard 'State Sovereignty and Freedom of Movement' in Opeskin, Brian; Perruchoud, Richard and Redpath-Cross, Jillyanne (2012) *Foundations of International Migration Law* at chapter 5.

United Nations Secretary-General, Kofi Anna 'State sovereignty, in its most basic sense, is being redefined – not least by the forces of globalization and international cooperation. States are now widely understood to be instruments at the service of their people, and not vice versa. At the same time individual sovereignty – by which I mean the freedoms of each individual as enshrined in the charter of the UN and subsequent international treaties – has been enhanced by a renewed and spreading consciousness of individual rights. When we read the UN Charter today, we are more than ever conscious that its aim is to protect individual human rights [...].[244]

Pertinent State interests

Mills covers the relationship between individuals and the State in the context of human rights and humanitarian issues, and argues that global events question traditional concepts of sovereignty. He further argues that sovereignty is undermined by a wide variety of international practices and normative reorientations. By examining international practice in the areas of human rights, self-determination, refugees, migration and humanitarian intervention, he argues that respect for human rights are inherent in the social purpose of the State and calls for a new concept of sovereignty which protects individual and group rights, while addressing problems which transcend State boundaries.[245] Hobbing argues that globalization and migration has an impact on border control, and this has resulted in the challenge of implementing high-tech equipment and biometrics while considering legal and ethical

[244] Anna, Kofi 'Two Concepts of Sovereignty', Former UN Secretary-General, The Economist 352, 18 September 1999 at 49-50.

[245] See: Mills K A (1995) *The New Sovereignty: The Changing Humanitarian Agenda in the Emerging Global Order* and Mills K A (1998) *Human Rights in the Emerging Global Order: A New Sovereignty?*

considerations.[246] Redpath highlights that reinforcement of the security aspect of migration and the implications of biometric systems as a response to ensure tighter control of frontiers has given rise to concerns among privacy and civil liberty advocates.[247] The above-mentioned authors have raised pertinent issues that States face today, however, the scale always seem to lean toward State interests trumping individual rights. There is indeed a tension between State sovereignty, globalization, migration, and human rights, but they can be compatible if the exercise of States sovereignty is done in conjunction with the exercise of State obligations under international human rights and humanitarian law and in line with national laws protecting individual rights.

Response to terrorism

Many States have turned their policy and legal focus to combating terrorism and have used the right to sovereignty and the State's prerogative to protect its borders and its citizens as a justification. Waldo et al argue that the effort of States in achieving this goal gives rise to the apparent conflict between individual privacy and national security, but what is needed is a balance between the types of information necessary to ensure national security and the constraints imposed on those that gather the information.[248] Mendel points out that one of the major problems with the justification of national security, is that unlike other interests that impose restrictions on rights, this

[246] Hobbing, Peter (2005) *Integrated border management at the EU level.*

[247] Op cit note 7, *Biometrics and International Migration.*

[248] Op cit note 3, *Engaging Privacy and Information Technology in a Digital Age* at 279.

area is highly political.[249] The European Court of Human Rights stressed that crime prevention and control 'should be exercised in a manner which fully respects the due process and other guarantees which legitimately place restraints on the scope of the State's action to investigate crime and bring offenders to justice, including the guarantees contained in Article 8 on the right to privacy.'[250] This applies to the international setting as well where States have the difficult job of having to balance their interests with competing human rights protections. On the one hand, they must protect their population against terrorist threats, and on the other, they must safeguard the fundamental rights of individuals, including persons suspected or convicted of terrorist activities.'[251]

The first Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Mr. Martin Scheinin, emphasizes that consistency with human rights is not sufficient when enacting terrorism laws, in addition, the conduct of agencies involved in countering terrorism must be in compliance with human rights and refugee law and applicable principles and provisions of international humanitarian law. To ensure this, monitoring mechanisms should be in place and 'where the law relating to terrorism confers discretionary powers upon public agencies, adequate safeguards, including judicial review, must exist for the purpose of ensuring that discretionary powers are not exercised arbitrarily

---

[249] Mendel, Toby (2003) 'National Security vs. Openness: An Overview and Status Report on the Johannesburg Principles' in Campbell Public Affairs Institute *National Security and Open Government: Striking the Right Balance* Maxwell School of Citizenship and Public Affairs Syracuse University, New York at 6.

[250] *Osman v The United Kingdom* (2000) 29 EHRR 245

[251] Council of Europe Commissioner for Human Rights 'Protecting the Right to Privacy in the Fight against Terrorism', Strasbourg, CommDH/IssuePaper (2008) 3 at 12.

or unreasonably.'[252] While measures taken to combat terrorism may indeed limit the enjoyment of individual rights, it is important for States to recognize that compliance with human rights is necessary to address the long-term conditions conducive to the spread of terrorism, and that effective counter-terrorism measures and the protection of human rights are complementary and mutually reinforcing goals.'[253] Another rising concern is the role of private agencies in the event that the States outsource security measures at border points. If States elect to privatize their functions, the private companies should be equally accountable and held to the same standards because they are acting as agents of the States.[254]

Legal basis for limiting human rights

The balancing of State interests in combating terrorism and protecting individual rights is complex and when laws are being developed legislators often need to look at international legally binding instruments together with best practice in implementing the rights and obligations thereunder to ensure a comprehensive approach. The Special Rapporteur says 'the identification of a best practice is based on three criteria: (a) a credible claim that the practice is an existing or emerging practice, and/or one that is

---

[252] Scheinin, Martin 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ten Areas of Best Practices in Countering Terrorism' (A/HRC/16/51), 14 February 2010 at 8 <http://www.ohchr.org/EN/Issues/Terrorism/Pages/Annual.aspx>

[253] Ibid, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ten Areas of Best Practices in Countering Terrorism' at 5.

[254] Ibid 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ten Areas of Best Practices in Countering Terrorism' at 9. This concern on outsourcing State responsibility was also raised by Perruchoud, Richard, Former Legal Advisor of the IOM Department of International Migration Law and Legal Affairs, in the informal interview conducted in Geneva.

required by, or has been recommended by or within, international organizations, international treaties or the jurisprudence of international, regional or domestic courts; (b) the practice relates to and promotes the effective combating of terrorism; and (c) the practice complies with human rights and/or promotes the enjoyment of human rights and fundamental freedoms.'[255] This assessment should be included in the balancing test which should not only come into play after legislation is in force; it is more effective if it is taken into account when laws are being developed. The Special Rapporteur puts forward a list that will help the Legislature in its balancing test, namely: 1) all proposals for new legislation or amendments to existing laws must include a written statement if there are apparent inconsistencies with the purposes and provisions of norms of international human rights and refugee law that are binding upon the State; 2) before the law is enacted the Legislature must review the proposed law in light of this statement and ensure that it conforms to the norms of international human rights and refugee law that are binding upon the State; 3) the Judiciary has a role to play and must be entrusted with the power to either adopt an interpretation of the law that is consistent with the purposes and provisions of norms of international human rights and refugee law that are binding upon the State, declare the inconsistent part of the law as invalid, or declare that the inconsistent law has no force or effect immediately or within a certain period of time to allow the Legislature to take remedial steps.' Ultimately the exercise of limitations on rights must be based on clear provisions of the law that exhaustively outline the obligations of those conferred with power and 'the exercise of such functions and powers may never violate peremptory or non-derogable norms of international law, nor impair the essence of any human

[255] Ibid, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ten Areas of Best Practices in Countering Terrorism' at 2.

right.'[256]

The judgments of the European Court of Human Rights and case law of the European Court of Justice underscore the following minimum standards for handing personal data when seeking to prevent terrorism. 'First there must be a legal basis for any collection, storing, use, analysis, disclosure and sharing of personal data for law enforcement and anti-terrorist purposes. A vague, broad general statutory basis is not sufficient; instead, the processing of personal data must be based on specific legal rules relating to the particular kind of processing operation in question. Secondly, these rules must be binding and they must lay down appropriate limits to ensure that the statutory powers have: 1) a precise description of the kind of information that may be recorded; 2) a precise description of the categories of people against whom surveillance measures are needed and why information gathering and storage need to be taken; 3) a precise description of the circumstances in which such measures may be taken with a clearly set out procedure to be followed for the authorisation of such measures; 4) limits on the storing of old information and on the time for which new information can be retained; 5) explicit and detailed provisions concerning the grounds on which files can be opened and the procedure to be followed for accessing the files; 6) the persons authorised to have restricted access to the files; and 7) the nature of the files and the intended use thereof.[257]

---

[256] Ibid, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ten Areas of Best Practices in Countering Terrorism' at 20 – 21.

[257] Op cit note 251, 'Protecting the Right to Privacy in the Fight against Terrorism' at 7.

The Council of Europe Commissioner for Human Rights goes further to outline that 'personal data of persons not suspected of involvement in a specific crime or posing a threat should not be collected, and neither should the collection of information be through intrusive, secret means (such as telephone tapping and email interception etc., bugging, informers, agents).' In addition, the use of 'profiling techniques, and "preventive" policing, must generally be subject to a particularly strict "necessity" and "proportionality" tests and there must be strong "safeguards established by law" which ensure appropriate and effective supervision of the activities ideally carried out by the Judiciary, or otherwise, by particularly strong alternative supervisory mechanisms.'[258]

Data collection for national intelligence

The European Commission of Human Rights point to the new trend used by States to avoid international and national obligations. This relates to the use of administrative law as a way to bypass the criminal law and the safeguards of the criminal justice system because it allows for lower standards of proof and the rules on the admissibility of evidence are relaxed in ways that seriously affect the rights of individuals to due process and privacy. [259] Waldo et al are of the opinion that this is compounded by a greater challenge related to the blurring of the traditional separation between national intelligence gathering by law enforcement agencies and intelligence security agencies, as this in turn, creates further challenges to the legality of data collection for the purpose of crime and terrorism.[260] Law enforcement serves as a government actor

[258] Ibid, 'Protecting the Right to Privacy in the Fight against Terrorism' at 6-7.

[259] Ibid, 'Protecting the Right to Privacy in the Fight against Terrorism' at 12.

[260] Op cit note 3, *Engaging Privacy and Information Technology in a Digital Age* at 32.

tasked to mainly help in conviction of suspects who have contravened the law, while national intelligent agencies are tasked with monitoring borders and protecting national security on behalf of the government. The inadmissibility of evidence in court based on information gathered by law enforcement that is obtained through unlawful means is a constitutional barrier and safeguard against potential police abuse.[261] This means that information gathered by law enforcement agencies and subsequently used as evidence in the prosecution of an individual eventually becomes public and is open to challenge by the person being prosecuted. However, 'information gathered by intelligence agencies for national security purposes must be kept secret and this is required not only to keep an adversary from learning what is known about him, but also to ensure that the sources of information cannot be identified and compromised. The need for secrecy in this realm means that those who might be the subjects of interest for information gathering cannot know what information is gathered about them (or even if information is being gathered about them), much less check or challenge the accuracy of that information.'[262]

A particular concern is that information collected by intelligence agencies are collected under the broad guise of State security interests without any parameters for lawful collection. What we see nowadays is that law enforcement are also involved in investigations for State security purposes which often have no specified purpose and the data collected is not subject to the same level of scrutiny as evidence in a court of law. Yet, it can still affect the lives of those whose names appear on watch lists and

[261] Ibid, *Engaging Privacy and Information Technology in a Digital Age* at 275.

[262] Ibid, *Engaging Privacy and Information Technology in a Digital Age* at 279.

can potentially prevent freedom of movement of those travelling lawfully.[263] There is also no balancing test required either because decisions of the police to collect personal information for wide-ranging investigatory reasons is not reviewable or appealable. Such phishing exercises intrude into the private sphere contrary to legal parameters that should be in place and it leaves the individual at a severe disadvantage when information is inaccurate or incomplete.[264]

European case law

With reference to case law of the European Court of Human Rights case, in *Leander v. Sweden*, the Court highlighted the dangers inherent in the electronic links between the police registers and other States' registers or Interpol's register. It is therefore important that 'individuals have a right of appeal against a data entry resulting from a fundamental mistake, even if the source of the information is kept secret and is known only to the independent authority that has jurisdiction to determine the applicant's appeal.'[265] In *Rotaru v. Romania*, the Court held that the exceptions to the Article 8 right of data protection in the EU Charter has to be interpreted narrowly because the phrase 'in accordance with the law' does not merely refer back to domestic law, but also relates to the quality of the law and this implies that there must be a measure of legal protection in domestic law against arbitrary interferences of rights by public

[263] Ibid, *Engaging Privacy and Information Technology in a Digital Age* at 253.

[264] Ibid, *Engaging Privacy and Information Technology in a Digital Age.*

[265] European Court of Human Rights, *Case of Leander v. Sweden* (Application no. 9248/81), Judgment, Strasboug, 26 March 1987 at 33.

authorities.[266] The Court said further that the 'secret collection of personal data for State security purposes amounted to an interference with private life and that only necessary categories of persons to whom such interference applies and the types of personal data needed should be described beforehand by law in a sufficiently precise and foreseeable manner in accordance with legitimate criteria.[267] Such criteria are useful for other jurisdictions as well.

Gathering personal data for investigatory and intelligence purposes that do not have a clearly defined specified purpose conflicts with the specified principle, which is a core Data Protective Principle under the legislation governing the collection and processing of personal data. In addition, the technologies used for intelligence gathering is often very advanced and the public are not informed of data collection methods used given the secrecy requirements in intelligence gathering. A rising concern is that the same technology is also being made available to law enforcement agencies in their investigatory efforts. This is intrinsically linked to migration and border control because, once migrants enter into a country, some States use these government actors to engage in clandestine tracking even though the migrants may be lawfully in the country. There is no justified State security reason to treat migrants as suspected criminals if they follow the laws according to their obligations under international law and act in compliance with immigration laws. In the case of *Leander v. Sweden*, the

[266] European Court of Human Rights, *Case of Rotaru v. Romania* (Application no. 2834/95) Judgment, Strasbourg, 4 May 2000 at 55.

[267] Ibid, *Case of Rotaru v. Romania.*

European Court of Human Rights held that a system of secret surveillance for the protection of national security poses a risk of undermining or even destroying democracy on the ground of defending it, and the Court must be satisfied that there exists adequate and effective guarantees against abuse.'[268]

Power of the State threatening individual rights

Waldo et al argue that 'it is the sheer imbalance between the power of the State and that of the individual which makes people understandably anxious about the information gathering abilities of the State. Consequently, the disparity in resources for the State versus those that are available to most individuals also justifies the imposition of certain limits on government's information gathering, even if such limits complicate or impede the task of law enforcement agencies.'[269] They argue further that the advance technology available for intelligence 'may define both the boundary for technology that can be privacy invasive, and the boundary for those technologies that can help to ensure privacy.[270] Indeed technology can have a dual purpose to protect the rights that it may potentially infringe upon. To do so, safeguards have to be built into the technology itself and State interests must be complemented by their obligations to protect human rights to ensure that any potential infringements on individuals are within the confines of the law.

---

[268] Op cit note 265, *Case of Leander v. Sweden* at 60.

[269] Op cit note 3, *Engaging Privacy and Information Technology in a Digital Age* at 277.

[270] Ibid, *Engaging Privacy and Information Technology in a Digital Age* at 278.

The historical distinction between law enforcement gathering information for detecting crime on the one hand, and intelligence agencies gathering information for national security reasons on the other hand, rested in the need to ensure privacy protections. This distinction has been blurred due to the September 11 attacks because as the argument goes 'had relevant information held by both the law enforcement agencies and the intelligence agencies been put together and seen correctly, the attacks could have been predicted and stopped.'[271] As a result, laws were passed and policies were created in the United States to make it easier for data exchange without much scrutiny, and other countries have followed suit. Such invasive responses to criminal threats do not really deter the terrorist incidents from happening. Instead, it weakens traditional checks and balances and if intelligence is gathered collectively by different agencies without any legal parameters it threatens the foundations of democracy within the country and with relations abroad.

As seen in the Snowden disclosures making news these days, if there are no legal barriers in place, the collection personal information for intelligence purposes can spread beyond border to other continents. Most recent news indicates that there is now also a threat to monitoring communications of the United Nations.[272] This is contrary to international data protection standards and it contravenes the diplomatic principle of privileges and immunities as guaranteed in the United Nations

[271] Ibid, *Engaging Privacy and Information Technology in a Digital Age* at 284 – 286.

[272] Al Jazera 'US Promises not to Spy on the UN - UN says it has been assured the US does not and will not spy on it, but doesn't comment on whether it do so in the past' 30 October 2013 <http://www.aljazeera.com/news/americas/2013/10/us-promises-not-spy-un-201310301934394770.html>

Conventions on Privileges and Immunities.[273] Such contraventions affect those UN agencies collecting and processing personal data of migrants because disclosures without the migrants' consent for purposes unrelated to humanitarian aid can jeopardize lives, especially in vulnerable situations as described in chapter 1.3 above. What is needed is the necessary reinforcement of privacy protections because it is possible that State security interests and the right to privacy can co-exist.

Reconciling privacy concerns

To ensure respect for privacy, transparency from the government and assurance that information gathered is accurate and appropriately treated and that it will only be used for genuine national security purposes is needed. In addition, clearly defined laws justifying any limitations and outlining oversight functions to monitor that appropriate data protection safeguards, and checks and balances must be in place to minimize inappropriate data intelligence gathering.[274] This will help to build trust in society and alleviate the 'tension between the privacy and national security, which parallels the tension between privacy and law enforcement,'[275] alleviating this tension could be to the collective benefit of the State and individuals. It is equally important for individuals to be proactive and become better informed about their rights. In the migration context, the humanitarian actors can be helpful catalysts in disseminating awareness of legitimate purposes and intended use of the information that would meet

[273] The 1946 Convention on the Privileges and Immunities of the United Nations and 1947 Convention on the Privileges and Immunities of the Specialized Agencies guarantee inviolability of premises, documents and archives for the effective functioning of the UN agencies and this immunity should be respected by all signatory States.

[274] Op cit note 3, *Engaging Privacy and Information Technology in a Digital Age* at 294 – 296.

[275] Ibid, *Engaging Privacy and Information Technology in a Digital Age* at 292 – 325.

the expectations of the migrants. The public opinion is important in changing perceptions, but the starting point is the government being accountable and transparent.

Waldo et al mention that if the policy choice results in a shift of the onus onto individuals to carry the burden of protecting their own privacy rights, then the law and regulation should assist individuals in asserting such rights. This is because privacy is at an inherent disadvantage when decision-makers weigh privacy against other interests where the benefits of the State appear to be more tangible. They recommend that the onus be on the governments to reduce this disadvantage by establishing formal mechanisms for institutional advocacy of privacy among government actors.[276] In his report to the UN Human Rights Council, the Special Rapporteur says that States no longer limit exceptional surveillance schemes to combat terrorism. Instead, they make these surveillance powers available for all kinds of unrelated purposes unknown to individuals and 'most worrying is that these technologies and policies are being exported to other countries where the most basic protections are lost in the process.

Regulating security initiatives

The need for terrorism laws and practice to be consistent with human rights was also reiterated by the current Special Rapporteur, Mr. Ben Emmerson.[277] The problem with

[276] Ibid, *Engaging Privacy and Information Technology in a Digital Age* at 15.

[277] Statement by the Special Rapporteur on the Promotion and Protection of Human Rights while Countering Terrorism at the International Seminar Terrorism and human rights standards, Santiago de

counter-terrorism measures, even if regulated in the law, is that the concept of terrorism is too open-ended. The European Commissioner for Human Rights notes, that unlike public emergencies that have a clear end, there is no end in sight to the fight against global terrorism and national laws tend to be semi-permanent.[278] Measures adopted on an emergency and temporary basis turn out to be permanent and are extended into law, but this is not compatible with the advanced technologies used for the surveillance of terrorist activities, which is rapidly changing all the time. To curb this, a narrow definition of State security, should be employed as recognized in the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (Johannesburg Principles).[279] According to Principle 2, 'a restriction is not legitimate unless its purpose and effect is to "protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force" from either an internal or an external threat. Mendel notes that this is probably an unrealistically high standard, for example, the September 11 attacks 'could hardly be said to have threatened the existence or territorial integrity of the United States, unless this is interpreted very broadly, which would largely defeat the purpose of a narrow definition.[280] In any event, the attacks did affect the State's capacity to respond to the immediate threat. To ensure a legitimate State purpose, any

---

Chile, 15 November 2011 <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=11737&LangID=E>

[278] Op cit note 251, 'Protecting the Right to Privacy in the Fight against Terrorism.'

[279] The Johannesburg Principles was adopted on 1 October 1995 by a group of experts on international law in Johannesburg and has been endorsed by the United Nations Commission on Human Rights and in the reports of the Special Rapporteure on Freedom of Expression. The principles are based on international and regional law and standards relating to the protection of human rights, evolving state practice (as reflected *inter alia* in judgments of national courts), and the general principles of law recognized by the community of nations. For further detail, see <http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf>

[280] Op cit note 249, 'National Security vs. Openness: An Overview and Status Report on the Johannesburg Principles' at 11.

restrictions on the rights of individual must be prescribed by safeguards, and conditions for such restrictions must be embedded in the law.

Intrusive data collection methods

The European Commission on Human Rights cautions that 'computer profiling may lead to intrusive and punitive action, including administrative action, against large numbers of innocent individuals, without being effective in stopping real terrorists. It also poses risks to discriminating against minority groups and can have a devastating effect on the individual, who is likely to be spied upon, harassed, refused permission to travel, denied a job, or even arrested. This approach will also have a chilling effect on democracy itself and undermines the objective of security.'[281] Data collection on terrorism, while aiming to target terrorists and criminals, involves broad sweeping collection methods which include collecting data on law abiding citizens and migrants. This has given rise to privacy concerns, particularly because in their efforts 'law enforcement agencies gather information about innocent individuals, or they use it for other purposes that are not related to investigations or prosecution, or even more concerning is when the very process of data collection or the knowledge thereof changes the behaviour of those who are clearly innocent.'[282] Waldo et al acknowledge that data collection, storage and analysis of large volumes of information is vital to the law enforcement process, but the inevitability of collecting 'information on persons who are manifestly beyond suspicion'[283] may end up changing behaviours thereby

[281] Op cit note 251, 'Protecting the Right to Privacy in the Fight against Terrorism' at 12.

[282] Op cit note 3, *Engaging Privacy and Information Technology in a Digital Age* at 275.

[283] Ibid, *Engaging Privacy and Information Technology in a Digital Age* at 275.

contributing to crimes. This goes to the argument in chapter 2.3 that this approach by implication results in a group of *male fide* travellers based on suspicion and this takes democracy back in centuries.

Balancing test

Any intended restriction or limitation to individual rights in the name of State security must undergo a strict balancing test. In particular, 'the limitation to the individual rights should be to the least intrusive means possible to achieve security, it must be necessary in a democratic society to pursue the security interests as a defined legitimate aim in accordance with international law, and it must be proportionate to the benefit obtained in achieving the legitimate aim in question.'[284] This is elaborated in Principle 1.3 of the Johannesburg Principles which provides that 'any restriction must apply only where the expression poses a serious threat, it is the least restrictive means available, and it is compatible with democratic principles. Mendel argues that this is a higher standard than applied by most international human rights courts and tribunals. It is, however, crucial because without the threshold barrier of serious harm and the requirement of the least restrictive means, States have less limitation and they will be able to make national security-based claims for restrictions in excessively wide circumstances.[285]

[284] Op cit note 252, 'Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Ten Areas of Best Practices in Countering Terrorism' at 20 – 21.

[285] Op cit note 249, 'National Security vs. Openness: An Overview and Status Report on the Johannesburg Principles' at 10.

The European Commission on Human Rights sets clear criteria when it comes to balancing State interests against fundamental individual rights, namely: 'inherent State security measures must be justified by the State as being: 1) in accordance with the law; 2) necessary in a democratic society, this means it is must be in the interests of national security, public safety or the economic well-being of the country, for the prevention of crime or disorder, or for the protection of the rights and freedom of others; 3) proportionate; and 4) non-discriminatory. In the context of anti-terrorism measures taken by the State, data protection needs to be reinforced, and therefore the following additional requirements must be met when conducting a balancing test: 1) all processing of personal data for law enforcement and anti-terrorist purposes must be based on clear and specific, binding, and published legal rules; 2) the collection of personal data of individuals who are not suspects of a specific crime or of posing a threat; collection of information through intrusive, secret means; and the use of profiling techniques must be subject to particularly strict "necessity" and "proportionality" tests; 3) factual and intelligence data should be clearly distinguished from data on different categories of data subjects; 4) access to police and secret service files should only be allowed for a specified purpose on a case-by-case basis and be under judicial control; 5) there must be limits on data retention; 6) the collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited; 7) reliance by private or public bodies on computers to take decisions on individuals, without human input is fundamentally contrary to the requirement of respect for the human identity and should only be allowed exceptionally under strict safeguards; 8) there must be strong safeguards established by law which ensure

appropriate and effective supervision over the activities of the police and the secret services in the fight against terrorism which should be carried out by the judiciary and through parliamentary scrutiny; and 9) all processing of personal data should be subject to close and effective supervision by independent and impartial data protection authorities.'[286] One additional factor to add in the migration context is: 10) threat and harm to civilian life must be at an absolute minimum when pursuing the State interest to deter terrorism and a proper risk assessment should be conducted and recorded for legal scrutiny.

Risks to data protection

The direct risk to data protection is that this growing area of law is often seen as an 'obstacle to effective anti-terrorist measures and this leads to the prime area of law that is often ignored, yet data protection is crucial to upholding fundamental democratic values and it is for this very reason that the tension between the desire to prevent terrorism and the importance of protecting human rights is a matter of pressing concern.'[287] Waldo et al say this is not a new tension; governments have been confronted with this hundreds of years long before the September 11 attacks.[288] However, the challenge to strike the balance between acknowledging the needs and objectives of law enforcement or national security on the one hand, and the protection of privacy and data protection on the other hand, has increased exponentially because the 'confluence of technology makes it easier to erode privacy far more extensively

[286] Op cit note 251, 'Protecting the Right to Privacy in the Fight against Terrorism' at 13.

[287] Op cit note 251, 'Protecting the Right to Privacy in the Fight against Terrorism' at 3.

[288] Op cit note 3, 'Engaging Privacy and Information Technology in a Digital Age' at 11-12.

than ever before.[289]

'Recording passenger names, credit card information and flight schedules relates to monitoring travel movements and migrant profiles that are based on sensitive personal data such as nationality, travel document, method and means of travel, age, sex, physical distinguishing features (e.g. battle scars), education, choice of cover identity, use of techniques to prevent discovery or counter questioning, places of stay, methods of communication, place of birth, psycho-sociological features, family situation etc.'[290] Profiling based on some of these grounds is tantamount to discrimination based on race or ethnic profiling, but authorities tend to broaden the category of personal data to make it seem more acceptable.

The fight against terrorism clearly intersects with data protection and the conflict that arises at this intersection has intensified over recent years. The *EU Council Framework Decision on the Protection of Personal Data in the Framework of Police and Judicial Co-operation in Criminal Matters* aims to address the tension created by the intersection. However, it falls short in 'setting the lowest common data protection denominator and it excludes national security from the listed data protection guarantees. It for this reason that the 'Framework received widespread criticism from the European Parliament, the European Data Protection Supervisor (EDPS), all the data protection authorities in the EU, civil society and a number of human rights

[289] Ibid at 12.

[290] Op cit note 251, 'Protecting the Right to Privacy in the Fight against Terrorism' at 11.

groups.'[291]

Global data protection law to limit abuse

After reviewing the expanding global use of surveillance measures and advanced databases by governments in their fight against counter-terrorism, the Special Rapporteur on Human Rights, Martin Scheinin, urged the UN to create a global declaration on data protection and data privacy.[292] Most recently in the wake of media reports relating to allegations that the United States is involved in spying on foreign dignitaries,[293] Germany and Brazil urgently called for a Global Data Protection Declaration and this has gained support from the European Union. States elsewhere may also have incentive to sign up to a declaration, which although not legally binding, would signify in a global agreement that the right to data protection exists across borders and warrants international protection. It is not clear whether the form would indeed be a Declaration.

The German Chancellor suggested that it could be a Protocol added to the 1966 International Covenant on Civil and Political Rights (ICCPR).[294] If this follows suit it

---

[291] Ibid, 'Protecting the Right to Privacy in the Fight against Terrorism.'

[292] Williams, Christopher 'UN Issues Call for International Privacy Statement' The Register, 20 January 2010 <http://www.theregister.co.uk/2010/01/20/un_terror/>

[293] Saul, Heather 'Angela Merkel calls for Tighter Internet Data Protection Rules for Websites Registered in the UK Amid Allegations of US Surveillance' The Independent, 15 July 2013 <http://www.independent.co.uk/news/world/europe/angela-merkel-calls-for-tighter-internet-data-protection-rules-for-websites-registered-in-the-uk-amid-allegations-of-us-surveillance-8708975.html>

[294] Ibid, 'Angela Merkel Calls for Tighter Internet Data Protection Rules for Websites Registered in the UK Amid Allegations of US Surveillance.'

would be a big step in the right direction and it would create binding obligations to States who become signatory to the envisaged Protocol. Arguably, the introduction of a Protocol to the ICCPR elaborating the right to data protection may gain better support by States who are signatory to this Convention as opposed to creating a new Convention as envisaged under the Madrid Resolution, simply because new conventions take years to gain support as seen with the Migrant Workers Convention. If this route is followed data protection would be seen as an extension to the right of privacy that requires further elaboration on the details relating to the data protection as a human right. The format of a binding data protection law at international level remains to be seen, but recent concerns may steer States to place data protection on their legislative agendas, which could in turn, result in the long awaited universally binding legal instrument on data protection.

As recent as 18 December 2013, coincidently on international migrants day, the UN General Assembly adopted the Resolution on *The Privacy in the Digital Age* reinforcing the right to privacy, emphasizing that unlawful or arbitrary surveillance and/or interception on communications as well as unlawful or arbitrary collection of personal data is highly intrusive acts violating the rights to privacy and to freedom of expression which may contradict the tenets of a democratic society, and calling on States to protect and respect the right to privacy including in the context of digital communication and to take measures to put an end to and prevent such violations by ensuring that national legislation complies with their obligations under international

human rights law.[295] This Resolution was adopted without a vote and is only recommendatory with no binding force, but it demonstrates the growing concern on intrusions to privacy and data protection and the role that intergovernmental organizations can play in urging the development of much needed laws.

Chapters 2 and 3 above cover a legal analysis of data protection and migration at the international level. In the absence of positive law on the interface between data protection and migration, the next chapter turns to the domestic law of South Africa for guidance. It looks specifically at the South African jurisprudence on data protection, which is developing in this area, and assesses whether it adequately protects sensitive personal data such as HIV/AIDS status and refugee claims. Finally, it seeks to establish whether relevant legal principles and criteria can be extrapolated to help inform the development of the law at the international level.

[295] The Right to Privacy in the Digital Age, 2013 [G.A. res. 68/167] adopted on 18 December 2013 without a vote <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167>

CHAPTER FIVE

5. BALANCING STATE INTERESTS AND INDIVIDUAL RIGHTS THROUGH THE LENS OF THE SOUTH AFRICAN LAW

> *'The concept of privacy is an amorphous and elusive one which has been the subject of much scholarly debate. The definition varies from jurisdiction to jurisdiction and differs according context. This does not imply that the right is not important, instead it illustrates the complex nature of privacy which is now compounded by the complexities of the information age.*[296]

State interests and individual rights are not mutually exclusive. For this reason individual rights should not be diluted or subjugated by the interests of States. Instead, there should be an appropriate balancing test to ensure that any limitation to the enjoyment of rights are justified and proportional and that the measures taken to achieve the State interest is the least intrusive and only alternative available. By looking at constitutional jurisprudence and at gaps in the South African law, this section aims to identify the criteria for balancing between the right to data protection, which is synonymous to information privacy, and competing constitutionally guaranteed rights. In so doing, it seeks to find the line that strikes the balance between the two and goes further to argue that the criteria for the balancing test can be transposed into situations where States interests compete with individual rights. It should be noted that even though many of the cases mentioned concern freedom of information, it does puts forward good criteria for balancing conflicting rights and this

[296] *Bernstein v Bester NO* 1996 (2) SA 751 (CC), see judgment of former justice Ackermann at para 65.

test is arguably transferable when balancing the right to privacy with other competing rights such as the State's right to limit the enjoyment of the right to privacy for reasons of State security and public safety. After a brief discussion of the right to information privacy in common law, case law and statutory law, an analysis of the recently enacted Protection of Personal Information Act 4 of 2013 is provided with a view to determine if it addresses the current gaps on data protection in the South African law.

Development in case law

Michalson stated that 'there have been no reported cases on information privacy at common law or based on the constitutional right to privacy.'[297] This statement is not entirely correct. Indeed, prior to 2007, the right to privacy has been ruled upon mainly in the context of free speech and defamation, but the analysis in the rulings and *obiter* in the judgements can be transferred to information privacy as seen in the cases of *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC), *NM and Others v Smith and Others* 2007 (7) BCLR 751 (CC) and most recently in *Mail and Guardian Media Limited and Others v Chipu N.O. and Others* Case No 136/12, 27 September 2013 (as yet unreported). Even as early as 1993 in *Jansen van Vuuren and Another NNO v Kruger*1993 (4) SA 842 (A), the Appellate Division as it then was, upheld the confidentiality of a patient's HIV status stating that 'individuals are entitled to dictate the ambit of disclosure.' In *National Jooste Ltd and Another*, 1996 (3) SA 262 (A), the Court also ruled that HIV/AIDS status cannot be revealed without consent and held that 'a right to privacy encompasses the competence to

[297] Michalson, L 'Guide to Data Privacy Law in South Africa' <http://securitysa.com/article.aspx?pklarticleid=3317 >

determine the destiny of private facts.'

Constitutional jurisprudence

Actually, constitutional jurisprudence has leaned towards the development of the law on information privacy rights since 1998. In *Mistry v Interim Medical and Dental Council of South Africa*,[298] the Constitutional Court noted that the 'degree of privacy that can be reasonably expected would vary significantly according to the activity that brings the person into contact with the State and the more public the interaction, the less is the expectation of privacy and this is due to the reasonable regulation and inspection which is an inseparable part of society with an effective regime of regulation.'[299] As stated by former justice Sachs 'the new Constitution requires us to repudiate the past practices which where repugnant to the new constitutional values, while at the same time reaffirming and building on those that were inconsistent with those values.'[300] The Court at that time already listed some important factors that are relevant to data protection: 'Whether the information was obtained in an intrusive manner? Whether the information was about intimate aspects of the data subject's personal life? Whether it provided for one purpose but was used for another? Whether

[298] *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC).

[299] Ibid, *Mistry* case at 345 -346 the Court stated that "[t]he more public the undertaking and the more closely regulated, the more attenuated would the right to privacy [be] and the less intense [the] invasion" and "[i]n the case of any regulated enterprise, proprietor's expectation of privacy with regard to the premises, equipment, materials and records must be attenuated by the obligation to comply with reasonable regulations and to tolerate the administrative inspections that are an inseparable part of an effective regime of regulation".

[300] Op cit note 298, *Mistry case* at 317.

the data subject disseminated it to the press or general public? Whether it could reasonably be expected that such information would be withheld?[301]

In the case of *NM and Others v Smith and Others*[302] the Constitutional Court for the first time ruled on privacy in a matter not relating to defamation. The minority decision held that the common law *Actio Iniuriarum* [303] should be developed in order to give effect to the applicants' rights to privacy and dignity as guaranteed in the 1996 Constitution. In cases prior to the NM Judgement, it was held that the *Actio Iniuriarum* was not automatically applicable to cases involving the disclosure of private facts.[304] In the Minority decision in the NM Judgement, however, former Sachs J acknowledged that HIV status called for special consideration of confidentiality, given the sensitivity of the information, and recognized that 'there is a greater need for caution when the private fact involved is significantly private to the individual concerned.'

5.1 *Constitutional Imperatives in the South African Context*

As stated in chapter 3.3, the Universal Declaration of Human Rights (1948) (UDHR) is the foundation of the international law on human rights. The fundamental rights

---

[301] Burchell, Jonathan 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid' *Electronic Journal of Comparative Law*, vol. 13.1, March 2009 <http://www.ejcl.org>

[302] *NM and Others v Smith and Others* 2007 (5) SA 250 (CC).

[303] For example: *Khumalo and Others v Holomisa* 2002 (5) SA 401 (CC) and *National Media Ltd v Bogoshi* 1998 (4) SA 1196 (SCA).

[304] Op cit note 302, *NM* case dissent judgment of O'Regan J.

contained in the UDHR, including the right to privacy, have been incorporated into international covenants such as the ICCPR, which are binding on the international community. South Africa's signature to the international legal instruments on human rights signifies its commitment to uphold the spirit and purpose of the rights by giving effect to it in national law. This section canvasses the importance of the right to privacy and data protection in the South African constitutional democracy.

Practical realities in a constitutional democracy

In June 2004 several major South African newspapers reported that the Post Office planned to make millions by selling personal data to private companies. This included personal data of all registered citizens contained in the National Address Database collected via census records, TV license payments, telephone accounts and national identity document records held by the Ministry of Home Affairs. Individuals were not aware of and would not have consented to the selling of their personal data for profit. As a result, members of the public were outraged. Not too long thereafter, in July 2004, the Financial Mail reported that an employee of Sentech had mistakenly e-mailed the company customer database to about 80 My Wireless customers.[305] Again, the public was not happy. These examples illustrate that there was a growing public concern, about a decade ago, that protection of personal data was needed.

Now South Africa has the Protection of Personal Information Act, which aims at

[305] See: De Kock Emmie 'Data Protection in South Africa' December 2005 <http://www.dekock.co.za/data-protection-in-south-africa/>

regulating the handling of personal data by the State and by private entities. The continuous public outcry to the Protection of State Information Bill relates to concerns that question the foundations of democracy, which is founded on an open and democratic society, and the threat of moving toward a society where freedom of information is suppressed. The Protection of State Information Bill does not fall within the scope of this thesis, but it should be noted the public outcry resulted in fears among private advocates that the encroachment of the State is moving too much into the private sphere of the individual. The Protection of Personal Information Act has not been as controversial and this is probably because much research and public participation went into drafting this law.[306]

Importance of the right to privacy

The Constitution of South Africa Act, 1996, being the supreme law of the land,[307] forms the starting point for all fundamental human rights enjoyed in the country. The right to privacy (Article 14), equality and non-discrimination (Article 9), human dignity (Article 19), access to information (Article 32), as well as the limitation on any rights (Article 36) are particularly important in context of data protection and migration. Article 14 of the Constitution provides:

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

[306] See: The Protection of Personal Information Act <http://www.search.gov.za/info/search.jsp>

[307] Article 2 of the Constititution of the South Africa Act, 1996.

Accordingly, '*everyone* has the right to privacy, which includes the right not to have the privacy of their communications infringed.' Moreover, Article 32 provides for the 'right to access information in the exercise or protection of any rights.' The right to privacy exists at common law, in particular everyone has the right to personality rights which include protecting the *dignitas* of the person, and any breach thereof can give rise to a an *Actio Iniuriarum* for wrongful intrusion on personal privacy or disclosure of private facts.[308] With reference to the constitutional right to privacy, it should be noted that Article 13 of the Interim Constitution of South Africa, 1993 (Interim Constitution)[309] is similar in essence to Article 14 of the Constitution of South Africa, 1996 (Final Constitution). The guarantee of the right to privacy is twofold. First, it protects the right to privacy positively, and second, it ensures non-interference with the listed protections in subparagraphs (a) – (d) as mentioned in Article 14 of the Constitution. De Waal, Currie and Erasmus emphasize that the second part is part and parcel of the general right to privacy.[310]

Thus, the right to privacy exists in common law and it is now given force as a fundamental constitutional right. It is therefore up to the Courts to interpret and develop the common law to bring it in line with the Constitution. The preamble and the founding provisions in the Constitution clearly confirm the sovereignty principle

---

[308] De Waal, Johan; Currie, Iain and Erasmus, Gerhard (2001) *The Bill of Rights Handbook* at 268. The reference is to the 4th Edition, however the Handbook has later editions, most recent is Currie, Iaian and de Waal, Johan (2013) *The Bill of Rights Handbook* 6th Edition.

[309] Op cit note 298, *Mistry v Interim Medical and Dental Council of South Africa.*

[310] Op cit note 308, *The Bill of Rights Handbook* at 267.

and the supremacy of the Constitution, while at the same reinforcing the country as a democracy founded on the value of human dignity, equality and advancement of human rights and freedoms.[311]

Privacy for everyone in the jurisdiction

From the case involving the Certification of the Constitution, it is clear that South Africa recognizes that the rights outlined in the Bill of Rights are universal rights. As stated by the Constitutional Court: '*Everyone* shall enjoy all universally accepted fundamental rights, freedoms and civil liberties, which shall be provided for and protected by entrenched and justiciable provisions in the Constitution.'[312] Since the rights are afforded to everyone, this should be taken to mean that it applies equally to all migrants in the country without distinction, unless there is a justifiable limitation to the enjoyment of the rights.

Balancing competing rights

Although the right to privacy is a fundamental right enshrined in the Constitution, it is not absolute and can be limited in accordance with the limitation clause in Article 36. This allows for a limitation to the right to privacy in terms of law of general application as the right to privacy has to be balanced with other rights entrenched in the Constitution. When balancing competing rights, a two-stage approach is adopted: first, the scope of the right is looked at in order to determine if there is an

[311] Article 1 (a) of the Constitution of South Africa, 1996.

[312] *Certification of the Constitution of the Republic of South Africa* 1996 (10) BCLR 1253 (CC) at 48.

infringement; and second, it is questioned whether the infringement to the right is justified in terms of general law of application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. For this balancing test the following factors are taken into account: the nature of the right, the importance of the limitation, the nature and extent of the limitation, the relation between the limitation and its purpose, and the less restrictive means to achieve the purpose.[313] In *S v Makwanyane and Another*, the Constitutional Court held that there is no absolute standard for determining reasonableness and justifiability; instead, whether the purpose of the limitation is reasonable and justifiable will depend on the circumstances to be determined on a case-by-case basis.[314]

Privacy right includes data protection

De Waal explains that the constitutional right to privacy is protected by the private law action *Actio Iniuriarum* and the common law right of privacy is protected by the law of delict. However, when it comes to data protection the situation is less clear. Notwithstanding the fact that the Constitution does not expressly refer to data protection, the most dominant argument is that information privacy is encompassed in the constitutional protection of privacy.[315] They say that privacy is essentially what feels private, although that feeling has to be a reasonable one shared objectively rather than entirely personal or eccentric.[316] This is also evident in the definition adopted by

[313] Article 36 of the Constitution of South Africa, 1996.

[314] *S v Makwanyane and Another* 1995 (6) BCLR 665 (CC) at 708.

[315] Op cit note 308, *The Bill of Rights Handbook* at 269.

[316] Ibid, *The Bill of Rights Handbook* at 269.

the Constitutional Court, as early as 1996, where it held in *Bernstein v Bester NO*[317] that: 'The concept of privacy in the Bill of Rights extends to those aspects of existence in regard to which a legitimate expectation of privacy can be harboured. A legitimate expectation of privacy has two components; one is a subjective expectation of privacy [...] that the society has recognized [...] and the other, is that it is objectively reasonable.' The *Bernstein case* was the first case to interpret the constitutional right to privacy.

Burchell states that 'the very essence of the right to privacy is that individual citizens are able to move around freely, without their comings and goings being recorded somewhere and without the possibility of such information falling into the wrong hands.' This, he says, 'was one of the most hateful aspects of apartheid - the ability of the State to infringe on and control every aspect of citizens lives.'[318] Having drawn from constitutions and freedom charters in developed democracies and after a vigorous comparative analysis to gather the best practice principles that are most suitable to South Africa, it could be argued that the Constitution is one of the most advanced constitutions in the world. Article 14 specifically protects the fundamental right to privacy, which includes the right not to have the privacy of communications infringed upon.

---

[317] *Bernstein v Bester NO* 1996 (2) SA 751 (CC) at 71 – 75.

[318] Op cit note 301, *The Legal Protection of Privacy in South Africa: A Transplantable Hybrid*

Informational privacy / data protection right

Neethling states that 'the processing of personal information threatens personality rights in two ways; firstly, compiling and processing personal information is directly linked to the individual's privacy; and secondly, the acquisition and disclosure of false or misleading information may lead to infringement of the individual's identity.[319] He defines privacy 'as an individual condition of life characterised by exclusion from publicity. This condition includes all those personal facts which the person himself or herself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he or she evidences a will for privacy.'[320] Thus, an individual's right to privacy entails control of personal information free from unwanted intrusions.[321]

In *Mistry v Interim Medical and Dental Council of South Africa* (*Mistry* case) the Constitutional Court went so far as to assume that even though breach of informational privacy was not expressly mentioned the Constitution, it would be covered by the broad protection of the right to privacy as guaranteed in the Constitution.[322] This allows for reading-in the right to data protection into the provisions of Article 14.[323] It should be noted though that the *Mistry* case explicitly left open the issue of whether the right to informational privacy could potentially reside in the right to access

[319] Neethling J, Potgieter JM and Visser PJ (2005) *Neethling's Law of Personality* at 270 - 271.

[320] Ibid, *Neethling's Law of Personality* at 32.

[321] South African Law Reform Commission (2005) 'Privacy and Data Protection: Discussion Paper 109' at 1-4 <http://www.doj.gov.za/salrc/dpapers.htm>. The Discussion Paper followed an earlier Issue Paper on the same topic (SA Law Reform Commission *Privacy and Data Protection* (Issue Paper 24 August 2003).

[322] Op cit note 298, *Mistry v Interim Medical and Dental Council of South Africa* at 14.

[323] Neethling's definition of privacy was, for example, accepted in the *Bernstein v Bernstein* case. See later discussion on the case law and the Constitutional Court pronouncements in this Chapter.

information as guaranteed by Article 32 of the Constitution. Nevertheless, access to information is part and parcel of data protection as seen in other jurisdictions, therefore, the right to access information should be read together with the right to privacy when focusing on data protection. The South African Law Commission's background paper to the Protection of Personal Information Bill also refers to data protection as an aspect of the right to privacy that is a fundamental human right given force by the Constitution.[324]

Development of specific data protection law

In South Africa the need for a specific law on data protection was recognized as early as 1994 when developing the Access to Information Law.[325] The Task Group on Open Democracy in considering legislative changes that were required for an open and democratic society, as opposed to the authoritarian and secretive Apartheid state, identified four principle laws: (1) freedom of information legislation applicable to information held by government bodies, (2) data privacy legislation providing for the correction of and protection against unauthorised use of personal information held by both government and private bodies, (3) open meetings legislation requiring government meetings to be open to the public, and (4) legislation for the protection of whistleblowers. These laws eventually together formed the Promotion of Access to Information Act of 2002 (PIAI), but the data privacy legislation was deliberately taken out because the Task Group was of the opinion that the PIAI should only deal with

[324] Op cit note 321, 'Privacy and Data Protection: Discussion Paper 109' at 4.

[325] Currie, Iain and Allan, Kate (2007) 'Current Developments: Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa' 23 *SAJHR* at 564.

access to information and not other privacy issues which found a better place in a separate piece of legislation in line with data protection statutes in other jurisdictions.[326]

While there was a clear objective to create data protection legislation, it has taken over a decade to find its shape. An alternative reason is that information privacy would find expression in access to information rights. This is plausible but while the right of an individual to access information relating to oneself is one of the commonly accepted data protection principle as mentioned in chapter 3, it is unclear why PIAI remained silent on data protection if this was indeed the intension. In any event, access rights only form part of data protection and does not cover all aspects related to it. Therefore a specific right to data protection is needed.

The data protection law was eventually placed again on the South African legislative agenda in 2000. An Issue Paper by the Law Commission was published in September 2003 and Discussion Paper No. 109 on Privacy and Data Protection was published in October 2005 together with the draft Protection of Personal Information Bill. A large volume of comments was received, the Bill was revised accordingly, and it was tabled at Parliament. Parliament recently approved the Bill on 22 August 2013 and the Presidential signed it into force on 26 November 2013. Following the parliamentary

[326] Ibid, 'Current Developments: Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa' at 566. Roos, Anneliese agrees that a separate legistlation was envisaged and provides an overview of relevant data protection principles in the Open Democracy Bill to illustrate this, for further detail, see: Roos, Anneliese (2000) 'Data Protection for South Africa: Expectations Created by the Open Democracy Bill' at 43.

debate, the Deputy Executive Director of the Open Democracy Advice Centre, Mukelani Dimba, said that 'it was a great moment of elation [...] the committee heard from various stakeholders from all walks of life and worked very closely with civil society organisations and constitutional bodies to incorporate most of the proposals made by the public.'[327] During the drafting phase, the South African Law Commission recognized that data protection could not be seen simply as a domestic issue because the increased ease of transmitting personal data outside borders called for a harmonized approach as seen in other jurisdictions.[328]

The South African Law Commission steered away from stating that the data protection law is human rights based, instead they stated that the law was being introduced as a package of laws intended to facilitate electronic commerce by setting up uniform rules.[329] Even if the law was not developed from a human right perspective, it does recognize data protection as a fundamental human right and this is echoed throughout the South Law Commission Paper.[330] This attitude is similar to the approach adopted in Europe where they focused on the objective of facilitating the transfer of personal data, however, they are now realizing the importance of ensuring that the law is indeed human rights based as evidenced by the EU data protection reform. The drafters in South Africa should not have followed the EU model in this regard, knowing that their laws were under revision; instead by explicitly recognizing the human rights

[327] See: The Freedom of Information website 'South African to create Information Regulator' 10 December 2012 <http://www.freedominfo.org/2012/12/south-africa-to-create-information-regulator/>

[328] Op cit note 321, 'Privacy and Data Protection: Discussion Paper 109' at 6.

[329] Ibid, 'Privacy and Data Protection: Discussion Paper 109' at 12.

[330] Ibid, 'Privacy and Data Protection: Discussion Paper 109.'

perspective they could have been at the forefront stating that data protection laws should be human rights based. This was a missed opportunity.

Nonetheless, it is clear from the South African Law Commission's final report that 'data protection forms an element of safeguarding a person's right to privacy. It provides for the legal protection of a person in instances where his or her personal information is being collected, stored, used or communicated by another person or institution.'[331] The law therefore provides for a statutory right to data protection stemming from the right to privacy and this should be read together with the constitutionally guaranteed right to privacy and access to information, the common law *Actio Iniuriarum* and constitutional jurisprudence on information privacy. The Protection of Personal Information Act will be discussed in more detail in section 5.2

i) *Constitutional court case NM and Others v Smith and Others*

This section looks in detail at the constitutional case *NM and Others v Smith and Others* 2007 (7) BCLR 751 (CC) (*NM* case) with the view to determine the gaps in the South African law. The analysis supports the view that the right to privacy should extend to HIV/AIDS status as a private fact, particularly since it relates to highly sensitive personal data, and questions whether the common law should have been

[331] South African Law Reform Commission Project 124 (2009) 'Privacy and Data Protection Report' Pretoria, South African Law Commission.

developed to impose liability on the negligent public disclosure of private and confidential information.

It should be noted at the outset that the development of the *Actio Iniuriarum* in previous cases of defamation[332] is not automatically applicable to cases involving the disclosure of private facts. Firstly, privacy in the context of defamation is distinguishable from privacy in the context of HIV/AIDS.[333] This is because defamation involves damage to the reputation of an individual, whereas disclosure of HIV/AIDS status involves infringement on the autonomy to choose the conditions upon which private medical information should be revealed to the public. Secondly, the law of defamation essentially protects the publication of untrue facts. The disclosure of medical information, however, deals with private facts that are true.

HIV/AIDS status is a highly sensitive private fact

The Majority decision correctly accepts that HIV/AIDS status is a private fact. HIV/AIDS unfortunately carries a negative stigma in our society. Although, as former justice O'Regan suggests in the Minority decision, we wish not to elevate HIV/AIDS above other diseases, we cannot ignore the reality that the social stigma attached to this particular disease far outweighs other diseases.[334] Recognizing this reality does not surmount to the reinforcement of the stigma, instead it takes account of the social

[332] Op cit note 303, *Holomisa and Bogoshi* cases. Also confirmed in the *NM case* at para 175, op cit note 302.

[333] Op cit note 302, *NM* case, for a further discussion on the difference between privacy and defamation in O'Regan J's dissent judgment at para 175-182.

[334] Ibid, *NM* case at para 138-141.

reality of people living with HIV/AIDS in our society. Unfortunately the social stigma of HIV/AIDS is reflected in the High Court judgment which suggests that people living in poorer sectors of society are less at risk of being socially stigmatized because of their levels of literacy and social standing in society.[335] Statistics in newspaper articles show that HIV/AIDS is more prevalent in poorer communities and that individuals are often ostracized when their status become known to family and community members. The social stigma is not only attached to the broader community of people actively involved in politics or to those who are known for their contributions to society. Many indigent persons live with the harsh realities of the social stigma and often do not have the resources and avenues available to them to protect their rights.

O'Regan J highlights the vulnerability of the applicants in this case and correctly states that 'this case reminds one of the profound vulnerability of those in the situation of the three applicants in many respects, but not least in relation to their ability to gain access both to medical care and legal advice [...], the facts of this case serve as a reminder of the need to ensure that medical care and legal advice be tendered to those who are as vulnerable as the applicants, in the best interests of those to whom it is provided, and with scrupulous attention to the demands of professional ethics at all times.[336] Discriminating between different classes of people suggests that poor people suffering from the disease do not form part of the broader social community. It serves as a secondary victimization which further enhances the stigma attached to the disease. The

[335] Ibid, *NM* case at para 53.

[336] Ibid, *NM* case at para 199.

Constitutional Court correctly rules that such discrimination of social class is not tolerable in our democratic society[337] and that poor people should be afforded the same protections of privacy regardless of their social standing, wealth or literacy levels.

Constitutional protection of information privacy

With one of the most advanced constitutions in the world, the South African Constitution affords protection to the right to privacy.[338] In the dissent judgment, O'Regan J puts forward two reasons why the right to privacy is constitutionally protected.[339] 'Firstly, as human beings we enjoy a sphere of personal intimacy and autonomy, and we should have a right to privacy in this regard because it serves to protect and foster the right to dignity which is a core protection in the Constitution. As a result, individuals hold the rights to personal information and this right extends to the choice as to when such information should be divulged to the public.[340] Secondly, privacy is entrenched in the Constitution as a result of our past. It ensures that the belongings and personal information of members of a democratic society are protected from the State. Medical information is intimately private and everyone should enjoy the freedom to choose when and to whom they wish to divulge this sensitive information.'[341] This is an unequivocal recognition that the right to privacy in the

---

[337] Ibid, *NM* case at para 53.

[338] In the United States, for example, there is no expressed protection for privacy in their Constitution. There have been decades of debate calling on reasons for maintaining privacy as a constitutional guarantee as opposed to questions whether it is in the public interest to allow the public the benefit of disclosure. Although the right to privacy is not constitutionally guaranteed it has been invoked through other provisions in the Constitution. Cases involving such interpretation usually involve the First, Fourth, Fifth and Ninth Amendments.

[339] Op cit note 302, *NM* case at para 131-134.

[340] Ibid, *NM* case at para 136.

[341] Ibid, *NM* case at para 136

Constitution includes information privacy/data protection. In South Africa the confidentiality of HIV/AIDS status is captured in several important sets of ethical guidelines on the treatment of medical data.[342] However, there is no law in force that governs the violations of data protection and the consequence of infringing upon the privacy and misuse of medical data.

Comparative jurisprudence on highly sensitive medical data

UNAIDS states that 'the risk of harm following a breach of confidentiality of HIV varies with the national or local context according to levels of stigma, lack of comprehensive public health safety nets, legal traditions of respect of privacy, religious perspectives, and other local conditions.[343] Regardless of the context though, the importance of data protection is increased in the context of HIV/AIDS status, which should be treated as a private fact. Generally, the courts in the United States have recognized medical information as a private fact. In *Schaill v. Tippecanoe County Sch. Corp.* the Court recognised a substantial privacy interest in the confidentiality of medical information.[344] In *Denius v. Dunlap* the Court stated that 'the "concept of ordered liberty" protected by the Fourteenth Amendment's Due Process Clause has been interpreted to include 'the individual interest in avoiding disclosure of personal matters.'[345] In *Arakawa v. Sakata* the Court held that 'the release of a Social Security

---

[342] These professional ethical guidelines include amongst others the Health Professions Council of South Africa (HPCSA) Guidelines of 2001, the South African Medical Association (SAMA) Guidelines, and the South African Nursing Council (SANC) Guidelines (ALP 2007).

[343] Op cite note 144, 'Guidelines on Protecting the Confidentiality and Security of HIV Information' at 23.

[344] *Schaill v. Tippecanoe County Sch. Corp.*, 864 F.2d 1309, 1322 n.19 (7th Cir. 1989).

[345] *Denius v. Dunlap* 209 F. 3d 944 (7th Cir. 2000).

number potentially rises to the level of a federal constitutional violation, especially when considering the amount of highly personal information that can be recovered as a result of its release.'[346] More specifically, in *Urbaniak v. Newton* the California Court of Appeal held that HIV positive status is clearly a private fact because the disclosure of it may be offensive and objectionable to a reasonable person of ordinary sensibilities.[347]

In *Multimedia WMAZ, Inc. v. Kubach* the Court held that 'unlike the identities of those involved in crimes, the identities of those suffering from AIDS are generally not a matter of public interest.'[348] In *Doe v. Town of Plymouth* the Court held that the plaintiff infected with the HIV virus had a constitutional right to privacy that encompassed non-disclosure of her HIV status, in this regard: 'Given the social stigma associated with the HIV and AIDS phenomenon, courts are especially vigilant in enforcing the individual privacy interest in avoiding disclosures. One court poignantly captured the high stakes of unwarranted and non-consensual disclosure. There are few matters of a more personal nature and there are few decisions over which a person could have a greater desire to control, than the manner in which he reveals that AIDS diagnosis to others. An individual's decision to tell family members as well as the

---

[346] *Arakawa v. Sakata* 133 F.Supp.2d 1223 (D. Haw. 2001).

[347] *Urbaniak v. Newton* 226 Cal.App.3d 1128 (1991).

[348] *Multimedia WMAZ, Inc. v. Kuba*212 Ga. App. 707, 443 S.E.2d 491 (Ga. App. 1994). In this case the plaintiff appeared on a television program in which he was interviewed about having contracted AIDS. Prior to the programme, the plaintiff and defendant reached an understanding that the Plaintiff's face would be disguised digitally so that he could not be identified. Apparently, due to the negligence of station employees, the plaintiff was recognizable at the beginning of the show. The Court held that the plaintiff had a claim because his right to privacy was infringed. In *Mason v. Regional Medical Center of Hopkins Cty*, 121 F.R.D. 300 (W.Dist. Ky 1988) the sensitivity of HIV status was similarly pronounced upon when the Court held that the status of a HIV-positive individual had to be kept confidential in court proceedings.

general community that he is suffering from an incurable disease, particularly one such as AIDS, is clearly an emotional and sensitive one fraught with serious implications for the individual.'[349]

The stigma associated with HIV/AIDS was similarly outlined in *Doe v. Coughlin* where the Court recognized the discrimination accompanying public dissemination of the diagnosis and the fact that family members may abandon the HIV/AIDS victim. The Court had to determine the nature and extent of the privacy rights of inmates who were tested HIV positive and balance that privacy interest against the asserted interest of the New York State Department of Correctional Services. The Court stated that: '[...] The objectives of the State are served in a constitutionally impermissible manner. Without question, those assigned to D-2 (the cell section) will be known by guards and the general prison population to be infected by the HIV virus and these inmates also face a substantial risk of having their diagnosis revealed to family members and friends. To justify these invasions, the State argued that its program is the most appropriate means of accomplishing its interest, however, the benefits are insufficient standing alone to warrant permitting infringement of the prisoner's right to privacy.'[350]

---

[349] *Doe v. Town of Plymouth* 825 F.Supp. 1102, 1107 (D.Mass. 1993). In this case the plaintiff sued on the basis of emotional distress against town and police officer, alleging civil rights claims arising out of disclosure of her HIV positive status. The Court held that the Constitution protects two types of privacy interests namely, individual interest in avoiding disclosure of personal matters, and interest in independence in making certain kinds of important decisions.

[350] *Doe v. Coughlin* 697 F.Supp. 1234 (N.D.N.Y.1998).

Disclosure of HIV/AIDS status

It should be noted that the right to privacy in the context of HIV/AIDS disclosure is not without limitation. In *Estate of Behringer v. Medical Center* the Superior Court of New Jersey held that: '[...] Although New Jersey's anti-discrimination statutes protected Dr. Behringer from having his surgical privileges revoked, the Medical Center demonstrated a reasonable risk to patients that justified suspending Dr. Behringer's privileges, or alternatively, requiring his patients' informed consent before operating. The Court found that the risk included not only actual HIV transmission, but also the possibility of surgical accidents.'[351] In *Doe v. City of New York* the Human Rights Commission was sued for revealing information identifying the plaintiff as an HIV/AIDS victim.[352] O'Neil states in his comment on the case that 'the Court recognized that AIDS infection is profoundly different from any other embarrassing revelation, and hinted that liability might follow even for the truthful disclosure of lawfully obtained information of obvious public importance. In this case there was another special feature, the purpose for which the infected worker sought the agency's help did not include publicizing its victory at his expense for its own ends.'[353]

---

[351] *Estate of Behringer v. Medical* Center 249 N.J.Super. 597 (1991). In this case the Medical Center had breached its duty of confidentiality when it failed to take reasonable precautions to prevent the patient's AIDS diagnosis from becoming public knowledge.

[352] *Doe v. City of New York* 15 F.3d 264 (2d Cir. 1994). In this case an airline employee was fired because he was AIDS infected. With the assistance of the city Human Rights Commission he successfully regained his job. The Commission then issued a celebratory press release, which without naming the employee, contained enough details that friends and colleagues could identify the person. The Commission was then sued for invasion of privacy.

[353] O'Neil, Robert M 'Privacy in the New Millennium: Virtual Trespass and Other Concepts' <http://www.abanet.org>

The above cases on HIV/AIDS are drawn from United States jurisprudence to illustrate the way in which courts in a foreign jurisdiction have addressed the sensitivity surrounding HIV/AIDS status. In the European context where data protection is explicitly recognized as a human right, the European Court of Human Rights stated that: 'Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the European Union. It is crucial not only to respect the sense of privacy of a patient, but also to preserve his or her confidence in the medical profession and in the health services in general [...]. The disclosure of HIV data may dramatically affect his or her private and family life, as well as social and employment situation, by exposing him or her to opprobrium and the risk of ostracism. For this reasons it may also discourage persons from seeking diagnosis or treatment and thus undermine any preventive efforts by the community to contain the pandemic. The interests in protecting the confidentiality of such information will therefore weigh heavily in the balance in determining whether the interference was proportionate to the legitimate aim pursued. Such interference cannot be compatible with Article 8 of the EU Charter unless it is justified by an overriding requirement in the public interest.'[354]

Thus, HIV/AIDS status is recognized as a special category of personal data that requires a higher standard of protection given the sensitivity of medical data and the social stigma attached to this disease and, as a result, confidentiality and non-disclosure weighs heavily when balancing this right against other rights or interests.

[354] European Court of Human Rights (Chamber) Case of Z b. Finland (Application no. 22009/93), Judgment, Strasbourg, 25 February 1997 at 95 – 96.

Specific issues in the NM case

The applicants in the *NM* case claimed that the publication of their names and HIV/AIDS status without expressed consent violated their rights to privacy, dignity, and psychological integrity. Although Article 14 of the Constitution was not directly invoked because of limitation in *Fose v Minister of Safety and Security*,[355] this constitutional protection does apply when looking at interpretation and development of the common law.[356] The applicants were volunteers to clinical trials conducted by the Immunology Clinic in the Medical Faculty of the University of Pretoria. The clinical trials tested a drug aimed at reducing the HIV levels of patients. The Strauss Report, which resulted from an investigation looking into the side effects of the drug, contained an annexure revealing the terms upon which the applicants consented to the publication of their identities and HIV/AIDS status and this did not include wide public dissemination.

Facts of the case

In a biography of Ms. Patricia de Lille (an active political figure), the author relied on the Strauss Report as a basis to publish the applicants' personal details. Neither the author nor Ms. de Lille viewed the annexure containing the limited consent of the applicants and they claimed damages on the basis that no expressed consent was given

[355] *Fose v Minister of Safety and Security* 1997 (3) SA 786 (CC) at paras 17-19 the Court held that if a matter is brought on the basis of common law the Court has to decide on this basis. In the *NM case* applicants invoked common law infringement and not the constitutional infringement.

[356] According to Article 39 of the Constitution: 'When interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights.

to publication of their names and status in the biography. Prior to instituting litigation, the applicants requested that their names be removed from the book, but the respondents' response was that they had no obligation to do so and that any legal action would be defended.[357] In the High Court proceedings, the respondents claimed that no confidentiality phrase was attached to the Strauss Report, and that in any event, the details of the applicants were not private facts at the time of the publication to warrant the protection of the right to privacy. The respondents claimed further that their actions were neither intentional nor negligent and that they had not acted unlawfully because it was reasonable to assume that they had attained the consent of the applicants as consent was given to publication in the Strauss Report.

The reason given for publishing the applicants' names and HIV/AIDS status was to authenticate the material in the biography.[358] This reason is unjustified. Assumption of consent is not sufficient particularly since the annexure, which formed an integral part of the Strauss Report, was evidence that the consent was limited to the Straus report and not to other publications. Consent signifies the unambiguous intent and will of the individuals concerned. In determining whether consent was validly given, one needs to look at the individuals' intention at the time of collecting consent, the specified purpose for which consent was obtained, the fact that the individuals should be made aware of all circumstances surrounding the collection and disclosure of their personal data, and the intended audience if publication is foreseen. In addition, the individuals need to be fully informed of wide public dissemination and its consequences if this

[357] Op cit note 302, *NM* case at para 7-20.

[358] Ibid, *NM* case at para 22-24.

forms part of the specified purpose.[359] It is clear from the facts that the applicants only gave consent for the specified purpose of the medical report in order to investigate the conduct of the staff at the University in conducting medical trials and the consent was limited to this purpose. According to international standards on data protection, consent to use personal data needs to be obtained for a specified purpose and using such personal data for any additional or unrelated purpose would require taking additional steps to obtain express consent for the new purpose. The applicants in no way gave expressed consent for publication in the biography and no real steps were taken by the author or Ms. De Lille to obtain the necessary consent or to even check the annexure that outlined the limitations of consent. In essence, the biography resulted in a hagiography of a political figure at the expense of infringing upon the privacy of vulnerable individuals.

Analysis of the Constitutional Court judgment

The Constitutional Court proceeded on the basis that the matter did not raise a constitutional issue. This was due to the fact that the applicants' claim was based on the common law principle of *Actio Iniuriarum.* The Court, however, found that it was in the interest of justice to hear the matter because it raised important considerations of balancing between the rights to freedom of expression on the one hand, and the right to privacy and dignity, on the other.[360] The Court correctly concludes that consent to the Strauss Report did not give a blanket disclosure to publication.[361] If the

[359] Op cit note 5, *IOM Data Protection Manual* at 41.

[360] Op cit note 302, *NM* case at para 27-31.

[361] Ibid, *NM* case at para 39.

respondents had taken the necessary steps to view the annexure they would have been aware of the fact that the consent was limited to the medical report. Private medical information is very sensitive and considering the negative impact that disclosure of HIV/AIDS status can have on the everyday lives of individuals, extra measures need to be in place to protect the right to privacy in this context. In a society rated with one the highest numbers of infected people, and where those infected face constant barriers within their respective communities, the potential long-term negative effects of disclosure have to be taken into account. The unauthorized disclosure of personal information, which could potentially result in harm, should give rise to a claim for damages. Unfortunately, the Constitutional Court missed a unique opportunity to develop the common law in light of the constitutional right to privacy.[362]

The Constitutional Court has pronounced on many occasions on the fundamentality of freedom of expression in a free and democratic society[363] and the respondents relied on this in their defence. The respondents and the *Amicus Curiae* contended that developing the common law to encompass the component of negligence, as an element of fault, would limit the right to freedom of expression. This argument is flawed. While freedom of expression remains a corner stone of democracy, it cannot be

---

[362] This argument is supported by Steinberg, Jonny in his critique of the *NM case*. See: Jonny Steinberg, Jonny '*Generous Judgment Instils Stigma'* Business Day, 24 April 2007 <http://www.businessday.co.za/articles/topstories.aspx?ID=BD4A445289>

[363] See: for example, *S v Mamabolo (E TV and Others Intervening)* 2001 (3) SA 409 (CC); *Islamic Unity Convention and Others v Independent Broadcasting Authority and Others* 2002 (4) SA 294 (CC); *Khumalo and Others v Holomisa* 2002 (5) SA 401 (CC); *Laugh it Off Promotions CC v SAB International (Finance) BV t/a SabMark International (Freedom of Expression Institute as Amicus Curiae)* 2006 (1) SA 144 (CC); *South African National Defense Union v Minister of Defence and Another* 1999 (4) SA 469 (CC), and *Phillips and Another v Director of Public Prosecutions, Witwatersrand Local Division, and Others*2003 (3) SA 345 (CC).

exercised to the detriment of other constitutional guarantees.[364] A balancing test is usually implemented in cases involving private medical records, between the individual's right or expectation of privacy and the public interest in accessing their medical records. Drawing from foreign jurisprudence, in the case of *Whalen v Roe* the Court in examining the asserted privacy rights of patients, identified two constitutional privacy interests: 'One is the individual interest in avoiding disclosure of personal matters, and another is the interest in making certain kinds of important decisions that affect the public. In addition, publicizing the private medical information of a person can only be warranted if it raises a legitimate concern or interest to the public.'[365] The Court in *United States v Westinghouse Elec. Corp.* set out seven factors to consider when determining whether an intrusion into an individual's privacy is justified, these include: 'the type of record requested; the information it does or might contain; the potential harm in any subsequent non-consensual disclosure; the injury from disclosure to the relationship in which the record was generated; the adequacy of safeguards to prevent unauthorized disclosures; the degree of need for access; and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.'[366] This case sets forward good criteria for balancing privacy rights with other rights and our courts could benefit from these guidelines when looking at data protection cases in the future.

---

[364] The Constitutional Court expressed this view in the cases of *Khumalo v Holomisa* 2002 (5) SA 401 (CC) at paras 22-24 and *South African Broadcasting Corporation v National Director of Public Prosecutions and Others* 2007 (2) BCLR 167 (CC) at para 24.

[365] *Whalen v Roe* 429 U.S 589 (1977). See also op cite note 349, *Doe v. Town of Plymouth.*

[366] *United States v Westinghouse Elec. Corp.* 638 F.2d 570 (3rd Cir. 1980). This case involved facilitating research and investigations of the National Institute for Occupational Safety and Health, and questioned whether strong public interest justified minimal intrusion into privacy with regard to the medical records of employees.

O'Regan J in the *NM* case agrees with the respondents that expanding the common law would limit freedom of expression[367] and states that: 'Media Code of Ethics is usually relevant in determining whether public interest dictates that privacy rights should be limited.[368] The names and HIV/AIDs status of the applicants were simply used to authenticate that Ms. De Lille was an HIV activist, this is not a legitimate reason for infringing upon the applicants' right to choose when and to whom they wished to disclose their personal data. There was also no public interest in printing their names in a biography that seems to be aimed at wide public dissemination for the purpose of enhancing personal political support from the general public.

The judgment of Sachs J is particularly helpful when considering the balancing test between the right to privacy and the right to freedom of expression.[369] Sachs J recognizes that there is a greater need for caution when the private fact involved is significantly private to the individual involved, and conversely that the greater the public interest, the greater the likelihood of limiting the individuals' right to privacy. In particular, he says: '[...] Given the extreme sensitivity of the information involved, she (Ms. de Lille) should have left no stone unturned in her pursuit of verification. Of even greater importance, if the slightest doubt existed, there was no need to publish the actual names of the applicants [...]. There might be some cases where the need for verisimilitude, a sense of actuality, may be overwhelming [...]. We are concerned with

[367] Op cit note 302, *NM* case at para 183-189.

[368] Ibid, *NM* case at para 149.

[369] Ibid, *NM* case at para 203-204.

people whose lives are dominated by anxiety and who are only slowly beginning to break through intense barriers of community prejudice [...]. When the expressive interests are balanced against the privacy interests, the scales come down with a clang on the side of privacy.'[370]

Former Chief Justice Langa[371] and O'Regan J[372] correctly held that a higher standard should be attributed to the media who are responsible for ensuring that freedom of expression does not encroach on individual rights. However, ordinary citizens should also be held to the standard of a reasonable person in light of the circumstance of a particular case. Langa CJ's reasoning that Ms. de Lille would escape liability by virtue of the fact that she is a layperson[373] is not correct. The political status of Ms. de Lille and the fact that she is a HIV/AIDS activist makes her well-versed in the potential harm that can flow from the disclosure of HIV/AIDS status. A reasonable person in her position would have taken all the necessary steps to attain the consent of the applicants prior to wide public dissemination. If the Constitutional Court developed the common law they would have found a case of negligence. However, O'Regan J on her summary of the facts, finds that the respondents did not act negligently. This is mainly attributed to the significant burden that would be placed on freedom of expression if the media could not rely on information published by reputable organizations.[374] This analysis fails because when compared to lay persons, the

[370] Ibid, *NM* case at para 205-207.

[371] Ibid, *NM* case at para 94

[372] Ibid, *NM* case at para 180.

[373] Ibid, *NM* case at para 99

[374] Ibid, *NM* case at para 183-189.

University testing HIV/AIDS patients and Ms. De Lille's (as well as her author) who had in-depth knowledge of HIV/AIDS and the consequences of unwanted disclosure had an additional obligation to ensure that constitutional rights are not infringed upon by their publications. This includes taking steps to ensure that consent is obtained when publishing private medical facts for particular purposes. The fact that the applicants' had given the University consent to publish their names in the Strauss Report containing results of the test did not relieve the respondents from the obligation to take all the relevant steps of ensuring that proper consent was in fact obtained for the purpose of publishing the biography. This goes to the issue of the functional creep. Simply stated, providing consent to the University for the specified purpose of the Straus Report does not mean that applicants gave an unfettered right to other writers to use their personal data for other purposes that are not known to them. It should make no difference that the information had been previously published, the obligation is to confirm consent for unrelated purposes remains, particularly in matters as sensitive as HIV/AIDS status.

Given the social stigma attached to HIV/AIDS status in our society, it is not unreasonable to require confirmation of consent. This does not imply that HIV/AIDS as a disease should be given preferential status. It merely takes the social reality of the disease into account and turns the focus to the intimacy of the private facts involved. The following passage of Sachs J supports this contention: 'From a legal point of view, then, the moral of the story is that unless overwhelming public interest points the other way, publishers should refrain from circulating information identifying the HIV status of named individuals, unless they have the clearest possible proof of consent to

publication having been given, or that the information is in the broad public domain.'[375] The protection of the right to privacy under the common law *Actio Iniuriarum* requires the elements of wrongfulness and the intention to impair one's privacy. In the context of the disclosure of HIV/AIDS status, the common law falls short of protecting an individual's rights in the circumstance where a reasonable person ought to have foreseen the potential harm that would result from disclosure. As criticized by Steinberg, the Constitutional Court focused too much on intent when negligence was not in dispute and it should have gone further to develop the common law to include the element of negligence,[376] particularly in the absence of legislation regulating data protection.

Majority view

Former justice Madala, writing for the Majority, felt that there was no need to develop the common law in light of the facts of this particular case.[377] Many aspects of the facts of this case were, however, not common cause in the court a quo. Suffice to say, there was disagreement about the nature of the consent given and content of information revealed in meetings leading up to the court proceedings. The respondents alleged that in allowing the presence of journalists at one of the meetings, the applicants waived their right to privacy. On examination of the facts it was established that the applicants' did not reveal their status at the meeting when the media was present. It is also clear from the evidence that the Strauss Report was intended as an

[375] Ibid, *NM* case at para 183-189.

[376] Op cit 362, 'Generous Judgment Instils Stigma'.

[377] Op cit note 302, *NM case* at para 57.

investigation into the conduct of the University within the context of the clinical trials. The fact that the University is a reputable institution does not result in the report being made public for broader use contrary to the intension of the applicants. The report was not stored in the library archives making it accessible to the public and it was only circulated to those involved and who had an interest in the results of the report. As the former Langa CJ states: 'Whether it is reasonable to rely on another document will depend on the nature of the document, the nature of the institution that produced the document, the importance of vindicate the interests involved and the relevant circumstances of the case.'[378]

Minority view

While it can be argued that the necessary requirement of intention for wrongfulness was not present in their conduct, the respondents acted negligently in publishing the names and status' of the applicants.[379] Indeed the respondents would not have deliberately tried to inflict harm through their publication, particularly because their involvement with the applicants stemmed from an intention to assist those who experienced negative effects as a result of the clinical trials. In addition, the background and experience of the first and second respondent in dealing with HIV/AIDS issues indicate that they would not intentionally reveal the identity of

[378] Op cit note 302, *NM* case at para 102.

[379] No defense was put forward to rebut the allegation that the respondents acted wrongfully, it was also never established that it was in the public interest to disclose the applicants' private medical information.

HIV/AIDS persons. Therefore, the partial dissent of Langa CJ[380] and the dissent of O'Regan J,[381] in this regard, is correct.

Ms. de Lille and her author acknowledged that Media Ethics prevented publication of private facts without consent. During testimony it was alleged that steps were taken to obtain sight of the annexure containing the terms of consent of the applicants. Those steps, however, fell short of the necessary steps needed to prevent harm to the applicants. A reasonable author of a biography that referred to personal medical information and a person in the position of Ms. De Lille who is well-versed in the social stigma and sensitivities attached to HIV/AIDS, would have foreseen the consequence of their negligence in not taking all the necessary steps to ensure that consent for disclosure had been obtained. Clearly the element of negligence was present and the facts of this case did call for the development of the common law so as to bring it in line with constitutional right to privacy. The negligence of the respondents resulted in the publication of private facts, which caused harm to the applicants and violated their rights to dignity by encroaching upon their freedom not to have their private information revealed to the public.

As confirmed by the Constitutional Court dignity is a fundamental constitutional right,[382] and therefore, a negligent action that results in the impairment of the right to

[380] Op cit note 302, *NM* case at para 93.

[381] Ibid, *NM* case at paras 156-169.

[382] Op cit note 302, *NM* case at paras 48-54.

privacy and dignity should give rise to a claim for damages. Article 7 of the Constitution reads: 'The Bill of Rights is a cornerstone of democracy in South Africa. It enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom.' Dignity is a core principle in the Constitution and it also lies at the root of the right to privacy.

Confidentiality of HIV/AIDS status

The Constitutional Court acknowledges that HIV/AIDS calls for special considerations of confidentiality.[383] Since the common law does not extend to negligence, it is not in keeping with the spirit, purport and objects of the Bill of Rights. Langa CJ noted that in developing the common law, negligence as an element of unlawfulness should remain separate to the inquiry of wrongfulness in the test for liability. When looking at the invasion of privacy by publication of private facts there are four essential elements that must be proven for negligence, namely: the disclosure was public; private facts were disclosed; the matter publicised was highly offensive to a reasonable person; and the matter was not a legitimate concern to public.[384] The requirement of publicity means that the matter must be communicated to the public at large, or that it must be substantially certain that the information would become one of public knowledge, be it to large or smaller group of people. Private facts can be defined as those facts closely connected to a person and which preferably remains confidential unless expressly consenting otherwise. A cause of action arises only when

[383] Ibid, *NM* case at para 63.

[384] Ibid, *NM* case at paras 95-97.

the publicity given is such that a reasonable person would feel justified in feeling seriously aggrieved.[385]

Prosser explains that the requirement of reasonableness is necessary because given the nature of society, 'no one can avoid the public gaze or public inquiry entirely and complete privacy does not exist in this world.'[386] Generally a person should not be held liable for the public disclosure of facts about another, unless he or she should have reasonably foreseen that the person would likely be offended. In the circumstances of this case, the ruling on costs does not seem to take into account the disparity between the applicants and respondents. The applicants are poor individuals who had to channel through the court system as a result of a well-renowned political figure, and her writer and publishers, who blatantly refused to take steps to redress the harm to the applicants. They acted negligently in failing to take all steps to obtain consent for the publication and directly refused to remove the names from the book once they were informed that it was unwanted disclosure. It is unfortunate that persons who already suffer because of the social stigma attached to their medical condition, should suffer further victimization as a result of individuals pursuing their own agendas. A more appropriate cost order would have been for the respondents to pay the costs of the applicants in both courts.

[385] Ibid, *NM* case at paras 95-97.

[386] Prosser, William L (1960) 'Privacy' 48 California Law Review 383 at 396.

The commentary on this case highlights that at the time the South African law fell short of explicitly protecting personal data from unwanted and unauthorized disclosure and guaranteeing confidential treatment and non-disclosure in the absence of expressed consent, and even more so, given the sensitivity of the medical data which required higher protections.

No legal recourse for negligence

Moreover, the common law did not provide recourse for negligent disclosure of private facts, and as seen from the analysis, the facts did allow for development of the law to bring it line with international data protection standards found in existing legal instruments. The fundamental international legal instruments protect the right to privacy, but the international trend shows that HIV/AIDS status calls for further special protections with emphasis on privacy, confidentiality and consent as essential elements of protecting HIV/AIDS status. The Constitutional Court should have taken account of the social realities not only in our country, but also the global recognition of the sensitivity of the disease. The following section makes reference to international instruments recognizing the special category of HIV/AIDS status and reinforcing the need for privacy and confidentiality.

International law on privacy of HIV/AIDS status

As stated above in chapter 3.3, the 1948 Universal Declaration of Human Rights (UDHR) serves as the basis for the protection of privacy at the international level. The

UDHR is a foundation for the United Nations human rights Covenants, including the 1966 International Covenant on Civil and Political Rights (ICCPR) which explicitly recognizes the right to privacy and the right to non-discrimination on the basis of nationality or other status. The UDHR is customary law and the ICCPR is binding on the international community. Specific reference to privacy and non-discrimination as a right can also be found in the Convention on Migrant Workers and the Convention on the Protection of the Child. 'Although the right to privacy was strengthened by its inclusion in the United Nations Covenants, it was the Council of Europe's 1981 CoE Convention, which considered health data as "special", and together with 1989 OECD Guidelines, it established the modern parameters for the principled regulation and security of medical data.[387]

The 1979 Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) binds signatory States to ensure that the respect of human rights and fundamental freedoms are afforded to the specific group of women and girls. It does not specifically address HIV status, but it is accepted that HIV positive women and girls have the right not to be discriminated against. Although international human rights conventions do not specifically provide for the protection against unfair discrimination on the basis of HIV/AIDS status, there are provisions that have been interpreted to provide for protection for people living with HIV/AIDS. These include the right to health and access to health care contained in the 1966 International Covenant on Economic, Social and Cultural Rights (ICESCR), CEDAW and the CRC.

[387] Knoppers, Bartha Maria 'Confidentiality of Health Information: International Comparative Approaches' <http://darwin.nap.edu>

In the absence of international instruments dealing specifically with HIV/AIDS, the Guidelines on HIV/AIDS and Human Rights provide a human rights framework for member states of the United Nations.

In 1997 the United Nations Commission on Human Rights passed a Declaration[388] emphasizing the need to intensify efforts to ensure universal respect for and observance of human rights and fundamental freedoms for all, to reduce vulnerability to HIV/AIDS and to prevent HIV/AID-related discrimination and stigma.[389] The annexure to the Resolution contains the following guidelines *inter alia*: 'Guideline 5: States should enact or strengthen anti-discrimination and other protective laws that protect vulnerable groups, people living with HIV/AIDS and people with disabilities from discrimination in both the public and private sectors, *ensure privacy and confidentiality and ethics in research involving human subjects*, emphasise education and conciliation, and provide for speedy and effective administrative and civil remedies; and Guideline 11: States should ensure monitoring and enforcement mechanisms to guarantee the protection of HIV-related human rights, including those of people living with HIV/AIDS, their families and communities.' The central theme running through the Resolution is that the full realization of human rights is an essential element in the global response to HIV/AIDS, in particular, that 'governments should commit themselves to enforce legislation, regulations and other measures to ensure all the rights of people living with HIV, including *privacy and confidentiality*

[388] The Protection of Human Rights in the context of HIV and AIDS, C.H.R. Res. 1997/33, ESCOR Supp. (No.3) at 115, U.N. Doc. E/CN.4/1997/33 (1997) <http://www1.umn.edu/humanrts/instree/HIV-AIDS.htm>

[389] Ibid, The Protection of Human Rights in the context of HIV and AIDS.

are protected and respected.[390] In 1999 a further Declaration was adopted urging States to implement the Guidelines adopted in the 1997 Resolution and reiterating that 'discrimination on the basis of HIV or AIDS status, actual or presumed, is prohibited by existing international human rights standards, and that the term "or other status" in non-discrimination provisions in international human rights texts should be interpreted to cover health status, including HIV/AIDS.'[391]

The United Nations Educational, Scientific and Cultural Organization (UNESCO) *Universal Declaration on Bioethics and Human Rights* also sets international standards for handling personal data of HIV/AIDS affected persons. The title of Article 9 of the Declaration demonstrates the commitment of the international community to data protection of HIV/AIDS status, stating as follows: '*Privacy and Confidentiality*: The privacy of the persons concerned and the confidentiality of their personal information should be respected. To the greatest extent possible, such information should not be used or disclosed for purposes other than those for which it was collected or consented to, consistent with international law, in particular international human rights law.'[392]

---

[390] Op cit note 144, 'Guidelines on Protecting the Confidentiality and Security of HIV Information' at 10.

[391] The Protection of Human Rights in the Context of Human Immunodeficiency Virus (HIV) and Acquired Immune Deficiency Syndrome (AIDS), C.H.R. res. 1999/49, U.N. Doc. E/CN.4/RES/1999/49 (1999) <http://www1.umn.edu/humanrts/instree/aidsresolution.html> Further Declarations where adopted to reinforce the 1997 Guidelines, see the United Nations Human Rights website for international instruments dealing specifically with HIV/AIDS. http://www.ohchr.org/EN/Issues/HIV/Pages/Documents.aspx

[392] United Nations Educational, Scientific and Cultural Organization (UNESCO) *Universal Declaration on Bioethics and Human Rights*, adopted by acclamation on 19 October 2005 by the 33rd session of the General Conference of UNESCO. <http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/bioethics-and-human-rights/>

At the 2001 United Nations Special Session on HIV/AIDS Declaration on Commitment of HIV/AIDS, heads of State and governments committed 'to enact, strengthen or enforce legislation, regulations and other measures to eliminate all forms of discrimination against and to ensure the full enjoyment of all human rights and freedoms by all people living with HIV/AIDS.'[393] In 2001 the General Assembly adopted a Resolution[394] outlining the international community's Declaration of Commitment on HIV/AIDS. The Resolution recognized that the full realization of human rights and fundamental freedoms of people living with HIV/AIDS an essential element in preventing stigma and related discrimination.[395] On 15 June 2006, the General Assembly adopted another Resolution on the Political Declaration on HIV/AIDS wherein it reaffirmed the commitment to recognize human rights and protect HIV/AIDS victims.[396] It further pledged to promote full *protection of confidentiality and informed consent* so as to promote a social and legal environment that is supportive of the safe disclosure of HIV status.[397] The right to privacy is expressly mentioned in the Resolution as follows: 'We (Sates) commit ourselves to intensifying efforts to enact, strengthen or enforce, as appropriate, legislation, regulations and other measures to eliminate all forms of discrimination against and to

---

[393] Ibid, see Paragraph 58 of the Declaration. See also other instruments of the International Community of Women Living with HIV/AIDS <http:www.icwglobal.org>

[394] Resolution adopted by the General Assembly (A/RES/S-26/2 with Annex, August 2, 2001) in a twenty-sixth special session.

[395] Ibid, see number 16 of the Resolution.

[396] Resolution adopted by the General Assembly (A/RES/60/262 with Annex, June 15, 2006).

[397] Ibid, see number 25 of the Resolution states that 'Therefore we [...] pledge to promote, at the international, regional, national and local levels, access to HIV/ AIDS education, information, voluntary counseling and testing and related services, with full protection of confidentiality and informed consent, and to promote a social and legal environment that is supportive of and safe for voluntary disclosure of HIV status.'

ensure the full enjoyment of all human rights and fundamental freedoms by people living with HIV and members of vulnerable groups, in particular to ensure their access to, *inter alia*, education, inheritance, employment, health care, social and health services, prevention, support and treatment, information and legal protection, while *respecting their privacy and confidentiality*; and developing strategies to combat stigma and social exclusion connected with the epidemic.' Portions of above are italicized to emphasize that confidentiality and consent are essential requirements when handling HIV/AIDS status. Although Resolutions adopted by the United Nations do not have the same binding force in law as treaties, it is soft law and since it signifies the support and aspirations of States they are expected to live up to the Declarations.

South Africa's treatment of HIV/AIDS status

South Africa has a Draft Paper on HIV/AIDS that seeks to address unfair discrimination in the context of HIV/AIDS status. In the Paper discriminatory conduct is classified under three categories, namely: individual, structural and institutional. The individual category involves discrimination on an intimate level in the personal relationships that people living with AIDS have with others. The forms of discrimination in this category include harassment, *disclosure of HIV status to others* or spreading rumours about a person's HIV status. The Draft Paper seeks to include HIV/AIDS as a prohibited ground in the Equality Act of 2000 so as to assist in developing a human rights based approach in keeping with international legal

trends.[398] While this analysis does not necessarily support the arguments put forward in the Draft Paper, it does align itself with the contention that special considerations are necessary when dealing with HIV/AIDS status. It supports the argument that disclosure of HIV/AIDS status without consent violates an individual's right to dignity and argues that data protection called for a change in the common law.

It is well known that the international community recognizes that the world needs to take positive steps to alleviate discrimination surrounding the HIV/AIDS disease. The Constitutional Court had a unique opportunity to set a precedent, but they failed to take the necessary steps in developing the common law.

Missed opportunity to develop the common law

Developing the common law to include negligence would have been a response to protect the perceptible and eroding levels of negligence in disregarding the social realities of people living with HIV/AIDS and taking precautionary steps to protect their HIV/AIDS status, a category of personal data which is deserving of the highest protections. Had they taken this unique opportunity, South Africa would have been the lead on the continent and it would have contributed to the international jurisprudence recognizing that safer safeguards are needed for handling personal data such as HIV/AIDS status, failing which, consequences may result if negligent actions result in unwanted disclosure and impact on the information privacy and dignity of those living

[398] The Draft Paper can be accessed on government website < http://www.doj.gov.za>

with HIV/AIDS, this includes migrants who are often found to be affected particularly in the SADC region. Due to the Constitutional Court's caution in developing the common law, data protection remained unregulated and the gaps in the law continued. The discussion in the next section demonstrates that the Court still remained conservative on data protection six years after the NM judgement.

ii) *Constitutional Court case Mail and Guardian Media Limited and Others v Chipu N.O. and Others*

Most recently the Constitutional Court was faced with the challenge of having to balance between public interest based on freedom of expression arguments put forward by the media and the principle of confidentiality as guaranteed in the South African Refugees Act 130 of 1998. This section will outline why the decision of the Constitutional Court in *Mail and Guardian Media Limited and Others v Chipu N.O. and Others*[399] (*Chipu* case) is flawed, in particular because it fails to appreciate the repercussions on the asylum seeking community and fear of reprisal to family, relatives and friends in their countries of origin.

Article 27 of the Refugees Act gives full legal protection to refugees. This includes the fundamental rights outlined in the Bill of Rights, including the right to privacy as

[399] *Mail and Guardian Media Limited and Others v Chipu N.O. and Others* Case CCT 136/12 (2013) ZACC 32; 2013 (11) BCLR 1259 (CC).

outlined in Article 14 of the Constitution. Privacy is reinforced in the context of asylum claims through the principle of confidentiality as outlined in Article 21 (5) which states that: 'confidentiality of asylum applications and the information contained therein must be ensured at all times.' The Constitutional Court had to decide whether absolute confidentiality is a reasonable and justifiable limitation on the right to freedom of expression. In its judgment delivered on 27 September 2013 in the *Chipu* case, the Majority 'declared that section 21(5) of the Refugees Act is inconsistent with section 16 (1)(a) and (b) of the Constitution to the extent that it precludes members of the public or the media from attending proceedings of the Refugee Appeal Board in all cases and fails to confer a discretion upon the Refugee Appeal Board to allow the public and media access to its proceedings in an appropriate case.'[400]

Facts of the case

This case concerns a media application to the Refugee Appeal Board to allow the press to be present at a rejected asylum seeker's appeal and to report on the proceedings to the public. The High Court refused to set aside the Refugee Appeal Board's decision to deny the application made by the media and found that although the Refugees Act limited the freedom of the press to receive and impart information, it was a justifiable limitation given the importance of confidentiality to the integrity of the asylum process. The applicants argued that the information relating to the rejected asylum seeker was already in the public domain and that public interest demanded that the rule

[400] Ibid, *Chipu* case at 60.

of confidentiality be lifted in particular circumstances at the discretion of the Refugee Appeal Board. Of particular relevance was the fact that the rejected asylum seeker in this case was subject to a pending extradition order initiated by his country of origin and the media already reported on alleged criminal activities committed by him both while abroad and in South Africa. Indeed, as a general rule, information that is already in the public domain is an exception to the principle of confidentiality, however, the truthfulness of the information may be unknown when it comes to media reports and allowing access to refugee appeal hearings and publication thereof could definitely jeapardize the appeal proceedings and the safety of the asylum seekers and their family, relatives and friends.

Senstivity of refugee status as a private fact

The respondents argued to the contrary that Article 21(5) of the Refugees Act constituted a reasonable and justifiable limitation on the right to freedom of expression because absolute confidentiality was essential for the integrity of the asylum system and it was necessary to protect asylum applicants as well as their families and friends against possible threats or danger to their safety and lives. The *Amicus Curiae*, the Southern Africa Litigation Centre, raised the concern that absolute confidentiality would render the asylum system vulnerable to abuse and compromise South Africa's obligations to ensure accountability for international crimes.[401] Lawyers for Human Rights tried to intervene as the second *Amicus Curiae* but their application was refused because they tried to raise new evidence that the Constitutional Court found to be

[401] See Constitutional Court media summary of the *Chipu* case <http://www.constitutionalcourt.org.za/Archimages/21375.PDF>

irrelevant to the question before the Court, or alternatively, that it carried little weight.[402] Even though it was weakly substantiated, Lawyers for Human Rights did raise pertinent issues and the Court failed to give sufficient weight to, amongst others, 'the sensitive nature of asylum claims based on the nature of persecution to which asylum seekers would have been subjected to in their countries of origin and the credible assessments of asylum seekers at first instance level and at appeal level cases.'[403] Unfortunately the Court ruled that this does not warrant consideration to the question of confidentiality. While Lawyers for Human Rights did raise the fact that the refugee appeal system in South Africa is generally bad in practice, they failed to explain why absolute confidentiality was necessary in appeal cases. Had they argued that the Refugee Appeal Board does act *de facto* act as a court of first instance in many cases and that they considered not purely appealable issues, but rather detailed personal facts relating to the asylum seeker's well-founded fear of persecution, the Court may have accepted their application to intervene. In addition, if asylum applicants were aware of the media presence in their appeal application, they would be reluctant to disclose truthful submissions knowing that it would form part of the public domain. This is exacerbated by the fact that news reports are made available electronically and any truthful submissions made by the asylum seeker could jeapordize lives in their countries of origin, particularly since the internet is available in almost all parts of the world and is easily accessible even on mobile telephones.

[402] Op cit note 399, *Chipu case* at para 13.

[403] Ibid, *Chipu* case para 10.

The Constitutional Court did recognize the need for confidentiality in refugee cases and the serious nature of asylum claims, however, they mistakenly found that it did not relate to the issue between the parties, that is, whether blanket confidentiality should be maintained or whether there should be flexibility to allow discretion to lift the confidentiality.[404] This seems contradictory because on the one hand the Court order does not provide any direct relief to the parties, but on the other hand the Court found the blanket confidentiality to be unconstitutional, and the latter clearly has a direct impact on all asylum claims.

Under the 1949 Geneva Conventions South Africa has an international obligation to either extradite or prosecute perpetrators of torture and cruel, inhuman or degrading treatment.[405] Moreover, Article 4 of the Refugees Act provides exclusionary grounds for the following categories if there is reason to believe that a person: 1) committed a crime against peace, a war crime, or a crime against humanity and prohibits the granting of asylum to such persons; 2) committed non-political crimes which if committed in South Africa would be deemed punishable; 3) has been guilty of acts contrary to the objects and principles of the United Nations Organization or the Organisation for African Unity; or 4) enjoys the protection of any other country in which he or she has taken up residence. This prohibition allows the country to comply with its international obligations and it goes further to meet the objectives of State security and crime prevention.

[404] Ibid, *Chipu* case at para 12 – 14.

[405] Ibid, *Chipu* case at para 23.

The applicants insisted on being present during the appeal application to determine the facts of the case and to disclose to the public whether the rejected asylum seeker would be excluded from refugee status based on the listed grounds in Article 4 of the Refugees Act. The media companies based their arguments on Article 16 (a) and (b) which states that 'everyone has the right to freedom of expression, which includes freedom of the press and other media and freedom to receive or impart information or ideas.'

Privacy vs freedom of expression

In weighing the rights to privacy against freedom of expression the Constitutional Court referred to its previous decisions stating that 'the relevant factors in the limitation clause in Article 36 of the Constitution should be viewed on a case by case basis applying proportionality between the limitation on the right in question and its purpose as well as the existence of less restrictive means to achieve this purpose.[406] The applicants relied on the 'open justice' argument stating that fair trials must be open to the public as it promoted accountability of the courts and administration of justice.[407] This argument should not have been given any weight at all because the appeal proceedings before the Refugee Appeal Board cannot be equated to criminal appeals. Refugee appeals are not part of the criminal justice system, instead, they are administrative in nature and given the sensitivities of refugee claims the proceedings are held under the 'closed court principle' which is a necessity due to privacy and security that is intrinsically linked to the well-founded grounds forming the basis of

[406] Ibid, *Chipu* case at 47-48.

[407] Ibid, *Chipu* case at 53.

refugee claims.

The applicants argued further that the information they sought was not of a personal nature and they wanted access to information relating the rejected asylum seeker's international criminal activity and his corrupt behaviour.[408] This goes against data protection because the rejected asylum seeker's name is in itself personal data and facts revealed during refugee appeals are of a personal nature and it includes all personal circumstances surrounding the refugee claim which is very sensitive. For a refugee claim to be warranted it should be based on both objective facts related to the safety of the asylum seeker and others in the country of origin and prevention of reprisals as well as subjective facts presented by the asylum seeker about his personal circumstances and that of his family, relatives and friends in the country of origin.

It should be noted that the purpose of refugee appeal proceedings is not to prosecute criminal activity and corruption. It is only to hear the appeal on the grounds for refusal and it does not go into the evidentiary proof of guilt that would be present in a criminal trial. Allowing media to be present in the appeal proceedings could result in prosecution by media for migrants and this is at odds with the South African justice system, which is adversarial, as opposed to a jury system. The Constitutional Court pointed out that 'a person who has committed a crime against humanity or who has committed a crime against peace is disqualified from receiving refugee status,[409] yet

[408] Ibid, *Chipu* case at 56.

[409] See Article 4 (1)(a) of the Refugees Act.

the confidentiality limitation in Article 21(5) is so wide that it continues to apply even after a refugee application has been rejected on the grounds that the person has committed a crime against peace or a crime against humanity. It also questioned the purpose for keeping the person's information confidential after the application has been rejected on the exclusionary grounds.'[410] The answer to this question lies in the integrity of the asylum process and the fear of other asylum seekers that their information will be made public if their refugee claims are rejected. This is relevant to the question of confidentiality and the Constitutional Court unfortunately failed to appreciate the impact on the refugee community.

Comparative jurisprudence on refugee protection

The United Nations High Commissioner for Refugees (UNHCR), the custodian of the 1951 Refugee Convention and its 1967 Protocol, states that: 'Confidentiality in asylum procedures is particularly important because of the vulnerable situation in which refugees and asylum seekers find themselves. For example, unauthorized disclosure of personal data to third parties in the country of origin or elsewhere could inhibit an asylum seeker from fully explaining his or her case, or even from making a claim for refugee status; endanger any relatives or associates of the asylum seeker remaining in the country of origin; endanger the asylum seeker in the event of his or her return to the country of origin; and cause the asylum seeker to become a refugee *sur place* (i.e. even if the persons were not refugees when they left the country of origin they may become refugees due to the circumstances that may arise during their absence in the

[410] Op cit note 399, *Chipu* case at 57.

country of origin). Hence, while an asylum seeker has a duty to assist the examiner to the full in establishing the facts of his or her case, the examiner is not ordinarily entitled to disclose the asylum seeker's personal data to a third party.[411]

UNHCR goes further to confirm that the need to respect confidentiality, as recognised by UNHCR's Executive Committee in Conclusion No. 82 (XLVIII) (1997), applies to all stages of the asylum procedure, including if and when an application for refugee status is rejected because the international Data Protection Principles require that an individual consent to the sharing of his or her personal data with a third party unless there is an overriding interest at stake, either of the individual concerned, or of another individual or of society at large. Circumstances in which consent is not required are an exception, in which case disclosure must be necessary, in accordance with law, and proportionate to the legitimate aim pursued.[412]

Constitutional court finding

The Constitutional Court duly recognized that the limitation to freedom of information serves the purpose of protecting the integrity of the asylum system and of providing asylum applicants with protection against disclosure of the fact that they have applied for asylum and the information in their asylum applications, however, the

[411] United Nations High Commissioner for Refugees (2003) 'Comments on the Source Country Information Systems of the International Centre for Migration Policy Development' at 4-5.

[412] United Nations High Commissioner for Refugees 'Asylum Processes (Fair and Efficient Asylum Procedures), Global Consultations on International Protection' Third Track – Executive Committee Meetings, EC/GC/01/12, 31 May 2001.

Constitutional Court found that there was a least restrictive means of limiting the freedom of expression than the blanket confidentiality statutory provision which is to allow a discretion to lift the confidentiality in certain situations.[413] To this end, the Constitutional Court raise the question concerning 'the purpose of the limitation achieved in a case where the person who, after arriving in South Africa, discloses publicly, maybe in a press conference, the reasons why he fled his country of origin and other information that is relevant to the asylum application? If the applicants in the present case wanted their journalists to attend the asylum appeal hearing of that person before the Appeal Board, why should section 21(5) preclude the applicants' journalists from attending that person's hearing and reporting on it?' The Constitutional Court found that in such a case there is no purpose served by the limitation and the limitation cannot be justified.[414] This scenario, however, depends if the person consents to unlimited disclosure because the principle of consent as outlined in data protection legal instruments does not allow for blanket consent, it has to be limited to a specified purpose of the particular media press conference. Thus, the consent of the person cannot be applied to the appeal procedures itself, unless explicit consent is provided for this purpose. In addition, and more importantly, the provision of consent is not sufficient because the 'do no harm' principle should be taken into account in refugee cases, in particular the potential harm resulting from the public disclosure that could be imposed on the family, relatives or friends of the asylum seeker in the country of origin. The right to life is the core and fundamental right necessary for the enjoyment of all other rights and the importance of threat to life and safety is a paramount consideration for the State's obligation exercised through the

[413] Op cit note 399, *Chipu* case at para 58.

[414] Ibid, *Chipu* case at 59.

Refugee Appeal Board.

Unfortunately the Court gave little weight to the respondents' reliance on UNHCR's pronouncements, stating further that it would appear that exceptions in the 1951 Refugee Convention would be allowed on national security grounds.[415] It should be noted that the issue before the Constitutional Court did not concern a balance between the statutory obligation of confidentiality and the public security; instead, it was freedom of expression based on public interest grounds that the Court had to weigh in the balancing test. Moreover, it is not warranted to apply the exception in the 1951 Refugee Convention on national security grounds to public interest arguments, which in itself is generally much broader, and in this case, it is limited to freedom of expression which is unrelated to the intention behind the exception in the 1951 Refugee Convention.

Discretion on disclosure in asylum cases

The Constitutional Court incorrectly relied on the applicants' arguments putting forward eight countries to demonstrate an international norm that allows for discretion to be applied when considering confidentiality of asylum procedures. While it could be argued that the Court was merely looking at comparative law, the applicants' arguments intended to establish that an international norm existed. Arguably, the laws cited constituted mere examples of countries that impose discretion in the law and just

[415] Ibid, *Chipu* case at 65-70.

because the respondents did not quote evidence to the contrary, does not provide sufficient grounds to warrant the incorrect assumption that the practice of eight countries constitute an international norm. When it comes to refugee cases, the UNCHR is the custodian of the 1951 Refugee Convention and signatory States are bound to follow UNHCR's interpretation of the language in the Convention. If a sample of national refugee laws fall short of meeting strict confidentiality as an absolute requirement, this does not mean it creates an international standard. The Constitutional Court also turned to the Extradition Act 67 of 1962 in South Africa stating that no confidentiality is required and therefore confidentiality in the Refugees Act should be flexible, however, the Extradition Act falls within the ambit of criminal court procedures and this differs from administrative refugee appeal procedures. The former focuses on criminal prosecutions, while the latter focuses on the State obligations under humanitarian and human rights law.

Safety is a paramount consideration

The Court could not appreciate 'why the integrity of the asylum system and the safety of the asylum applicants and their families and friends would be threatened by the publication of information in an asylum application that would not tend to disclose the identities of the asylum applicant, his family and friends' and further stated that 'obviously in considering a request for access the Appeal Board all relevant factors including, whether or not prohibiting the publication of information that does not tend to reveal the identity of the asylum applicant or his or her family and friends would not

be a sufficient protection should be considered.'[416] This is not so obvious and it cannot be assumed that this is indeed a consideration. In fact a discretion to reveal the identities and personal circumstances of the refugee claim would not be sufficient protection as it could result in real harm to the asylum seeker and others and it could also be a deterrent to other asylum seekers providing full information for the proper determination of refugee claims. The Court compared a number of different national laws that give a discretion to presiding officers to allow a person to attend court proceedings.[417] As mentioned above, the proceedings are different with refugee cases and the threat to life and safety are key considerations and this makes the Refugees Act different.

Court order

For reasons related to the separation of powers, the Court only made a temporary order, but it nonetheless put forward criteria for how the Refugees Act should be amended. The court order resulted in a temporary reading-in of words to create a discretionary power while the Legislature amends the Refugees Act, but the criteria for determining whether confidentiality should be lifted is based entirely on freedom of information arguments put forward by the applicants.[418] The court order states as follows: 'It is declared that section 21(5) of the Refugees Act 130 of 1998 is inconsistent with section 16(1)(a) and (b) of the Constitution to the extent that it precludes members of the public or the media from attending proceedings of the

[416] Ibid, *Chipu* case at para 92.

[417] Ibid, *Chipu* case at para 86 – 91.

[418] Ibid, *Chipu* case at para 86 – 91.

Refugee Appeal Board in all cases and fails to confer a discretion upon the Refugee Appeal Board to allow the public and media access to its proceedings in an appropriate case [...]. Section 21(5) of the Refugees Act 130 of 1998 is to be read as providing as follows: "The confidentiality of asylum applications and the information contained therein must be ensured at all times, except that the Refugee Appeal Board may, on application and on conditions it deems fit, allow any person or the media to attend or report on its hearing if (a) the asylum seeker gives consent; or the Refugee Appeal Board concludes that it is in the public interest to allow any person or the media to attend or report on its hearing, after taking into account all relevant factors including (i) the interests of the asylum seeker in retaining confidentiality; (ii) the need to protect the integrity of the asylum process; (iii) the need to protect the identity and dignity of the asylum seeker; (iv) whether the information is already in the public domain; (v) the likely impact of the disclosure on the fairness of the proceedings and the rights of the asylum seeker; and (v) whether allowing any person or the media access to its proceedings or allowing the media to report thereon would pose a credible risk to the life or safety of the asylum seeker or of his or her family, friends or associates."'[419]

Unfortunately the Court gave the temporary order in consideration of arguments relating to the rejected asylum seeker in question and without giving due consideration to the impact on other refugee cases that would be affected in the interim. The Court also reads-in language which goes much further than examples quoted in the eight jurisdictions where discretion is allowed. In those cases it refers to allowing one person being exceptionally allowed access and does not make explicit reference to the

[419] Ibid, *Chipu* case at para 115.

media making an application. The intention behind such discretion does not necessarily relate to public interest of freedom of information as the Court seems to assume. In addition, Parliament would have to do a thorough analysis of other foreign jurisdictions to determine whether or not it is an international norm to lift confidentiality to allow media access with interventions from the public including the UNHCR, Lawyers for Human Rights and other agencies involved in protecting the rights and interests of refugees.

Missed opportunity to develop the law on data protection

The Constitutional Court had a unique opportunity to pronounce, once again, on data protection but did not go far enough. While it recognized the issue of confidentiality, which is a core data protection principle, it did not take into account how allowing discretion to lift confidentiality could impact on future asylum claims and potentially jeopardize life and safety of asylum seekers and their families and relatives. The temporary order relates to the case in question but it has far reaching implications. While legislation on this is left to Parliament, this temporary order will apply in the interim, and legislators could take years to amend the law as an appropriate analysis and thorough research is required before changing the law which could potentially harm the lives of asylum seekers, their families and relatives, and threaten the integrity of the asylum process.

Unfortunately in this case insufficient weight was given to the potential harm that could result from public disclosure, a reality experienced by asylum seekers and

refugees even beyond their refugee status determination hearing. The Court was conservative in its finding and thus the gaps in the law remained. This turns the discussion to whether the recently enacted Protection of Information Act takes the law further and remedies existing gaps.

5.3 *Protection of Personal Information Act*

As seen above, the Constitutional Court was conservative in its findings in the *NM* case and failed to expand the common law and in the *Chipu* case it failed to fully recognize the sensitivities surrounding confidentiality of refugee cases and the potential harm and threat to life of asylum seekers that could result from its interim court order. This section examines whether the recent Protection of Information Act of 2013 covers the current gaps in the law.

Project 124 on data protection

Substantive work has gone into the South African Law Commission Project 124, which resulted in the promulgation of the Protection of Personal Information Bill published in August 2009.[420] The details of Project 124 have been discussed above in part and do not require repetition, save to say, that the Report on the Protection of Personal Information and Privacy provides a very good overview and insight into the

[420] Protection of Personal Information Bill, Government Gazette No. 32495 of 14 August 2009 [B 9-2009] <http://www.pmg.org.za/files/bills/090825b9-09.pdf>

current legal framework on data protection at the international level and in Europe.[421] One lacking aspect though, is the issue of migration, which is nowhere featured in any of the discussion papers. It is unclear why this was absent from the table. Silence on this issue, does not however, necessarily mean that it does not accommodate migrants or that it conflicts with existing rights afforded to migrants including refugees in the country.

In researching the various comments made by refugee and migrant rights actors, no concerns were raised during the consultations. Lawyers for Human Rights, a rights-based law centre, indicated during informal interviews that the Bill can be interpreted to apply to migrants as well and therefore they found no need to voice any major concerns. It would, for example, ensure adequate protection for the collection of biometric data as introduced into the Refugee Amendment Act of 2011 and this could help to expedite the issuance of refugee permits.[422]

The law on data protection

The Protection of Personal Information Act aims to provide a legal basis for the collection and processing of personal data, give legal force to Data Protection Principles, provide protection against unauthorized disclosure by private and public bodies, and regulate its application to ensure conformity with the EU Directive. It

[421] South African Law Reform Commission Project 124 (2009) 'Privacy and Data Protection Report' Pretoria, South African Law Commission.

[422] Informal interview with Ramjathan-Keogh, Kaajal, Head Refugee and Migrant Rights Programme, Lawyers for Human Rights conducted in Johannesburg.

serve as the overarching legal instrument on the protection of personal data for both private and public sectors by giving effect to the core Data Protection Principles that have evolved over time in various jurisdictions around the world. It establishes minimum requirements for processing personal data, provides for the establishment of an Information Protection Regulator (which is the equivalent of a Data Protection Supervisory Body in Europe), outlines procedures for issuing codes of conduct and regulates the flow of personal information across the borders of South Africa.

Other relevant legislation in South Africa, that exists to date, include the Electoral Act of 1998, the Promotion of Access to Information Act of 2000, and the Electronic Communications and Transactions Act of 2002, as well as the Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002. The Promotion of Access to Information Act only covers access to information; it does not extend to the collection and processing of personal information. This has been a gap from the outset, but as stated in chapter 4 above it was foreseen that a separate law on information privacy would eventually follow. The Electronic Communications and Transactions Act provides a regulatory legal framework for processing electronic records and puts forward a list of data protection principles along the lines of the commonly accepted principles at international level. However, the principles are not mandatory, instead the language in the Act is tentative and businesses have an option to apply the principles to consumers. The principles therefore lack legal force. The Interception of Communications and Provision of Communication-related Information Act prohibits surveillance of all personal communications, but this Act has a narrow focus and does not cover other aspects of

the right to information privacy/data protection. As outlined by Currie and Klaaren, the Promotion of Personal Information Act should be read together with existing legislation because addressing the gaps and making amendments to existing laws were foreseen during the development of this new law that aims to be all-encompassing.[423]

Analyzing the Protection of Personal Information Act

In line with the international trend, the Protection of Personal Information Act adopts the twin goals of ensuring protection of the right to data protection and facilitating the free flow of personal data across borders as outlined in the EU Directive. However, it is tailored specific to the South African context. The preamble expressly recognizes the constitutional right to privacy and affirms that it includes the right to protection against the unlawful collection, retention, dissemination and use of personal information. The latter part gives effect to a statutory right to the protection of personal information and the language in the first part confirms case law findings that the constitutional right to privacy includes this right to data protection.

Nature of the Act

The Act is a hybrid law that draws extensively on the EU Directive, but also on the 1980 Guidelines of the Organisation for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation and the 2005 Asia-Pacific

[423] Iain Currie, Iain and Klaaren, Jonathan (2011) 'Evaluating the Information Bills: A Briefing Paper on the Protection of Information Bill.'

Economic Cooperation (APEC) Privacy Framework. Its hybrid nature was confirmed during the Parliament debates where it was described as a hybrid legislation that incorporates both human rights while providing for economic expediencies.[424] To this end, it follows the EU Directive focusing on the commonly accepted Data Protection Principles and the transborder flow of personal data, but also draws on the 1980 OECD Guidelines and APEC Privacy Framework focusing on the economic value of data exchange.

The Protection of Personal Information Act, like its parent in Europe, is a 'framework law: instead of stipulating in casuistic fashion detailed provisions for regulating the processing of personal information, the 'Information Protection Principles' are instead rather diffusely formulated general rules for such processing. Specific allowance is made for the subsequent development of more detailed regulatory norms as the need arises.'[425] The principle-based approach with a concentration on the spirit of the law is in accordance with international instruments. Currie says the main reason for this approach is to avoid circumvention of the law that is further enhanced by allowing for Codes of Conduct and other sector-specific legislation, some of which already exists, for example PAIA, the Protection of State Information Bill, the National Credit Act,

[424] Parliamentary Monitoring Group (PMG) 'Protection of Personal Information Bill; Constitution 17th Amendment Bill: briefing; UN Security Council proclamations in respect of entities involved with terrorist activities' Recent Meetings for NCOP Security and Constitutional Development, 15 November 2012 <http://www.pmg.org.za/report/20121114-department-justice-and-constitutional-development-protection-state-in>

[425] Currie, Iain (2010) 'The Protection of Personal Information Act and Its Impact on Freedom of Information' at 6 <http://www.opendemocracy.org.za/wp-content/uploads/2010/10/The-Protection-of-Personal-Information-Act-and-its-Impact-on-Freedom-of-Information-by-Iain-Currie.pdf>

the Consumer Protection Act and the National Health Act.[426] In addition, to bring South African in line with other jurisdictions, another benefit of the law is the potential to enhance investment from outside the country, as this will in turn, create much-needed jobs in South Africa.

State security exception

Article 6 provides for exclusions amongst others for 'processing personal data by or on behalf of the State if it is for reasons of State security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defense or public safety.' The State security exception seems broad, but it is similar in language to the exceptions in the EU Directive and the specific laws on data protection in other jurisdictions. It should be noted that it is not an open-ended exclusion, the drafters deliberately included a limitation with a proviso that the exclusionary grounds are 'to the extent that adequate safeguards have been established in specific legislation for the protection of such personal information or if it relates to processing personal data of children.' The condition goes further than the EU Directive, which only states that 'adequate legal safeguards' should be in place. In the Act it is explicitly stated that adequate safeguards must be clearly established and embedded in specific legislation, thereby narrowing the State security interests and requiring legal justifications and safeguards to be enacted in legislation for the limitation to the right to data protection before the derogation can apply.

[426] Ibid, 'The Protection of Personal Information Act and Its Impact on Freedom of Information'.

Special consideration for children

A special category is introduced in Article 35 for children, this is commendable when compared to laws in other jurisdictions, and demonstrates South Africa's commitment to acknowledging the vulnerable status of children. It is also in line with the European Commission's opinion in the EU data protection reform emphasizing that children deserve specific protection, as they may be less aware of risks, consequences, safeguards and rights in relation to the processing of personal data.[427]

Stricter safeguards for sensitive personal data

Like other laws, extra special safeguards are required for 'sensitive personal data' as it is called in other jurisdictions. The drafters called this 'special personal information' in Part B of the Act and it is based on the prohibitions in the EU Directive. The definition normally given for sensitive personal data in international data protection texts refers to 'data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and data concerning health or sexual life as well as data on offences, criminal convictions or security measures.[428] This caters for personal data in refugee cases that require extra safeguards because well-founded fear of persecution are based on these grounds as well as HIV/AIDS status on medical grounds as pointed out in the *NM* and *Chipu* cases above. The reason for treating certain types of personal data with extra precaution stems from the concern

[427] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions 'A Comprehensive Approach on Personal Data Protection in the European Union' COM (2010) 609 final 9, Brussels, 4 November 2010 <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf> at 6.

[428] Op cit note 158, *Data Protection at ICPO-Interpol: Assessments, Issues and Outlook* at 13.

that misuse of the personal information could have more severe consequences of impeding individual's rights, for example, discrimination can result from processing the special personal information and this can have long term and lasting negative effects on the individual concerned.

Specific provision for biometric data

Interestingly a further category of biometric data is introduced and this puts South Africa at the forefront of the issue as many existing laws in other jurisdictions are currently being amended to accommodate biometrics. For the purpose of the Act, biometrics is defined as 'a technique of personal identification that is based on physical characteristics, including fingerprinting, DNA analysis, retinal scanning and voice recognition.' The explicit reference to photographs is excluded in the Act, but this could be read into the general definition of personal data that identifies an individual. The inclusion of biometrics is quite progressive because the definition not only focuses on fingerprints which is the dominant biometric feature used for identifying individuals (along with photographs), but it takes account of the use of other types of biometric features which are rapidly expanding with the availability of advanced technology. Hosein and Nyst state that South Africa has one of the oldest biometric registration systems in the world stemming back to 1925 when the government collected fingerprints from non-white citizens for the purpose of racial registration.[429] This raises the important question of identification systems that have the potential to be used for discriminatory and segregation purposes. Since the

[429] Hosein, Gus and Nyst, Carly (2013) *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries* at 34.

definition of biometrics in the Act includes DNA analysis, from the privacy perspective, caution should be applied because DNA facilitating genetic profiling can assist in the creation of racial and ethnic profiling.[430]

The European Court of Human Rights in the case of *S and Marper v United Kingdom*,[431] made a distinction between the level of interference with the right to data protection in Article 8(1) of the EU Charter when taking and retaining DNA as opposed to taking and retaining fingerprints. The Court held that 'taking and retaining an individual's DNA was regarded as particularly intrusive, given the amount of genetic and health information it contains and the purposes for which such samples and related data could potentially be used, both now and at a future date.'[432] It is therefore important that government entities and their outsourcing private companies using biometric systems do so within the limits of the law and without discriminatory motives. Due to the risks involved it is recommended that DNA be excluded from biometrics when using it for immigration purposes.

According to Ramjathan-Keogh, Kaajal, Head Refugee and Migrant Rights Programme at Lawyers for Human Rights, 'the use of biometrics in migration management is better for refugees because it is tool to identify people and it allows for

---

[430] Ibid, *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries* at 39.

[431] *S and Marper v United Kingdom*, [2008] ECHR 1581.

[432] Ibid, *S and Marper v United Kingdom*.

the issuance of documents. For example, during the xenophobic riots and attacks on migrants in 2008 refugee permits were lost and fingerprint verification would have been the easiest way to reissue refugee permits or to validate permits as refugees often lose their documents. Biometrics is also very useful for preventing asylum shopping and to curb fraudulent applications. From Lawyers for Human Rights perspective biometrics has more positive elements than negatives.' She further highlighted that the 'nature of their work involves collecting sensitive information from refugees and migrants and that sometimes sharing personal data is inevitable. In the first consultation clients will a sign power of attorney at first level and if, for example, they refer a matter to UNHCR for assistance, the case file containing all sensitive and personal information would be transferred only upon instruction of the client and with their written consent.

Respecting confidentiality

In practice however confidentiality is not always respected, for example, there have been instances where asylum seeker and refugee clients were placed into witness protection programmes with limited access to their personal information and whereabouts, but despite being in witness protection the refugees were discovered and their whereabouts become known thereby jeopardizing their safety.' She attributes this to corruption and says Lawyers for Human Rights has to often balance corruption against the protection of asylum seekers' personal information and their safety. She is of the opinion that corruption has a significant role in balancing State interest and the rights of migrants. What is needed to increase individual protection and respect for individual lives, is incentives and sanctions, as well as protection for

whistleblowers.[433] The Protection of Personal Information Act does include sanctions and this could be extended to corruption if personal data is mishandled and if a case is made governmental officials who have access to personal information in witness protection programmes and take bribes to reveal information and whereabouts of refugees could be sanctioned through this Act.

Practical protections are important, but legal protections are even more important to ensure accountability and to protect individuals' safety and kept their personal data confidential especially in very sensitive cases that require witness protection. Unfortunately in South Africa corruption poses a threat to privacy and the Act should allow enforcement of law with sanctions to adequately protect individual rights.

Data collection for unspecified purposes

Mariano, Bernardo, Regional Director of Southern Africa at the International Organization for Migration, questioned 'what is done with biometrics collected from asylum seekers that are not successful in their asylum applications and are migrants aware of what happens to their personal data? The South African government has a database that includes registration data of Zimbabweans seeking asylum as well as their biometrics and photographs. There is interest from the government to use the database to match fingerprints for criminal purpose. In addition, the government is trying to have better access on patient data to profile diseases. Profiling migrant data

[433] Informal interview with Ramjathan-Keogh, Kaajal, Head of Refugee and Migrant Rights Programme, Lawyers for Human Rights conducted in Johannesburg.

can be done based on disaggregated data by private and public hospitals, but there are attempts by the Ministry of Health to have access to the database. However, there are no parametres governing such access. A concern is that migrants are stigmatized for bringing diseases and this fuels xenophobia.' There is an argument to gain access to health data in the public interest, but this should not trump data protection safeguards that are needed and laws that should regulate how health data is handled.

Lack of humanitarian clause

The need for special provisions for children and biometrics has been called upon by the Working Party on Data Protection in Europe and South Africa is thus advanced in this area. The prohibition on processing special or sensitive personal data does not, however, make explicit reference to humanitarian grounds, which is also a gap in the current existing laws elsewhere. The need to include a humanitarian clause was raised by Amnesty International and UNHCR during the drafting of the UN Guidelines on data protection because collecting sensitive personal data is integral to the operations of international humanitarian aid workers and the prohibition would circumvent the goal of protecting the individuals and their rights.[434] Therefore an exception to the prohibition on processing special personal information based on humanitarian grounds should have been clearly stated. Perhaps it can be read into Article 37 of the Act in that the Data Protection Supervisory Body has the discretion to grant exceptions to the Data Protection Principles, but this means that all national humanitarian agencies would have to go through the procedural step to apply for an exemption before it can

[434] Annexure to the United Nations General Assembly 'Human Rights and Scientific and Technonogical Developments: Guidelines for the regulation of computerized personal data files' Report of the Secretary-General [A/44/606] 24 October 1989 at 13.

process special or sensitive personal data. This does not seem feasible as humanitarian assistance is often in response to emergency situations.

For South Africa it could relate to large influx of migrants who need assistance at border posts. Humanitarian situations involve not only international agencies, but also local agencies with mandates focused on humanitarian relief and in the scope of their functions all types of special categories of personal data may be needed for the purpose of providing protection or provision of food, medical treatment and safety, to name but a few. Article 27 (c) of the Act does refer to data processing that is necessary to comply with an obligation of international public law, but this does not address the issue because it applies to the State obligations under international law and does not necessarily cater for individuals or entities collecting special personal data as agents or that are *de facto* carrying out the international obligations of States in terms of their humanitarian work and neither for national NGOs doing humanitarian and protection work. An explicit reference to humanitarian reasons would have been advancement to the law.

Accountability

Ramjathan-Keogh, Kaajal, raised two concerning issues in the context of migrant and refugee assistance, in particular: 1) cell phone companies have personal data and provide or sell it to other companies without consent and it is used for profit without any recognition of the vulnerabilities of the people involved, and 2) there is an increase in soliciting credit history and trying to sell a product without consent or

knowledge of the person and using it for the profit of private companies.'[435] Indeed, this is a concern and it is heightened when private companies take advantage of vulnerable groups. The Protection of Personal Information Act does cover these issues as it regulates handling of personal data by private companies and particularly requires consent of individuals before they can process their personal information for any purpose.

Marketing and criminal behaviour

Compared to other jurisdictions, there are additional sections on unsolicited marketing by electronic communications and detailed provisions on monitoring of criminal behaviour, these can be seen as additions to the law in light of the South African context and due to concerns currently being raised in the international community.

Exemptions

Article 37 of the Act allows for exemptions to be granted to specific Data Protection Principles by the appointed Data Protection Supervisory Authority for reasons of: 'a) public interests, provided it outweighs to a substantial degree, the interference with privacy of the data subject; or b) if there is a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.' To allow for such exceptions, certain conditions can be set by the Data Protection Supervisory Body for

[435] Interview with Ramjathan-Keogh, Kaajal Head Refugee and Migrant Rights Programme, Lawyers for Human Rights conducted in Johannesburg.

granting such exceptions. This illustrates that it is qualified exceptions and data protection is not simply overridden for the interests of the State.

Data protection supervisory body

Currie argues that the Promotion of Personal Information Act will not only interact with the Promotion of Access to Information Act, but it will also supplement it in a number of ways, with the intention of improving it particularly the fact that 'the freedom of information regime has been hamstrung by the absence of an accessible and affordable dispute-resolution mechanism and a specialized regulator with oversight powers.'[436] Klaaren in his assessment of the avenues of the courts as a means to enforce the right to access to information notes that 'on the whole, the experience of PAIA in the court shows the hallmarks of specialist and niche litigation strategy, rather than being a tool of normal professional practice.'[437] He goes further to question State reliance on a judicial enforcement model and concludes that effective implementation of the right of access to information can most effectively be complemented and supplemented by the appointment of Supervisory Body and supplementing codes of conduct.[438]

---

[436] Op cit note 425, 'The Protection of Personal Information Act and Its Impact on Freedom of Information' at 7.

[437] Klaaren, Jonathan (2010) 'PAIA Though the Courts: Case Law and Important Developments in PAIA Litigation 2005-2009' (Open Democracy Advice Centre) School of Law, University of the Witwatersrand, Johannesburg

<http://www.wits.ac.za/files/resc05a76f83bb2434ab05da4464788c0e6.pdf>

[438] Ibid, 'PAIA Though the Courts: Case Law and Important Developments in PAIA Litigation 2005-2009' at 9.

The introduction of the Information Regulatory Body as seen in chapter 5 of the Act seeks to vest responsibility in a Supervisory Body for application and enforcement of the rights and obligations outlined in the Act, for developing codes of conduct and guidelines, and most importantly, for taking up dual role of being the Information Regulatory Body for the PAIA to cure its defect. According to the EU Working Party on Data Protection, an 'effective data protection system has three components: 1) compliance with the rules must be ensured by making data subjects and controllers aware of their rights and duties and by the presence of effective sanctions for breach of the rules; 2) individuals must be able to enforce their rights rapidly and effectively and without prohibitive cost by approaching an independent institution; and 3) individuals must be able to obtain appropriate redress for breach of the rules, including compensation, by recourse to a system of independent adjudication or arbitration.[439] The Protection of Personal Information Act seems to meet this standard and would be considered as a law that is 'adequate' by the European Data Protection Authority who is responsible for assessing the standards of laws outside Europe. Currie and Allan argue further that even if these standards are met, an effective data protection system requires an independent Data Protection Authority as seen in Europe emphasizing its independence.

The responsibilities of the Authority include an oversight function; powers to monitor, investigate, and intervene; the capacity to engage in legal proceedings and the

[439] Op cit note 15, 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator' with reference to the European Commission Working Party on the Protection of Individuals with regard to the Processing of Personal Data 'Working Document: Transfers of Personal Data to Third Countries: Applying Articles 2 and 26 of the EU Data Protection Directive' (1998) ('Working Document 12') at 7 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf>

discretion to make decision and relief subject to judicial appeal.[440] The EU model places emphasis on enforceable data protection rights, and as seen in the failings of PIAI, a statutory rights regime will be ineffective if there is no adequate, effective and enforceable rights mechanism.[441]

The introduction of a Data Protection Authority will kill two birds with one stone as it can serve to enforce both the right to access to information and the right to data protection. This will not only cure the defect in the PIAI, but it will also result in an Authority that can resolve disputes without having to resort to courts at first instance.[442] In addition, the Article 18 provides that responsible parties are required to notify the data subjects of their processing activities and Article 22 provide for mandatory notification to Regulator in the event security compromises. This introduction of notification into the law is much in line with the latest proposed amendments made to the EU Directive, as introduced in the EU data protection reform, which aims to ensure that private and public entities are proactive in ensuring compliance with their data protection obligations.[443] Countries with traditions of data protection laws, such as Australia, are also amending their laws to include mandatory data breach notification provisions for agencies and organisations that are regulated by the law.

---

[440] Ibid, 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator' at 573.

[441] Ibid 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator' at 578.

[442] Ibid, 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator' at 564.

[443] See chapter 3.2 above for a discussion on the EU data protection reform.

Room for improvement

The German law is often hailed as the most successful national laws on data protection. Waldo et al, as well as, Flaherty confirm this, the latter says in his comparative analysis of data protection laws in five countries that the German 'advisory model' is indeed an effective one to replicate.[444] Interestingly Germany was the first country to have a specific law on data protection and this stems from its background where the State used trojan ways to spy on the movement of people and infringe upon their rights. South African is analogous in its former 'generations of egregious violations of privacy that seeped into public administration'[445] and which resulted in laws that disrespected individual rights at the expense of broad State interests. We can therefore learn from the German legislation on data protection that aimed to address violations into the private space.

One particular factor to note for future amendments to the South African law is the 'legal obligation imposed on entities to appoint internal privacy officers and its encouragement of the systematic application of data protection that is integrated into the design and development of information systems and infrastructure.'[446] The German law also has effective oversight and enforcement mechanisms that can be attributed to a number of factors: namely, the countries commitment and dedication to data protection, the legalistic nature of administrative and corporate cultures, and the

---

[444] Op cit note 3, *Engaging Privacy and Information Technology in a Digital Age* at 382 - 397. See also Flaherty, David H (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United State*s at 17, 19 and 183.

[445] See the judgment of Sachs J in *Mistry v Interim Medical and Dental Council of South Arica* 1998 (4) SA 1127 (CC) at 316.

[446] Op cit note 3, *Engaging Privacy and Information Technology in a Digital Age* at 382.

strong persuasive personalities who have been appointed as data protection commissions while serving in the role of the Data Protection Authority. The German law does have flaws in that the Authority does not have the power to issue legally binding orders and the mass rules are so dense that it is unwieldy and creates confusion, and there is also an issue with lack of transparency during implementation.[447]

Chapter 9 Institution

The new South African law introduces the Data Protection Authority which could be established as a Chapter 9 institution under the 1996 South African Constitution to regulate two pieces of legislation with vested powers to make binding decisions while serving as a recourse before resorting to court litigation. Currie and Allan agree that a Chapter 9 institution is the best option because the Data Protection Authority has to fall manifestly outside the government it order to meet its objectives of being independent and impartial in exercising its functions without fear, favour or prejudice as clearly envisaged by the language in the Act.[448] Section 181(2) the Constitution states that such institutions 'are independent and subject only to the Constitution and the law, and they must be impartial and must exercise their powers and perform their functions without fear, favour or prejudice.' De Vos explains that Chapter 9 institutions were envisaged to be credible independent watchdogs 'steeped in the

[447] Ibid, *Engaging Privacy and Information Technology in a Digital Age* at 397.

[448] Op cit note 15 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator' at 575.

disciplining paradigm of human rights' and supporting constitutional democracy.[449] If established as a Chapter 9 institution, the Data Protection Authority would be well placed to serve as a guardian and protect the constitutional right to privacy including data protection.

Strengthening individual rights

As an insight to the current debate in Europe, it should be noted that the European model falls short because of its initial focus on cross border data sharing and there is now a move toward elevating the focus to the rights of the individuals. In addition, the transposition of the EU Directive into national laws has been slow and even though most countries have laws in place now, there are low levels of enforcement, compliance and awareness at the national levels, and the Data Protection Authorities lack resources that have an impact on effective implementation of the laws.[450] South Africa should ensure that there is sufficient awareness of the rights and obligations embedded in the Protection of Personal Information Act and the appointed Data Protection Authority needs have muscle to be actively involved in raising awareness, ensuring redress and assisting in legal enforcement of the statutory delict which the law creates for individuals facing infringement of their right to data protection. Even though the Information Regulatory Body for South Africa will serve as a first recourse and alternative to resorting to courts,[451] the courts still have a role to play in civil suits

[449] De Vos, Pierre (2012) 'Balancing Independence and Accountability: The Role of Chapter 9 Institutions in South Africa's constitutional democracy' at 160-161.

[450] Op cit note 3, *Engaging Privacy and Information Technology in a Digital Age* at 398.

[451] Op cit note 423, 'Evaluating the Information Bills: A briefing paper on the Protection of Information Bill' at 24-26.

and in interpreting the law and enforcing data protection as legal right. In terms of chapter 10 of the Act, the courts may issue warrants if there are reasonable grounds of interference or suspected offences in violations of the Act, there are provisions for civil remedies for aggrieved data subjects whether or not there is intent or negligence, court review and appeal procedures are available, and criminal sanctions will apply if an enforcement order issued by the Data Protection Authority is not upheld.

Harm test and remedies

In their evaluation of the controversial Protection of State Information Bill, Currie and Klaaren point to a harm test that would significantly improve the draft.[452] They argue that this would put the focus on the harm and consequences caused rather than the act of disclosure itself, and in so doing, it moves away from the requirement of *mens rea* (criminal intent). This harm test is evident in the Protection of Personal Information Act as it caters for circumstances of negligence and allows recourse in the law, a defect that existed in the South African law as illustrated in NM case. While negligence is not a requirement for accountability in terms of Act, language such as 'reasonable foresight' is echoed throughout, and this provides for a remedy in the event that personal data is processed negligently. For migrants this is an important element because they often have little recourse to remedies and proving intent is a high standard. The common law only covers wrongful acts of invasions to privacy and the constitutional right to privacy does not explicitly mention data protection even though it is read-in by courts in their interpretation of the right to privacy. Currie explains that

[452] Ibid, 'Evaluating the Information Bills: A briefing paper on the Protection of Information Bill' at 24.

the Protection of Personal Information Act creates a statutory delict of 'interference with the protection of the personal information of a data subject'.[453] Thus, the concomitant right of data protection and data subjects having the right not to have their data protection rights infringed upon is a statutory right that stems from the constitutional right to privacy.

Remedy for breach is embedded in the law in that any breach of the guaranteed data protection principles or breach of provision in a code of conduct can be reported through a complaints mechanism to the Data Protection Regulator who is responsible for 'intervening to enforce the right against the alleged interference, investigating the complaint, deciding to take no action (if, *inter alia*, the complaint is moot, trivial or frivolous) or institute a civil action for damages arising from an interference with the protection of the personal information of a data subject.'[454] The Act therefore provides for civil remedies and civil sanctions to the aggrieved data subject whether or not there is intent or negligence established. This cures the defect in the common law that only allows for remedies if wrongful acts are established as was evident in the *NM* case.

Ongoing international reform to improve the domestic law

A criticism the Protection of Personal Information Act lies in the timing of its enactment. It comes into force at a time when the global trendsetters on data protection

[453] Op cit note 425, 'The Protection of Personal Information Act and Its Impact on Freedom of Information' at 7.

[454] Ibid, 'The Protection of Personal Information Act and Its Impact on Freedom of Information' at 7.

are revising their laws to enhance protection of individual rights. As such, it does not benefit from the debates that will enhance those laws and keep South Africa at the forefront of the issue. However, given the long delay in creating this specific law, the urgency to enact it goes without saying. The Legislature can always amend the law in line with latest international developments. In the meantime South Africa can benefit from a comprehensive law giving force to a data protection right and since it is adequate for European standards it can be useful in trade relations. The Act explicitly refers to factors for the Information Regulatory Body to consider in ensuring that any public interest in allowing the processing of personal data outweighs the public interest in adhering to the Data Protection Principles, this includes considering any general developing international guidelines relevant to the better protection of individual privacy. This is an important factor in the balancing test that allows for imposing stricter conditions on data collection and transfer in keeping with the latest developments at the international level.

Transborder flow of data

The adequacy of other laws for the transfer of personal data outside South Africa differs to the EU model in that the criteria for adequacy is not embedded in the law. Instead, it merely refers to the recipient of the data transfer having to be subject to a law, binding code of conduct or contract. In the EU Directive the contractual obligations is an alternative to adequate laws being in place. This intention of the drafters to keep it less burdensome for neighbouring States can be linked to the South African context and the region where data protection laws are for the most part absent. The contractual obligations imposed on neighbouring States in the absence of data

protection laws is a good starting point, but the law falls short in setting the threshold higher. It should have included the requirement of adequate laws in the Act, and in the interim where countries do not have laws in place, the contractual obligations with adequate safeguards embedded in the contractual terms could have sufficed. The alternative of codes seems to stem of the OECD and APEC models adopted by the United States focusing on industry legislation. This however creates piecemeal protection that is, in itself, not sufficient to encourage the development of legislation in neighbouring States. The requirement of adequate laws is the way in which the EU has managed to drive the expansion of data protection laws globally. This is a missed opportunity because South Africa could similarly be the driver in SADC and the African Union for the development of data protection laws in the region. The alternative is for South Africa to still act as the lead and encourage neighbours to place data protection on their legislative agendas through other political forums such as Migration Dialogue for Southern Africa (MIDSA).

South Africa to lead the region

MIDSA is a forum for training and policy debate focusing on issues relating to migration management in the region. Crush et al (2005) are of the opinion that the absorption of MIDSA into SADC as an eventuality will have important impacts on harmonizing national laws on migration and data collection systems, and this could in turn, promote more effective migration management in the region.[455] This is indeed an

[455] Crush, Jonathan; Vincent Williams, Vincent and Peberdy, Sally (2005) 'Migration in Southern Africa' A paper prepared for the Policy Analysis and Research Programme of the Global Commission on International Migration at 24 <http://lastradainternational.org/?main=documentation&document=2276>

aspiring goal and with the complex issues of mixed migration currently on the MIDSA agenda, this objective may be realized in the not too distant future.

The Protection of Personal Information Act is indeed advancing the law in South Africa, and since data protection legislation has been almost 20 years in the making, its enactment is long overdue. It will create a data protection culture in the country and it will serve as guidance for other African states, in particular for member states of the African Union or SADC that could benefit from the transborder flow of information provided adequate level of laws are in place in the region. The Act fills the big gap in the law in that it recognizes data protection as a right, but it does not explicitly recognize it as a human right. This is now left open to interpretation and the Data Protection Regulator as the avenue of first recourse, and later to the courts, who will have to interpret this with reference to the background papers where reference is made to a human rights approach. A human rights based approach helps to draw the line between balancing State interests and individual rights and clarity in the text of the law would have been in line with the recent EU data protection reform where the emphasis is placed on individual rights to balance the scale with extensive powers of the State and private entities.

As mentioned above, the South African law in some respects goes further than the EU model and this, coupled with the criteria for balancing rights as extrapolated from constitutional jurisprudence can be usefully and appropriately applied to the areas at the intersection between data protection and migration, and this could in turn, assist in

the development of comprehensive migration policies which incorporate data protection safeguards.

Since migration by its very nature involves cross border movements, the South African law cannot be reviewed in isolation. South African laws have to be examined within the regional context because national laws on migration and protection of migrant data will inevitably have an impact on neighbouring countries. The next chapter will assess whether any legal instruments exist at the SADC level and whether the European Union model can be replicated in this region, which is significantly different to the European context.

CHAPTER SIX

6. REPLICATING THE EUROPEAN MODEL IN THE SOUTHERN AFRICAN DEVELOPMENT COMMUNITY

The legal concept of privacy rights is rooted in European and North American philosophy of individual rights. When it comes to Africa the legal regimes on data protection are the least developed in the world and this is probably due to the lack of the right to privacy in the African Union legal instruments. This chapter looks at concept of *Ubuntu* and the complexities of migration in the Southern African Development Community (SADC)[456] and questions whether the European model on data protection can be replicated in this region.

6.1 *Concept of Ubuntu*

> '*Ubuntu is the fundamental belief that* 'motho ke motho ba batho ba bangwe/ umuntu ngumuntu ngabantu', *which literally translated means, a person can only be a person through others.*'[457]

In the African context, the right to privacy is not included in any of the African Union

[456] The 14 member states are Angola, Botswana, Lesotho, Malawi, Mauritius, Mozambique, Namibia, South Africa, Seychelles, Swaziland, Tanzania, Zambia, Zimbabwe and the Democratic Republic of Congo.

[457] Mokgoro J *Ubuntu and the Law in South Africa* Paper delivered at the first Colloquium Constitution and Law, Potchefstroom, 31 October 1997. <http://www.ajol.info/index.php/pelj/article/viewFile/43567/27090>

regional legal instruments on human rights, with the exception of the African Charter on the Rights and Welfare of the Child Rights (1999). In particular Article 10 states that: 'No child shall be subject to arbitrary interference with his privacy, family home or correspondence, or to the attacks its honour and reputation, provided that the parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.' This is interesting because the right to privacy does not find expression in the African Charter on Human and People's Rights (1981), yet it is explicit in the 1999 law on the rights of the child. Is it possible that the drafters came to a later realization of the importance of the right to privacy 18 years later when drafting the regional law on the rights of the child? This seems to be a reasonable explanation because the legal regime on human rights in African predates the enactment of the law on the rights of the child and there are also national laws in Africa that recognize the right to privacy as a human right afforded to all individuals without limiting it to persons under the age of 18 years.

Questioning absence of privacy in regional law

Olinger, Britz and Oliver attribute the omission of the right to privacy in the African Charter to communal considerations that have to be taken into account in the context of Africa and argue that community interests override individual protection needs because of the concept of *Ubuntu.*[458] Although the concept of *Ubuntu* is a South African transformative concept, as explained by former constitutional judge Mokgoro,

[458] Olinger, H N; Britz J J and Olivier M S (2005) 'Western Privacy and Ubuntu - Influences in the Forthcoming Data Privacy Bill' at 9 – 10 <http://mo.co.za/open/ubuntu.pdf>

it can be seen as an African philosophy of life. Cornell and Muvungu argue further that Ubuntu goes beyond its roots in Africa, it is an ethical notion, and when translated into the law it helps to expand the thinking of a modern legal system's commitment to universality and is important in any human rights discourse.[459]

Bygrave agrees with Oliver et al that communal considerations that override the individual is the reason for the underdevelopment of a data privacy regime in the African Charter of Human Rights, and therefore unlike all the other major international human rights documents, it does not have provisions on the right to privacy.[460] This reasoning is not without criticism. While communal considerations are integral to African philosophy, it is not necessarily the reason for the lack of privacy laws and the title of the Charter illustrates otherwise stating that the intension is to cover both individual (human) and collective (peoples') rights. Bygrave does argue convincingly that there is a need to argument advancement of data privacy provisions while respecting cultural values. Rotenberg similarly notes that the only exception in main fundamental human rights instruments is the African Charter for Human Rights because other instruments, namely the UDHR (Article 12), ICCPR (Article 17), Convention on the Rights of Migrant Workers (Article 14), and the Convention on Protection of the Child (Article 16), together with the main regional human rights treaties such as the European Convention on Human Rights and Fundamental Freedoms (ECHR – Article 8), the American Convention on Human Rights (Article

[459] Cornell, Drucilla and Muvungu, Nyoko ed.s *Ubuntu and Law: African Ideals and Post-Apartheid Jurisprudence* at xi and as explained in the synopsis.

[460] Bygrave, Lee A (2004) 'Privacy Protection in a Global Context-A Comparative Overview' at 319-348 and 328.

11), the Cairo Declaration on Human Rights in Islam (Article 18(b) – (c), as well Article V of the American Declaration of the Rights and Duties of Man (1948) expressly recognize privacy as a human right.[461]

Olinger et al argue that the *Ubuntu* culture requires consent of the family, clan and community; and this requirement goes against the notion of autonomous individual decisions, which is central to the right to privacy. They argue further that *Ubuntu* does not focus on the individual, as privacy does in western cultures. Instead, the emphasis is on the society as a communal entity and this contradicts the concept of individualism.[462] These arguments seem to be refuted by the preamble of the Universal Declaration of Human Rights (1948) (UDHR) which states that 'everyone has inalienable rights as members of the human family,' an underlying principle to which the 1981 African Charter prescribes.

Philosophy of Ubuntu finds legal expression

Former justice Mokgoro, described *Ubuntu* as a 'philosophy of life, which in its most fundamental sense represents personhood, humanity, humaneness and morality; a metaphor that describes group solidarity [...] and where the fundamental belief is that a person can only be a person through others [...]. Thus, its value has also been viewed as a basis for a morality of co-operation, compassion, communalism and concern for

[461] Op cit note 122, 'Data Protection Day: Joint High Level Meeting From European to International Standards on Data Protection Remarks of Marc Rotenberg.'

[462] Op cit note 458, 'Western Privacy and Ubuntu - Influences in the Forthcoming Data Privacy Bill' at 9 – 21. See also Wikipedia for further philosophical discussion on in African and Western cultures <http://en.wikipedia.org/wiki/Ubuntu_(philosophy)>

the interests of the collective respect for the dignity of personhood, all the time emphasizing the virtues of that dignity in social relationships and practices.'[463] Indeed, *Ubuntu* focuses on the community, but the individual is an integral part of the community. As concluded by Olinger et al, while there initially appears to be tension between the concept of *Ubuntu* and the right to privacy, the two can co-exist in a modern society[464] as seen in the South African context.

Ubuntu is a fundamental value that is echoed throughout the Constitution of South Africa Act, 1996 (Final Constitution), which is the supreme law of the land. Although *Ubuntu* it is not expressly mentioned, as was the case in the Constitution of the Republic of South Africa Act 200 of 1993 (Interim Constitution), it nevertheless remains fundamental and as stated in *S v Makwanyane* 'it is a concept which stresses humanness, social justice and fairness [...] and it runs like a golden thread along cultural lines.'[465] The right to privacy as guaranteed under Article 14 of the Final Constitution includes the protection of dignity and this is in harmony with *Ubuntu*.[466] In addition, the adoption of the United Nations Guidelines for the Regulation of Computerized Personal Data Files (1990) by the member states of the United Nations underlines the reality that data protection stemming from the right to privacy is not simply a 'first world' western notion.[467]

---

[463] Op cit 457, 'Ubuntu and the Law in South Africa'

[464] Op cit note 458, 'Western Privacy and Ubuntu – Influences in the Forthcoming Data Privacy Bill' at 9 -14.

[465] *S v Makwanyane and Another* 1995 (3) SA (CC) at 307-308.

[466] Op cit note 458, 'Western Privacy and Ubuntu - Influences in the Forthcoming Data Privacy Bill' at 14.

[467] Op cit note 3, *Engaging Privacy and Information Technology in a Digital Age* at 382.

Notwithstanding the aforementioned, the absence of the right to privacy in the 1981 African Charter remains and when looking at the entire African continent there are currently only a very few countries in this region with comprehensive data protection laws in force. One can only speculate as to why no binding law on the right to privacy exists for all individuals in the supranational laws in Africa. Perhaps children's rights call for an explicit reference to the right to privacy given their lack of legal capacity to consent? The more plausible argument is that the absence of the right to privacy of all individuals is an oversight. The recognition of the right to privacy in the *African Charter on the Rights and Welfare of the Child Rights* (1999) is likely due to the growing concerns with privacy issues post the enactment of the African Charter on Human and People's Rights (1981). As it stands now, the right to privacy is afforded to children and not to adults. This creates a legal lacuna that needs to be addressed by legislators at the African Union level. Nevertheless, the fundamental right to privacy is guaranteed at the international level by Article 12 of the UDHR and this applies in the absence of regional law and States are bound to respect the right to privacy that should be afforded to everyone without discrimination and must ensure non-arbitrary interference with this right.

Data protection in the African context

Flaherty rightfully points out that 'there still does not exist a truly global convention or treaty dealing specifically with data protection although interest in the right of privacy

increased in the 1960s and 1970s with the advent of information technology.[468] Nowadays, data protection considerations and concerns are increasing even more due to advanced technology being employed in Africa by governments and also by migrants themselves when moving across borders either voluntarily or as a result of forced migration. Consequently, there are a number of countries with draft data protection laws in the making. According to deliberations at the South African Parliament held on the Protection of Personal Information Act, the process of developing a Convention on the Protection of Personal Information was in discussion at the African Union.[469] This, however, seems to have fallen off the priority table given other pressing problems in Africa. In the interim, some African countries have already started developing adequate legislation to enable transfer of personal data to facilitate data exchange with Europe, and other countries are following suit.[470]

In the modern information age, data protection is a reality that cannot go without legislative regulation. If data protection were to be recognized as a legal right at the international level, it could lead to the development of regional law in Africa recognizing not only the right to privacy but also the right to data protection as dual and complementary rights. One suggestion would be to include this in one text recognizing both as fundamental rights and to append it to the African Charter on

---

[468] Flaherty, David H (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* at 22.

[469] Parliamentary Monitoring Group (PMG) 'Protection of Personal Information Bill: Departmental and Public representations' See PMG website for compilation of parliamentary debates <http://www.pmg.org.za>

[470] For example, two existing national laws can be found in Senegal (Law No. 2008-12 of 2008 on the Protection of Personal Data) and in Morocco (Law No. 09-08 Relative to the Protection of Individuals with regards to their Personal Data of 2009). See also op cit note 13 for a global overview of existing and emerging national laws on data protection.

Human Rights.

6.2 *Regional Specific Dynamics*

SADC is one of the most prominent sub-regional organizations in Africa with its member states committed to addressing regional integration and the free movement of people.[471] However, it is yet to meet the objective of enforcing a Protocol on the Free Movement of Persons in SADC much akin to the free Schengan visa regime in Europe.

Regional law on migration

In the absence of a regional legal instrument, cross border migration in the region is governed by national migration and refugee legislation, but the focus is on law enforcement, border control and exclusion.[472] In a survey conducted by the Southern African Migration Project (SAMP) it was emphasized that although there is longevity of SADC as a formal institution, there is an absence of any sense of solidarity between countries in the SADC and this has direct implications for migration issues. The survey concluded that an urgent challenge confronting the SADC and migration agencies in the region is to develop strategies and build a real sense of regional

[471] Martens, Jonathan (2007) 'Moving Freely on the African Continent: The Experiences of ECOWAS and SADC with Free Movement Protocols' at 349 in *International Migration Law: Developing Paradigms and Key Challenges.*

[472] Op cit note 455, 'Migration in Southern Africa' at 24.

consciousness amongst citizens and policymakers.[473] One of the main challenges in reaching consensus on migration issues is the economic disparity between SADC member states and the fear of being the hub for migrants that would create further challenges to citizens having to compete for scarce jobs. Equally important are their diverse historical backgrounds, development levels and political structures that often cause them to drift apart while attempting to realise the goal of facilitating the movement of persons within the SADC region.[474]

Xenophobia hampers regional harmonization

Landau, Loren, Director of Forced Migration and Refugees Studies Programme, indicated in the informal interview that 'even though South African politicians publically commit to regional integration and show nominal recognition of South Africa's humanitarian obligations, such objectives and responsibilities are not reflected in legal or administrative mechanisms on immigration.'[475] This he attributes to xenophobia attitudes that have an impact on the notion of free movement of people, free trade and freedom to choose residence in any country in the region.[476] The media is a key contributor to xenophobia because it perpetuates negative stereotypes of

---

[473] Pendleton, Wade 'Migration and Xenophobia in South Africa <http://www.iiz-dvv.de/index.php?article_id=725&clang=1>

[474] Oucho, John O (2007) 'Migration in Southern Africa: Migration Management Initiatives for SADC Member States' Institute for Security Studies (ISS) Paper 157 <http://www.iss.co.za/pgcontent.php?UID=29462>

[475] Informal interview with Landau, Loren, Director of Forced Migration and Refugees Studies Programme, conducted in Johannesburg.

[476] One example of xenophobia referred to in a political comment is as follows: 'South Africa is faced with another threat, and that is the SADC ideology of free movement of people, free trade and freedom to choose where you live or work. Free movement of persons spells disaster for our country' is evidence hereof. See: Buthelezi, Mangosuthu, 'After Amnesty: The Future of Foreign Migrants in South Africa,' Keynote Address, 20 June 1997.

migrants and often to do not distinguish between migrants travelling lawfully and those travelling irregularly, nor do they highlight the complexities of mixed migration and the special needs of vulnerable migrants.

Data protection issues are a reality in the region

Mayet, Achmed, Senior Litigator at Legal Aid South Africa, indicated in the informal interview that 'during the xenophobic attacks in 2008, the Legal Aid collaborated with Lawyers for Human Rights, Red Cross in South Africa, Human Rights Commission and UNHCR to look at criminal aspects of related charges brought against migrants for being illegally in the country and charges brought against individuals for violence and disturbing the peace. The aim of the joint collaboration was to check how many people came to Legal Aid for assistance to determine if claims were really based on xenophobia.'[477]

Mayet emphasized that cross sharing of information between the different law clinics and agencies called for heightened confidentiality. While confidentiality is dealt with by client-attorney privilege, to protect themselves against civil claims if they disclose information without consent in contravention of client confidentiality, necessary safeguards are put in place by the law clinics to allow sharing of files for the purpose of assisting clients. In the xenophobia case they had a large number of clients, and as a

[477] Informal interview with Mayet, Achmed, Senior Litigator at Legal Aid South Africa conducted in Johannesburg.

consequence, they operated under 'Chinese Walls'[478] to ensure confidentiality when lawyers represented more than one client. This was needed to prevent conflict of interest and also to ensure that the personal details of migrants were kept strictly confidential given the potential harm that could be inflicted on migrants if their personal data became known to the public.

Migration viewed positively

The UN General Secretary, Ban Ki-moon, in his world migration address said that 'we are seeing austerity measures that discriminate against migrant workers, xenophobic rhetoric that encourages violence against irregular migrants, and proposed immigration laws that allow the police to profile migrants with impunity, but with economic downturns it is worth remembering that whole sectors of the economy depend on migrant workers and migrant entrepreneurs help to create jobs.'[479] Crush et al correctly state that policies in SADC that focus on anti-immigration do not take account of the realities of globalization, the skills market and local economic development needs.[480] Indeed, if countries in the region where more proactive in developing national policies that attract economic immigrants, it could help with economic growth and employment opportunities in their own countries. As recommended by the World Migration report, migration needs to be viewed positively,[481] otherwise if it is viewed

[478] The creation of a 'Chinese Wall' is an information barrier implemented within a firm organization to prevent exchanges of information that could cause conflicts of interest. See Wikipedia for further detail <http://en.wikipedia.org/wiki/Chinese_wall>

[479] Ki-moon, Ban 'Secretary-General's Message for 2012 on International Migrants Day18 December' <http://www.un.org/en/events/migrantsday/2012/sgmessage.shtml>

[480] Op cit note 455,'Migration in Southern Africa' at 12.

[481] See op cit note 8 and note 11, *The World Migration Report 2013: Migrant Well-Being and Development.*

as a threat rather than an opportunity the market for those facilitating irregular migration will remain and flourish.

Irregular migration

The lack of a legal regime does have a link to the increase in the number of irregular movements across borders because migrants will continue to turn to unlawful methods for economic and survival reasons, and this in turn, fuels the trade in forgery of travel documents, police corruption and increase in exploitation of trafficked persons.[482] Migration has increased throughout the SADC in recent years. Crush et al say this is 'due in part to the end of Apartheid in South Africa, the integration of South Africa into the region's linkages to the global economy, increased rural and urban poverty and unemployment, the impact of HIV/AIDS, as well as a history of forced migration and the mass relocation of people.'[483] While the numbers of migrants travelling irregularly have increased in the region, this is not unique to the region; States are facing this same challenge in all regions of the world.

Rights based approach

Ngandwe rightfully points out that 'States have to adopt a rights based approach to migration and refugee laws and policies. Comprehensive approaches to irregular migration, beyond treating it as a law and order issue, are needed to address its root

[482] Op cit note 455, 'Migration in Southern Africa' at 13.

[483] Ibid, 'Migration in Southern Africa' at 30.

causes, and to protect the basic human rights of workers with irregular status in line with international norms.' Moreover, 'once domestic laws and policies are in harmony with international law, there will be synergy in legislation and policy at national level and on an international plane.[484] Indeed in their efforts to manage migration comprehensively and effectively, SADC should be mindful of the mixed flows of people making their way to the tip of Africa. Vulnerable migrant groups such as refugees, trafficked persons and unaccompanied migrant children often also travel without the requisite travel documentation, yet they require States to exercise their obligations under international human rights and humanitarian law to protect them. A regional response to mixed migration can assist SADC member states to meet their international law obligations and at the same time they can create regional strategies and laws to address migration more comprehensively and this incudes data protection.

Trafficked persons

According to Martens, Jonathan, Senior Specialist on human trafficking issues at the International Organization for Migration, 'since trafficked persons are often exploited by sophisticated criminal networks, the need for data protection is paramount. This is because criminal groups have the capacity to carry out retributive action against victims of trafficking and their families and relatives back home. In addition, victims of trafficking are also vulnerable to stigmatization and ostracization on account of the

[484] Ngandwe, Phazha Jimmy (2013) 'The Paradox of Migration and the Interests of the Atomistic Nation-States: The Southern African Perspective' at 444 – 445.

exploitation suffered.'[485] The absence of an internationally binding law on data protection has resulted is an array of different national data protection laws. While some laws require non-disclosure of personal data, others do not, and this can result in serious risks and endanger trafficked persons and their families. For example, access to bank details of family members could result in individuals being kept as ransom because they are a good target and reprisal against the trafficked person is a common technique used by traffickers. The need for strict data protection safeguards are heightened with the potential threat to life and when weighing the principle of confidentiality with the need to access personal data to investigate trafficking crimes, the 'do no harm' principle which is central to victim assistance will always trump any third party interest.

Regional discourse

At the UNHCR Regional Conference on Refugee Protection and International Migration: Mixed Movements and Irregular Migration from East Africa and the Great Lakes to Southern African held in 2011, the following vulnerable groups amongst others travelling in mixed migratory flows where highlighted to ensure that immigration officers at borders take account of their special needs; 1) *Women*: identification of 'women-at-risk' through pre-screening is essential because they need separate sleeping and washing arrangements in reception centres, as well as the presence of appropriate female staff who are also involved in conducting interviews relating to their travel experience; 2) *Trafficked persons*: special procedures are needed

[485] Informal interview with Martens, Jonathan, Migrant Assistance Specialist at the International Organization for Migration conducted in Geneva.

to identify potential victims of trafficking to ensure they are separated from traffickers and to prevent traffickers and smugglers from accessing reception centres; and assistance is needed to receive asylum seekers and in preparing asylum claims; 3) *Victims of torture or trauma*: availability of basic medical facilities and psychological support is important, and specific assistance with asylum applications or other procedures are needed; '*Children*, particularly unaccompanied and separated migrant children require the appointment of guardians, systematic determination of their best interest, assistance with access to asylum procedures and preparation of their asylum claim, and alternative accommodation arrangements.[486]

Children

UNCHR states that the 'best interests of the child' principle requires 'comprehensive child protection systems comprised of laws, policies and procedures designed to prevent and respond effectively to child abuse, neglect, exploitation and violence.'[487] Under the 1989 Convention of the Rights of the Child (CRC) all children, regardless of their nationality, enjoy inalienable human rights. This is echoed in the cardinal principles of the 1999 African Charter on the Rights and Welfare of the Child. Children are by their nature vulnerable because they lack legal capacity and are dependent on the support of parents to look out for their best interests. During the migration process, and more increasingly in mixed migration, there is inevitably significant numbers of minors who are unaccompanied and they are even more

[486] United Nations High Commissioner for Refugees (UNHCR) 'Regional Conference on Refugee Protection and International Migration: Mixed Movements and Irregular Migration from East Africa and the Great Lakes to Southern African' Dar es Salaam, Tanzania, 6-7 September 2011, Summary Report at 30-33 <http://www.unhcr.org/4d7f7ef711.pdf>

[487] United Nations High Commissioner for Refugees (2008) 'UNCHR Guidelines on Determining the Best Interests oft he Child' at 17.

vulnerable because they lack the support of their parents to help them deal with traumatic experiences.

In South Africa, for example, unaccompanied migrant children sometimes face further difficulties as they continue without support structures, often find it difficult to access Refugee Reception Offices and as a result remain in the rural border areas without documentation where they are vulnerable to arrest and deportation.[488] Unaccompanied migrant children require the State to appoint legal guardians who can best serve their interests. Even though the unaccompanied migrant children who are under 18 years of age will not have the legal capacity to consent to the collection and processing of their personal data, their views and opinions should be taken into account depending on the age and level of maturity. The consent of their legal guardians should therefore be supplemented by the consent of the child in cases where the child is capable of appreciating and understanding the reasons why personal data is collected and for what reasons it will be used. This is in line with Article 12 of the CRC and it will also help to identify and address the specific needs of the unaccompanied migrant children.

Asylum seekers and refugees

All SADC member states have ratified or comply with the 1951 Convention Relating to the Status of Refugees and the more inclusive 1969 OAU Convention Governing

[488] Makhema, Mpho (2009) 'Social Protection for Refugees and Asylum Seekers in the Southern Africa Development Community (SADC)' Discussion Paper No. 0906, Social Protection and Labour, the World Bank' at 34 < http://siteresources.worldbank.org/SOCIALPROTECTION/Resources/SP-Discussion-papers/Labor-Market-DP/0906.pdf>

the Specific Aspects of Refugee Problems in Africa. The countries in the region, however, follow different refugee models and South Africa is only the country that does not require refugees to live in designated areas or camps.[489] Despite claims based on well-founded fears of persecution, asylum seekers and refugees often face secondary vicitimization and are blamed for crime and unemployment in the region, sometimes this is warranted but not always. While some refugees may indeed be involved in crime, statistics has not proven that migrants are a contributing factor to the level of crime rates.

Often refugees are well skilled and qualified professionals in their country of origin, but they are willing to take low skilled jobs to survive in their new destination country. If SADC were to focus on making use of their profession skills it could create sustainable economic growth and job development for lower skilled labourers. What is needed is a data collection exercise that would result in an analysis of the varied skills available among the refugee communities. Such data collection exercises would have to be undertaken in accordance with a common research methodology while upholding adequate data protection standards.

Data protection for SADC

Since SADC aims to develop regional strategies on common issues experienced amongst member states, it would also be useful for SADC to develop a data protection regional law for the region that would facilitate data exchange using the same set of

[489] Op cit note 455, 'Migration in Southern Africa' at 26-26.

data protection standards to ensure uniformity. Collecting personal data of migrants is crucial to understanding the root causes of migration and it is necessary to analyze the needs of vulnerable migrants arriving at border posts. As acknowledged by Roos, when collecting personal data every aspect of the data processing cycle is influenced, including the manner of its collection, periods of retention, further processing, disclosure to third parties and any further issues that may apply to the processing of the information.[490] Having a data protection regulatory framework in place is therefore important. Principle 2 of the UNHCR 10 Point Plan on Mixed Migration and Refugee Protection focuses on data collection and analysis with the view to capacitate States to build protection-sensitive systems when managing migration.[491] Accordingly, data collection methods, analysis and the exchange of personal data in this context need to be in accordance with internationally accepted data protection standards. It is, thus, important to mobilize SADC to put data protection on the policy, legislative, and political agenda and to incorporate it into comprehensive responses to migration management.

Data protection concerns

The different groups of migrants travelling in mixed migratory flows lie at the intersection between migration and international protection and they accurately reflect the diversity of migrants as it includes unaccompanied migrant children, victims of human trafficking and human smuggling, disabled persons, asylum seekers and

[490] Roos, Anneliese (2008)'Data Protection' in *Information and Communications Technology Law* at 374.

[491] United Nations High Commissioner for Refugees (2011) 'Refugee Protection and Mixed Migration: The 10-Point Plan in Action' at 53 < at: http://www.refworld.org/docid/4d9430ea2.html>

refugees, stranded migrants and economic migrants.[492] As stated in chapter 2, unwanted and inappropriate disclosure of personal data, particularly sensitive data could result in a wide range of risks. This is exacerbated for vulnerable migrant groups such of asylum seekers and refugees, unaccompanied migrant children and trafficked persons who have specific needs when travelling alongside other migrants in mixed migratory routes.

With mixed migration there are inevitably significant numbers of irregular migrants, some who travel for economic reasons, but also others who fall in the blurred line of travelling irregularly and who are at the same time fleeing persecution and human rights abuses. A law enforcement approach to migration management and border control is therefore not sufficient as it obscures the States' international human rights obligations in protecting the specific needs and vulnerabilities of certain migrants. To address this, the World Migration Report encourages States to approach migration management in a coherent and systematic manner by taking account of the human rights and the positive aspects of migration.

Human rights and data exchange

Notwithstanding the challenges of adopting regional laws to facilitate free movement, SADC has made significant progress on the issue of trade.[493] The dominance of the

[492] Ibid, 'Refugee Protection and Mixed Migration: The 10-Point Plan in Action.'

[493] Op cit note 471, 'Moving Freely on the African Continent: The Experiences of ECOWAS and SADC with Free Movement Protocols' at 360.

European Union in international trade and politics has led to the development of data protection laws beyond the borders in Europe.[494] Similarly if SADC recognizes the transborder flow of data as a trade issue, it may have better success in developing and implementing a regional law on data protection. Data protection laws have the twin goal of protecting human rights and facilitating data exchange across borders. The latter has economic value and has been used as a trade incentive by Europe to encourage the development of national laws on data protection even outside Europe.

South Africa is currently increasing its presence on the continent and many South African companies have offices throughout the region that would engage in business requiring the handling of personal data of South Africans across borders. Cross border trade by business and movement of people and goods through informal trade is evident in SADC even if such movements are not regulated. Oucho says that 'regional incentives and integration is meaningless unless people within a defined area of jurisdiction share experiences, exchange interests and move with their products across borders.[495] Research into this area is needed and the data collection requires a common data protection standard to ensure that personal data and the outcome of qualitative data can be easily analysed and mutually beneficial to countries in the region. Data protection is, thus, an important issue for trade relations and SADC can replicate a regional data protection framework law as implemented in Europe in order to address the complexities in the region.

---

[494] Op cite note 458, 'Western Privacy and Ubuntu - Influences in the Forthcoming Data Privacy Bill' at 9 – 13

[495] Op cit note 474, 'Migration in Southern Africa: Migration Management Initiatives for SADC Member States.'

South Africa lead by example

South Africa could spearhead discussions between SADC member states based on its recently enacted data protection law. However, it would have to explicitly highlight and ensure that migration issues are also present to ensure that the interface between data protection and migration is covered. According to Bernardo, Mariano, Regional Director of Southern Africa at the International Organization for Migration, South Africa cannot drive this initiative on its own; instead support from three or more middle-income countries is needed. A factor to consider is that South Africa is one of the countries in the region that has the technological capacity to integrate biometric systems and process data electronically. Other countries are still processing personal data manually, thus, compatibility needs to be taken into account when developing laws to facilitate data exchange in the region.

Mixed migration affects many countries including Tanzania, Mozamibique, Namibia, Zambia, Zimbabwe and South Africa, but each country has an individual state-by-state response to address the challenges.[496] Migration involves cross border movements, and questions relating to migrants' rights and how to assist specific needs of vulnerable migrants, require cooperation and coordination to approach migration in a holistic manner. In addition, the impact of national law on migration goes beyond borders and this has an impact on other countries in the region.

[496] Informal interview with Mariano, Bernardo, Regional Director of Southern Africa, at the International Organization for Migration conducted in Geneva while on travel duty.

Replicating the European data protection model

Similar to other migration issues, data protection of the personal information of migrants should be addressed from a regional perspective. Of significance is the fact that data protection was already discussed by SADC in 2012 within the context of the workshop on the harmonization of a draft cyber-security legal framework which aimed at reviewing, amending and validating regional model laws on electronic transactions, protection of personal data and the fight against cybercrime.[497] This initiative was instigated by Botswana who was in the process of developing a national law on cyber security and had concerns with the change to paperless information gathering methods which gave rise to stealing of personal identities and hacking of databases.

Draft model data protection law

During the workshop delegates drafted three draft Harmonized Model Laws including a Draft Harmonized Data Protection Law. The draft model law was validated by the SADC delegates and critical next steps where discussed.[498] Even though this model draft law would not have any binding force and would merely be seen as a best practice model, it could be seen as the stepping stone to develop a regional law on data protection. Since South Africa has recently enacted its data protection legislation, it would be perfectly placed to reopen discussions and emphasize the need to create a

[497] 'Media Statement on the Validation Workshop of SADC Harmonized Cyber Security Legal Framework' held at the GICC in Gabrone from the 27th February to 2nd March 2012 <http://tis.sadc.int/files/1813/3232/7429/media_statement_cyber_security_version_2.pdf>

[498] Ibid, 'Media Statement on the Validation Workshop of SADC Harmonized Cyber Security Legal Framework' at 3.

binding regional instrument to govern data protection and to include necessary aspects of migration that are region-specific. The model law on data protection could then be attached as an annexure to the binding law to ensure harmonization in the region. Although the dynamics in Europe and SADC are different, the challenges surrounding migration and data protection are similar albeit complicated by the traditional lack of harmony amongst member states in SADC. The South African law is a good starting point because the approach taken by the drafters included tailoring the European model to best fit the South African context. This saves counties in the region from having to reinvent the wheel and start research initiatives from afresh.

By drawing on the South African law, it could be used as a benchmark for developing a regional legal instrument. While a top down approach is usually better, in the absence of a legally binding instrument on data protection at the international level, laws can be developed from the bottom up and this could give States the opportunity to share experiences and collaborate in finding solutions to challenges arising in the area at the interface between data protection and migration. MIDSA and other international fora could be used to keep the momentum going, and this could in turn, assist the SADC block to reach consensus to strengthen privacy and data protection rights in this region.

CHAPTER SEVEN

7. CONCLUSION

The purpose of this thesis was to look at the intersection between migration and data protection. Specifically, to what extent should States be allowed to intrude into the private sphere of the individual migrant? Should advanced technology drive policy or should we rather adopt a cautionary approach and develop laws that are flexible in its reach? Where do migrants fall in the discussion when developing laws on data protection and is the current legal framework on data protection at national, regional and international level sufficient to address the rights of people on the move?

The last decade has witnessed the increased use of advanced technology to manage large volumes of personal data and monitor migratory movements. Since migration law and policy tend to focus on border control as its main objective, the use of advanced technology within the migration context poses a real challenge to the human rights of people on the move. Migration management has gained political salience due to globalization, terrorism and irregular movements within and across borders. To ensure effective migration management, initiatives should not only cover deterring clandestine movements across borders and combating terrorism, but it should also cover protecting human rights at all stages of the migration cycle. This will help States to address migration more comprehensively. The security interests of States and the rights of individuals are not, and should not be mutually exclusive. While State sovereignty envisages the right to protect borders and to determine nationality, admission and conditions of stay and removal; once in the country States are obligated

by international law to protect respect and enforce human rights without any discrimination and regardless of whether the individual is travelling in a regular or irregular manner.

A commonality between the two spheres of data protection and migration is that there currently exists no global overarching binding legal instrument, and as a result, the area at the interface between the two is in itself challenging. The rights of migrants are dispersed across different bodies of international law. Similarly, the regulation of data protection is only covered by the UN Guidelines, which has had little influence on State's actions due to its non-binding nature. The application of a human rights approach to both migration and data protection is essential to ensure that the exercise of State sovereignty is reasonably justified when it intrudes on individual rights. A human rights approach seeks to ensure that the exercise of State sovereignty is legitimate and proportional, and more importantly, that it has a justified reason embedded in the law to which States can be held accountable.

Although some countries have specific data protection laws, government agencies and law enforcement authorities have been given significant exemptions to protect the interests of States. In other countries, laws have not kept up with advanced technology or they simply do not have specific data protection laws, leaving significant gaps. States are aware of their international obligations, but they need to go further, to establish adequate national legal regimes confirming the legal rights of individuals. States should acknowledge the risks associated with unwanted and inappropriate

disclosure of personal data, including endangering the safety and security of individuals because this is an inescapable reality in the migration context. The increased use of advanced technology, such as biometric systems, is indeed a means by which to manage borders and gather information to protect State security, but it should not be used at the expense of infringing the rights of individuals, particularly the right to privacy and data protection, human dignity, non-discrimination, free lawful movement and family unity. While biometrics should be used with caution, the technology itself can also enhance data protection and this aspect should not be neglected. This applies equally to the use of crisis mapping, when used as a tool in humanitarian interventions. As argued by Hornung, technology and privacy are intertwined because 'technology influences people's understanding of privacy, and people's understanding of privacy is a key factor in defining the direction of technological development.'[499] A major concern is that technology often drives policy when the opposite is needed. Laws and policy imperatives should regulate the use of advanced technology. The recommended starting point is the promulgation and ratification of an international legal instrument that is binding on States and that recognizes the need to collect and process personal data, while ensuring adequate data protection safeguards.

The right to data protection stems from the right to privacy, which is protected as a human right in the Universal Declaration of Human Rights and this right is reiterated in international treaties such as the ICCPR. Even though the UDHR is soft law, it

[499] Op cit note 23, 'Regulating Privacy Enhancing Technologies: Seizing the Opportunity of the Future European Data Protection Framework.'

forms part of customary law, and this together with the international treaties creates positive obligations on the international community. This thesis argues that the right to privacy forms the basis for establishing a separate legal right to data protection which is needed due to the rapid growth of technology and the imbalance between the power of the State and the power of individuals to assert their rights. Privacy and data protection is, however, not without limitation and matters of public interest or legitimate government purposes may often override the scope of this protection. Core principles of data protection include confidentiality and consent and this is based on the notion that every individual has the right to choose when and to whom they wish to reveal their personal data. While there may be legitimate purposes for limiting individual rights, a big brother approach is not welcomed in the 21st century where democracy allows for the equality of all and separates the public from the private sphere.

The information age has brought the rapid expansion of technology and this is being used to manage migration, often in the absence of any regulatory laws. Since technology will continue to advance in the coming years, a legally binding framework law on data protection is needed which is flexible enough to cater for future advancements in technology. The approach of having a framework law that allows for the creation of code specific rules to protect the right to data protection is the correct one. The provisions on sensitive data are most relevant to migrants because this is needed, for example, to issue travel documents or permits as a means by which to address the rights and needs of persons fleeing a well-founded fear of persecution and to determine the special needs of other vulnerable migrants such as migrants with

HIV/AIDS, trafficked persons and unaccompanied migrant children who often cross borders irregularly and usually live outside a regulatory framework. If the personal data of migrants are used inappropriately and disclosed without authorization it could result in wide range of risks ranging from discrimination to physical harm and loss of life. It is, thus, important to always properly balance the benefit of collecting personal data with the risk of unauthorized disclosure.

The growing gap between the rapid increase in the use of advance technology and the lack of laws regulating data protection calls for immediate action by States. There is no need for a specific data protection law to cover migrants. The creation of a binding international treaty on data protection could broadly cover people on the move. States would have obligations to equally protect the rights of these individuals when engaging in the collection, processing and sharing of personal data for State purposes such as border control and terrorism. It would also help to ensure that there is indeed a balance between State interests and individual human rights with an emphasis on avoiding migrant profiling, discrimination and xenophobia. A data protection treaty would give rise to legally binding obligations requiring the enactment of national laws to give effect to the dual purpose of facilitating the use of advanced technology while equally ensuring that personal data is handled with due care and in accordance with acceptable data protection standards and human rights obligations. States, legislators and policy-makers should always bear in mind that any restriction to individual rights must not impair the essence of the right and that the relation between the right and the restriction, or between the principle and the exception, should not erase the right.

Principally, the laws authorizing restrictions must include precise criteria and the law itself has to establish the modalities under which rights may be restricted; otherwise it leaves unfettered discretion to those responsible for implementing and enforcing the law. The factors put forward by the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism for determining whether intrusion into the privacy sphere is reasonable and justified are useful and may serve as a model in this area. These include: 'the type of record requested; the information it does or might contain; the potential harm in any subsequent non-consensual disclosure; the injury from disclosure to the relationship in which the record was generated; the adequacy of safeguards to prevent unauthorized disclosures; the degree of need for access; and whether there is an express statutory mandate or articulated public policy militating toward access for public interests reasons.'[500]

When weighing competing rights and interests, the nature of the right, the importance of the limitation, the nature and extent of the limitation, the relation between the limitation and its purpose, and the less restrictive means to achieve the purpose should be taken into account. Since there is no absolute standard for determining reasonableness and justifiability and there is no immutable standard of privacy expectation, this balancing test will depend on the circumstances to be determined on a case-by-case basis.[501] If individuals have to carry the burden of protecting their own privacy rights, then the law and regulation should assist individuals in asserting such

[500] See chapter 4.1 discussed earlier.

[501] See chapter 5 discussed earlier.

rights. This is because privacy is at an inherent disadvantage when decision-makers weigh privacy against other interests where the benefits of the State's interest appear to be more pressing. The onus is therefore on States to reduce this disadvantage by establishing formal mechanisms to advocate for the right to data protection, especially because rights on paper are often of little value if it is not respected and enforced. Data Protection Supervisory bodies can play this role as independent guardians of fundamental rights and freedoms with respect to the protection of personal data. As an interim mechanism before application to courts, Data Protection Supervisors can facilitate review and appeal procedures that are more easily accessible to individuals and less costly than court procedures. Such review and appeal procedures will also help to ensure due process and regulate the wide-ranging powers of police and intelligent agents using personal data gathered through surveillance for investigatory reasons.

In South Africa the Protection of Personal Information Act is clear in its intent, it aims to regulate the collection and processing of personal data by the State and private bodies. Extensive academic research has guided the development of this law and the South African Law Commission has done a good job to eloquently describe the history of the right to data protection and to analyse existing laws in other jurisdictions in order to ensure that the South Africa's law is in line with the international trend. South African case law includes relevant factors for balancing the right to privacy with other constitutional guarantees and this is transferable to future cases involving data protection. Since personal data is easily accessible through the internet and social media, it has a cross-border dimension and the South African law cannot be seen in

isolation. If data protection were to be recognized as a legal right at the international level, it could also lead to the development of a regional law in Africa recognizing not only the right to privacy but also the right to data protection. One suggestion is to include the right to privacy and data protection into one legislative text recognizing both as human rights and to append it to the African Charter on Human Rights to give it the legal force it requires. Placing data protection on the legislative agenda at the African Union may, however, take time due to capacity and legitimacy problems a the African Union and because other urgent issues on the continent require attention. In the interim, the SADC could benefit from drawing on and replicating the European data protection model that will have to be tailored for the regional specific needs. A

s a sub-regional organization that is already focused on migration issues, SADC has the potential to be instrumental in developing a comprehensive approach to migration strategies by including data protection in their discussions. It is true that SADC has had little muscle due the economic disparity and diverse political priorities between its member states. However, the increase in mixed migration flows in Southern Africa has placed the need for collaboration between member States back on the agenda. Recent discussions between some SADC member states include exploring regional solutions to address migration management and the protection of personal data of migrants could contribute to this discussion, particularly if the value of data protection is seen from the economic perspective. In any event, the application of the data protection law in South Africa will have to be examined within the regional context because it will inevitably have an impact on neighbouring countries. With the EU data protection reform there is a shift that tilts the scale from data sharing and cross border flow of

information to individuals having the right to have their personal data adequately protected. This human rights approach could be the starting point for African counties and it will help to advance democracies amidst economic and political challenges. It also has the potential to place the SADC block, which is rich in resources, as an equal player to Europe. The data protection law in South African has taken almost 20 years to find its shape, it is now finally enforced and South Africa should use this opportunity to open discussion with its neighbours in order to set a good standard data protection model for the region.

It is equally important for States to look at the practical challenge of giving expression to human rights in the context of migration management. Mere legislation is not enough because human rights should be guaranteed *de jure* and *de facto*. Cooperation and training is essential and it should be seen as major tools in rethinking how best to address the complex issues that arise at the interface between data protection and migration. 'The factors driving migration are numerous and complex: many migrants migrate in search of greater opportunities to earn a better living, to live in a more agreeable environment or to join family or friends abroad. Of course, a significant number of migrants do not move of their own free will but are forced to do so – refugees escaping persecution, for instance; people devastated by conflict or natural disaster; or victims of trafficking [...] and the consequences of migration for the lives of individual migrants can easily be overlooked. [...] Instead of being the passive subjects of enquiry, migrants should be given the opportunity to tell their stories. This emphasis on the experiential dimension [...] could open the door to policymaking that

is more attuned to human needs.[502] The voice of the migrant is important in developing laws addressing the interface between data protection and migration. It will also help to ensure that laws are implementable which will, in turn, enhance the protection of the human rights of migrants.

At the international level the increase of privacy concerns and data protection has led to the Madrid Resolution and the *Joint Proposal for Setting International Standards on Privacy and Personal Data Protection*. While the Draft Law received input from Data Protection Supervisors and privacy advocates around the world, its failure is simply due to the absence of the participation of States and policy makers. A comprehensive approach involving dialogue between all stakeholders from both the private and public sector is necessary to ensure global consensus and the Draft Law can lead the next step discussions.

The German Chancellor alluded to having the global law take the form of a Protocol to be attached to the International Covenant on Civil and Political Rights (ICCPR). This approach would be similar to the United Nations Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children supplementing the United Nations Convention against Transnational Organised Crime of 2000. One common critique of the Trafficking Protocol is that it falls short from the human rights perspective because it is viewed through the criminal lens by virtue of its attachment

[502] Op cit note 11, *The World Migration Report 2013: Migrant Well-Being and Development* at 175.

to a crime prevention international treaty.[503] To cure a similar defect, the data protection law could supplement the ICCPR, which is a human rights treaty.

Since the use of technology must be compliant with the prevailing norms and international standards governing the right to data protection, this thesis supports the view that data protection should have a firm legal basis to ensure that State interests do not overshadow individual rights. The ongoing public debate surrounding the use of advanced technology and the threat that it poses on individuals and democracies calls for an urgent need to develop a binding law on data protection to prevent identity theft, discriminatory migrant profiling, and continuous surveillance that disregard individual human rights. The importance of data protection must become a legislative priority at the international, regional and national level, lest we fall prey to invasions of privacy as demonstrated by the ongoing leaks made by Edward Snowden in the United States of America where the absence of legislation and regulation resulted in unwanted and secret disclosure under the guise of protecting people from terrorism which is now threatening global relations.

The choice between the rights of individuals and the use of modern technology to protect State interests in managing migration creates a false dichotomy because technology and data protection can mutually exist. There is indeed a tension between State sovereignty, globalization, migration, and human rights; but they can be compatible if the exercise of States sovereignty is done in conjunction with the

[503] See for example, Danziger, Richard; Martens Jonathan and Guajardo, Mariela (2009) 'Human Trafficking and Migration Management at 261 – 298.

exercise of State obligations under international human rights and humanitarian laws if echoed in national laws protecting individual rights and equally ensuring that the objectives of States interests are fulfilled. It is understandable that drafters require time, but the societal needs today are far too great to lag behind and legislators need to act in haste to keep up with the growth in advanced technology that are impacting on existing individual rights.

This thesis does not argue that States are unaware of their international obligations. Instead, it seeks to emphasize that States need to go further, to establish adequate legal regimes confirming the legal right to data protection in order to protect all nationals and migrants alike. Given the broad scope of the research further areas of research were identified as future topical issues. First, the volume of research material on privacy, data protection and migration as separate areas gave rise to interesting issues at their points of intersection, however, only limited issues could be covered in this thesis as the focus turned to the South African context. The topic of the research is relevant to the international community and more needs to be written from the global perspective as the law continues to develop. Second, while States have sovereignty to control borders, this right is sometimes outsourced to private entities who engage in cross border activities and become *de facto* state agents while not being subjected to the same obligations as *de jure* State agents. The question of whether States are responsible for *de facto* agents needs further discussion. It would, thus, be interesting to determine the extent to which the outsourcing of migration management is covered in the developing law on data protection at the international level. Third, in the absence of an internationally binding instrument on data protection, the policies and

codes of conduct in organizations working directly with migrants are disparate. International organizations often provide States with technical expertise on migration issues, which in turn, inform the development of national laws and policy. A detailed survey of these varying data protection standards used by international organizations would thus be useful, but most UN agencies are still in the process of developing their internal laws on data protection. This assessment can only take place once such laws are implemented and will have to be canvassed in another paper.

CHAPTER EIGHT

8. ATTACHMENTS:

8.1 ANNEXURE A – INTERVIEW QUESTIONS

This thesis focuses on the balance between States interests and individual rights and looks specifically at the meeting point and challenges in the area at the interface between migration and data protection. Your expertise and experience would be very helpful to help draw the line to ensure that State interests do not overshadow individual rights. This interview is based on a semi-structured questions and the flow of the discussion will depend on your area of expertise.

- What categories of migrants are assisted by your organization and can you explain the types of assistance provided?
- Does your organization collect and process personal data of migrants either directly or indirectly?
- For what purpose(s) does your organization collect personal data and who are the actors/partners involved internally and externally?
- Are there any laws, policies, rules and procedures followed by your organization when collecting and processing the personal data of migrants for the purpose of your work and has your organization had any challenges in its implementation?

- Are there any safeguards in place when handling personal data e.g. information storage and security around electronic and paper records and any conditions surrounding access to files in the office?
- Are migrants aware of the reasons for collecting and processing their personal data, how do you go about obtaining consent prior to collecting personal data, and have you had any challenges in this regard?
- Does your organization engage in risk assessments or have a procedure for identifying sensitive categories of personal data prior to collecting it from migrants and can you explain any partners that would require access to such data in order to assist the migrants?
- Do you have any experience in relation to requests by third party to access client information, and if so, which kinds of entities usually make such access requests?
- What are your opinions on the use of biometrics in migration management and do you foresee any implications on the human rights of migrants?
- Did you have any cases involving personal information access or infringements on privacy rights of your clients?
- Are you aware of any privacy issues of migrants arising out of the xenophobic attacks in South Africa?
- Has your organization been involved in mixed migration, privacy rights, or specific data protection issues?
- Where you/your organization engaged in comments made on the Protection of Personal Information Bill in South Africa?
- What are your views on the impact of the Protection of Personal Information Bill on the South African law and does it adequately cover migrant groups?

- Do you think there is a need for special protections when it comes to certain types of sensitive personal data such as refugee status or HIV status?
- Are you aware of any laws in the Southern African Development Community (SADC) covering data protection and are member states keen to discuss this as part of their migration management strategies and policy initiatives?
- What are the specific migration challenges in the region and do you foresee SADC member states taking data protection more seriously and placing it on the agenda for discussion?
- What are your thoughts on reconciling State interests stemming from sovereignty and individual migrant rights stemming from universal human rights afforded to them regardless of their nationality or immigration status?
- What are your views on the EU Directive on data protection and its latest reforms?
- Traditionally data protection is seen within the realm of privacy, do you think there is a need for a separate right on data protection?
- What are your views on creating a separate multilateral agreement on data protection to enforce data protection as a universal legal right?
- Do you have any recommendations on how to address the gaps in the law to better protect migrants when collecting their personal data for migration management and humanitarian purposes?
- What do you foresee as challenges both legally and in practice in the area at the interface between data protection and migration and do you have any views on how to address such challenges?

8.2 ANNEXURE 2 – KEY TERMS DEFINED

Since this thesis focuses on data protection in the context of international migration, the key terms that are used are drawn from the IOM Glossary on Migration, 2nd Edition. As acknowledged by the authors, there is an absence of universally accepted definitions when it comes to migration. This is because migration is a dynamic concept, addressed traditionally within national contexts, and even its implications and effects are interpreted from varying perspectives within a given country. [504]

Asylum: A form of protection given by a State on its territory based on the principle of *non-refoulement* and internationally or nationally recognized refugee rights. It is granted to a person who is unable to seek protection in his or her country of nationality and/or residence in particular for fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion.

Asylum seeker: A person who seeks safety from persecution or serious harm in a country other than his or her own and awaits a decision on the application for refugee status under relevant international and national instruments. In case of a negative decision, the person must leave the country and may be expelled, as may any non-national in an irregular or unlawful situation, unless permission to stay is provided on humanitarian or other related grounds.

Biometrics: The study of measurable biological characteristics. "Biometric

[504] Op cit note 2, *International Migration Law: Glossary on Migration*

identifiers" (BIs) are pieces of information that encode a representation of a person's unique biological make up (e.g. fingerprints, retinal scans or voice scans). Some governments have introduced the use of biometrics as an improved security measure in issuing passports, visas or residence permits.

Border control: A State's regulation of the entry and departure of persons to and from its territory, in exercise of its sovereignty, whether this is conducted at the physical border or outside of the territory in an embassy or consulate.

Border management: Facilitation of authorized flows of persons, including business people, tourists, migrants and refugees, across a border and the detection and prevention of irregular entry of non-nationals into a given country. Measures to manage borders include the imposition by States of visa requirements, carrier sanctions against transportation companies bringing irregular migrants to the territory, and interdiction at sea. International standards require a balancing between facilitating the entry of legitimate travellers and preventing that of travellers entering for inappropriate reasons or with invalid documentation.

Child: An individual being below the age of eighteen years unless, under the law applicable to the child, majority is attained earlier *(Art. 1, UN Convention on the Rights of the Child, 1989).*

Crimes against humanity: As identified in *Art. 7 of the Rome Statute of the International Criminal Court, 1998,* crimes against humanity are crimes "committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack." The crimes contemplated under this definition include murder; extermination; enslavement; deportation or forcible transfer of population;

imprisonment or other severe deprivation of physical liberty in violation of fundamental rules of international law; torture; rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization, or any other form of sexual violence of comparable gravity; persecution against any identifiable group or collective on political, racial, national, ethnic, cultural, religious, gender (as defined in paragraph 3 of *Art. 7),* or other grounds that are universally recognized as impermissible under international law, in connection with any act referred to in this paragraph or any crime within the jurisdiction of the Court; enforced disappearance of persons; the crime of apartheid; other inhumane acts of a similar character intentionally causing great suffering, or serious injury to body or to mental or physical health.

Globalization: A process of interaction and integration among the people, corporations, and governments of different States; a process driven by international trade and investment and aided by information technology. This process has effects on the environment, culture, political systems, economic development and prosperity, and human well-being in societies.

Human rights: Those liberties and benefits based on human dignity which, by accepted contemporary values, all human beings should be able to claim "as of right" in the society in which they live. These rights are contained in the *International Bill of Rights,* comprising the *Universal Declaration of Human Rights, 1948,* the *International Covenant on Economic, Social and Cultural Rights,* and *the International Covenant on Civil and Political Rights, 1966* and have been developed by other treaties from this core (e.g. *The Convention on the Protection of All Migrant Workers and Members of Their Families, 1990).*

Humanitarian assistance: Aid that addresses the needs of individuals affected by crises. It is primarily the responsibility of the State but also supported by international organizations, non-governmental organizations (NGOs) and the Red Cross/Red Crescent Movement. This assistance is provided in accordance with the humanitarian principles, particularly the principles of humanity (human suffering must be addressed wherever it is found, with particular attention to the most vulnerable in the population, such as children, women and the elderly; the dignity and rights of all victims must be respected and protected), neutrality (humanitarian assistance must be provided without engaging in hostilities or taking sides in controversies of a political, religious or ideological nature), and impartiality (humanitarian assistance must be provided without discriminating as to ethnic origin, gender, nationality, political opinions, race or religion. Relief of the suffering must be guided solely by needs and priority must be given to the most urgent cases of distress).

International migration law: International norms and principles relating to migration deriving from State sovereignty – such as the right to admit, detain and expel migrants, to combat trafficking and smuggling, to protect borders, to confer nationality – and from human rights instruments. These two elements constitute the main pillars of international migration law. Instruments of international migration law are spread across various branches of law, such as human rights law, humanitarian law, labour law, refugee law, consular law, trade law and maritime law.

Country of destination: The country that is a destination for migratory flows (regular or irregular).

Country of origin: The country that is a source of migratory flows (regular or irregular).

Country of transit: The country through which migratory flows (regular or irregular) move.

Data protection: The systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the collection, storage, use and disclosure of personal data.

Data subjects: Individuals that can be directly or indirectly identified by the reference to a specific factor or factors. Such factors may include a name, an identification number, material circumstances and physical, mental, cultural, and economic or social characteristics.

Discrimination: A failure to treat all persons equally where no objective and reasonable distinction can be found between those favoured and those not favoured. Discrimination is prohibited in respect of "race, sex, language or religion" (Art. *1(3), UN Charter, 1945)* or "of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status" (Art. *2, Universal Declaration of Human Rights, 1948).*

Exploitation: The act of taking advantage of something or someone, in particular the act of taking unjust advantage of another for one's own benefit (e.g. sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs).

Family unity (right to): A family's right to live together and, as a fundamental unit of a society, to receive respect, protection, assistance and support. This right is not limited to nationals living in their own State and is protected by international law

Forced migration: A migratory movement in which an element of coercion exists, including threats to life and livelihood, whether arising from natural or man-made causes (e.g. movements of refugees and internally displaced persons as well as people displaced by natural or environmental disasters, chemical or nuclear disasters, famine, or development projects).

Freedom of movement: A human right comprising three basic elements: freedom of movement within the territory of a country (Art. *13(1), Universal Declaration of Human Rights, 1948:* "Everyone has the right to freedom of movement and residence within the borders of each state."), the right to leave any country and the right to return to his or her own country (Art. *13(2), Universal Declaration of Human Rights, 1948:* "Everyone has the right to leave any country, including his own, and to return to his country."). *See also Art. 12, International Covenant on Civil and Political Rights.* Freedom of movement is also referred to in the context of freedom of movement arrangements between States at the regional level (e.g. European Union).

Genocide: "Any of the following acts committed with the intent to destroy, in whole or in part, a national, ethnic, racial or religious group, such as: killing members of the group; causing serious bodily or mental harm to members of the group; deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part; imposing measures intended to prevent births within the group; forcibly transferring children of the group to another group" (Art. *II, Convention on the Prevention and Punishment of the Crime of Genocide, 1948, Art. 6, Rome Statute of the International Criminal Court, 1998).*

Irregular migrant: A person who, owing to unauthorized entry, breach of a condition of entry, or the expiry of his or her visa, lacks legal status in a transit or host country.

The definition covers inter alia those persons who have entered a transit or host country lawfully but have stayed for a longer period than authorized or subsequently taken up unauthorized employment (also called clandestine/undocumented migrant or migrant in an irregular situation). The term "irregular" is preferable to "illegal" because the latter carries a criminal connotation and is seen as denying migrants' humanity.

Irregular migration: Movement that takes place outside the regulatory norms of the sending, transit and receiving countries. There is no clear or universally accepted definition of irregular migration. From the perspective of destination countries it is entry, stay or work in a country without the necessary authorization or documents required under immigration regulations. From the perspective of the sending country, the irregularity is for example seen in cases in which a person crosses an international boundary without a valid passport or travel document or does not fulfil the administrative requirements for leaving the country. There is, however, a tendency to restrict the use of the term "illegal migration" to cases of smuggling of migrants and trafficking in persons.

Migrant: At the international level, no universally accepted definition for "migrant" exists. The term migrant was usually understood to cover all cases where the decision to migrate was taken freely by the individual concerned for reasons of "personal convenience" and without intervention of an external compelling factor; it therefore applied to persons, and family members, moving to another country or region to better their material or social conditions and improve the prospect for themselves or their family. *Notwithstanding this definition, for the purpose of this thesis, the term migrant is referred to more broadly and includes all forms of movement whether free or*

coerced.

Migration: The movement of a person or a group of persons, either across an international border, or within a State. It is a population movement, encompassing any kind of movement of people, whatever its length, composition and causes; it includes migration of refugees, displaced persons, economic migrants, and persons moving for other purposes, including family reunification.

Migration management: A term used to encompass numerous governmental functions within a national system for the orderly and humane management for cross-border migration, particularly managing the entry and presence of foreigners within the borders of the State and the protection of refugees and others in need of protection. It refers to a planned approach to the development of policy, legislative and administrative responses to key migration issues.

Mixed flows / mixed migration: Complex migratory population movements that include refugees, asylum-seekers, economic migrants and other migrants, as opposed to migratory population movements that consist entirely of one category of migrants.

Personal data: All information that could be used to identify or harm data subjects.

Refugee: A person who, "owing to a well-founded fear of persecution for reasons of race, religion, nationality, membership of a particular social group or political opinions, is outside the country of his nationality and is unable or, owing to such fear, is unwilling to avail himself of the protection of that country. (Art. *1(A) (2), Convention relating to the Status of Refugees, Art. 1A(2), 1951 as modified by the 1967 Protocol).* In addition to the refugee definition in the *1951 Refugee Convention, Art. 1(2), 1969 Organization of African Unity (OAU) Convention* defines a refugee as

any person compelled to leave his or her country "owing to external aggression, occupation, foreign domination or events seriously disturbing public order in either part or the whole of his country or origin or nationality." Similarly, the *1984 Cartagena Declaration* states that refugees also include persons who flee their country "because their lives, security or freedom have been threatened by generalized violence, foreign aggression, internal conflicts, massive violations of human rights or other circumstances which have seriously disturbed public order."

Separated children: Children who are separated from both parents, or from their previous legal or customary primary caregiver, but not necessarily from other relatives. These may, therefore, include children accompanied by other family members. In the terms of the *Statement of Good Practice, 2004* in the Separated Children in Europe Programme (SCEP), separated children are "children under 18 years of age who are outside their country of origin and separated from both parents or their previous legal/customary primary caregiver." The SCEP uses the term "separated" rather than the term "unaccompanied" because "while some separated children appear to be "accompanied" when they arrive in Europe, the accompanying adults are not necessarily able or suitable to assume responsibility for their care." *See also child, minor, unaccompanied children*

Smuggled person/migrant: A migrant who is enabled, through providing financial or material benefit to another person, to gain illegal entry into a State of which he or she is not a national or a permanent resident.

Smuggling: "The procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State Party of which the person is not a national or a permanent resident" (Art. *3(a), UN Protocol Against the*

Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime, 2000). Smuggling, contrary to trafficking, does not require an element of exploitation, coercion, or violation of human rights.

Sovereignty: Sovereignty as a concept of international law has three major aspects: external, internal and territorial. The external aspect of sovereignty is the right of the State freely to determine its relations with other States or other entities without the restraint or control of another State. This aspect of sovereignty is also known as independence. The internal aspect of sovereignty is the State's exclusive right or competence to determine the character of its own institutions, to enact laws of its own choice and ensure their respect. The territorial aspect of sovereignty is the authority which a State exercises over all persons and things found on, under or above its territory. In the context of migration, this means the sovereign prerogative of a State to determine which non-nationals should be admitted to its territory subject to the limitations of the *non- refoulement* principle, human rights, and provisions in bilateral or regional agreements (e.g. free movement or integration agreements).

State: A political entity that has legal jurisdiction and effective control over a defined territory and the authority to make collective decisions for a permanent population; a monopoly on the legitimate use of force; and an internationally recognized government that interacts, or has the capacity to interact, in formal relations with other entities. The criteria of statehood for purposes of international law are commonly held to be possession of a permanent population, a defined territory, government and capacity to enter into international relations with other States (Art. *1, Montevideo Convention on the Rights and Duties of States, 1933).*

Terrorism: In the absence of a generally accepted definition under international law, "terrorism" can be defined as the intentional and systematic use of actions designed to provoke terror in the public as a means to certain ends. Terrorism can be the act of an individual or a group of individuals acting in their individual capacity or with the support of a State. It may also be the act of a State, whether against the population (human rights violations such as forced labour, deportation, genocide, etc.), or in the context of an international armed conflict against the civil population of the enemy State. Certain categories of terrorist acts are specifically mentioned by the international treaties annexed to the *International Convention for the Suppression of Financing of Terrorism, 1999.* This same Convention qualifies terrorism as "any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature and context, is to intimidate a population, or to compel a government or an international organization to do or abstain from doing an act."(Art. *2(1)(b)).*

Trafficker (human): An intermediary who is involved in the movement of person in order to obtain an economic or other profit by means of deception, physical or psychological coercion for the purpose of exploitation. The intent *ab initio* on the part of the trafficker is to exploit the person and gain profit or advantage from the exploitation.

Trafficking in persons: "The recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the

consent of a person having control over another person, for the purpose of exploitation" (Art. *3(a), UN Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the UN Convention against Transnational Organized Crime, 2000).* Trafficking in persons can take place within the borders of one State or may have a transnational character.

Unaccompanied minors / children: Persons under the age of majority in a country other than that of their nationality who are not accompanied by a parent, guardian, or other adult who by law or custom is responsible for them. Unaccompanied children present special challenges for border control officials, because detention and other practices applied to undocumented adult non-nationals may not be appropriate for children.

Undocumented migrant: A non-national who enters or stays in a country without the appropriate documentation. This includes, among others: a person (a) who has no legal documentation to enter a country but manages to enter clandestinely, (b) who enters or stays using fraudulent documentation, (c) who, after entering using legal documentation, has stayed beyond the time authorized or otherwise violated the terms of entry and remained without authorization.

Victim of human trafficking: Any natural person who is subject to trafficking in human beings.

Vulnerable group / migrants: Any group or sector of society that is at higher risk of being subjected to discriminatory practices, violence, natural or environmental disasters, or economic hardship, than other groups within the State; any group or sector of society (such as women, children, the elderly, persons with disabilities,

indigenous peoples or migrants) that is at higher risk in periods of conflict and crisis.

Xenophobia: At the international level, no universally accepted definition of xenophobia exists, though it can be described as attitudes, prejudices and behaviour that reject, exclude and often vilify persons, based on the perception that they are outsiders or foreigners to the community, society or national identity. There is a close link between racism and xenophobia, two terms that can be hard to differentiate from each other.

8.3 ANNEXURE B – ABBREVIATIONS

APEC - Asia-Pacific Economic Cooperation

APEC Privacy Framework - Asia-Pacific Economic Cooperation Privacy Framework (2005)

CEDAW - Convention on the Elimination of All Forms of Discrimination against Women (1979)

CoE Convention - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)

Constitution – Constitution of South Africa, 1996

CRC - Convention on the Rights of the Child (1989)

CRPD - Convention on the Rights of Persons with Disabilities (2006)

EU Directive - Directive 95/46/EC on the protection of personal data and on the free movement of such data (1995)

EU Charter - Charter on Fundamental Rights of the European Union (2000)

EDPS - European Data Protection Supervisor

Madrid Resolution –

HLD - High-level Dialogue on International Migration and Development

HIV/AIDS - Human Immunodeficiency virus/Acquired Immune Deficiency Syndrome

ICAO - The International Civil Aviation Organization

ICC - International Criminal Court

ICCPR - International Covenant on Civil and Political Rights (1966)

ICRC - International Committee for the Red Cross

ICTR - International Criminal Tribunal for Rwanda

ICESCR - International Covenant on Economic, Social and Cultural Rights (1966)

ICCPR - International Covenant on Civil and Political Rights

Interim Constitution - Constitution of the Republic of South Africa Act 200 of 1993

Interpol - International Criminal Police Organization

IOM - International Organization for Migration

Johannesburg Principles – Johannesburg Principles on National Security, Freedom of Expression and Access to Information

Madrid Resolution – International Standards on the Protection of Privacy and Data Protection (2009)

MIDSA Migration Dialogue for Southern Africa

MWA - International Convention on the Protection of All Migrant Workers and Members of their Families (1990)

OHCHR - United Nations Office of the High Commission for Human Rights

OECD - Organization for Economic Co-operation and Development

OECD Guidelines - Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)

PIA - Privacy Impact Assessment

PAIA - Promotion of Access to Information Act of 2000

Refugees Act - Refugees Act of 1998

SADC - Southern African Development Community

SAMP - Southern African Migration Project

UN – United Nations

UDHR - United Declaration of Human Rights (1948)

UNAIDS - Joint United Nations Programme on HIV and AIDS

UNDP - United Nations Development Program

UNESCO - United Nations Educational, Scientific and Cultural Organization

UN Guidelines - United Nations Guidelines for the Regulation of Computerized Personal Data Files (1990)

OCHA - United Nations Office for Coordination of Humanitarian Affairs

CHAPTER NINE

9. BIBLIOGRAPHY

BOOKS

Adepoju, Aderanti *Migration in Sub-Sahara Africa* (2008) Sweden, Nordiska Afrikaininstitutet

Aleinikof, Thomas Alexander and Chetail, Vincent *Migration and International Legal Norms* (2003) The Hague, T.M.C Asser

Amerasinghe, C F *Principles of the Institutional Law of International Organizations* (2005) Cambridge, Cambridge University Press.

Amnesty International (2006) *Living in the Shadows: A Premier on the Human Rights of Migrants* Amnesty International Publications, London <http://www.amnesty.ch/it/doc/temi/asilo-e-migrazione/fatti-e-cifre/en-savoir-plus>

Appave, Gervais; Laczko, Frank; et al *World Migration Report 2011: Communicating Effectively about Migration* (2011) Geneva, International Organization for Migration

Appave, Gervais; Laszko, Frank; et. al *World Migration Report 2013: Migrant Well-Being and Development* (2013) Geneva, International Organization for Migration

Bagshaw, Simon *Developing a Normative Framework for the Protection of Internally Displaced Persons* (2005) New York, Transnational Publishers

Brettel, Caroline and Hollifield, James F *Migration Theory: Talking Across the Disciplines* (2000) New York, Routledge

Bygrave, Lee A *Data Protection Law: Approaching its Rationale, Logic and Limits* (2002) Kluwer Law International, The Hague, London, New York.

Campbell, Dennis and Bàn, Chrysta *Legal Issues in the Global Information Society* (2005) New York, Ocean Publications

Campbell Public Affairs Institute *National Security and Open Government: Striking the Right Balance* (2003) New York, The Maxwell School of Syracuse University

Castles, Stephan and Miller Mark J *The Age of Migration: International Population Movements in the Modern World* (2003) New York, Guilford Press

Cate, Fred H *Privacy in the Information Age* (1997) Washington D.C., Brookings Institution Press

Cavallar, Georg *The Rights of Strangers: Theories of International Hospitality, the Global Community and Political Justice since Vitoria* (2002) Ashgate Publishing Limited

Cavoukian, Ann *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation* (1999) Toronto, Ontario, Information and Privacy Commissioner, Ontario

Cholewinski, Ryszard; Perruchoud, Richard; and MacDonald, Euan *International Migration Law: Developing Paradigms and Key Challenge* (2007) The Hague, T.M.C. Asser

Cholewinsky, Ryszard *Irregular Migrant: Access to Minimum Social Rights* (2005) Strasbourg, Council of European Publication

Cholewinski, Ryszard *Migrant Workers in International Human Rights Law: Their Protection in Countries of Employment* (1997), Oxford, Caledon Press

Cornell, Drucilla and Muvungu, Nyoko eds. *Ubuntu and Law: African Ideals and Post-Apartheid Jurisprudence* New York, Fordham University Press

Coats, William Sloan; et al *The Practitioner's Guide to Biometrics* (2007) Chicargo, American Bar Association Section of Science & Technology Law

Dauvergne, Catherine *Challenges to Sovereignty: Migration Laws in the 21st century* (2003) Geneva, United Nations High Commissioner for Human Rights

De Borchgrave, Arnaud *Cyber Threats and Information Security: Meeting the 21st Century Challenge* (2001) Washington D.C, CSIS Press

De Waal, Johan; Currie, Iain and Erasmus, Gerhard (2001) *The Bill of Rights Handbook* 4th Edition, Cape Town, Juta & Co Ltd

Dhillon, Gurpreet *Information Security Management: Global Challenges in the New Millennium* (2001) Hershey Pa, IDEA

DLA Piper *Data Protection Laws of the World (2013)* United Kingdom, DLA Piper *<http://www.thelawyer.com/Journals/2013/03/20/t/b/l/Data_Protection_Laws_of_the_World_2013-414865.pdf>*

Flaherty, David H *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States* (1989) Washington, University of North Carolina Press

Gamlen, Alan *People on the Move: Managing Migration in Today's Commonwealth – Action to Re-Connect Historical Links* (2010) London, Ramphal Centre

Ghosh, Bimal *Managing Migration: Time for a New International Regime?* (2000) England, NewYork, Oxford University Press

Goulboune S *Law and Migration* (1998) Nothampton, Edward Elgar Publishing

Gromovs, Juris *A Compendium of Legal Instruments of the European Union and the Council of Europe concerning the Use of Security Features and Biometric Identifiers in Passport and Travel Documents, Residence Permits and Short-term Visas* (2008) Minsk, European Commission, International Organization for Migration

Guild, Elspeth and Van Selm, Joanne *International Migration and Security: Opportunities and Challenges* (2005) London and New York, Routledge

Gutwirth, Serge and De Hert Paul; et al *Reinventing Data Protection?* (2009) The Netherlands, Springer, Science and Business Media B.V.

Harzig, Christian and Hoerder, Dirk *What is Migration History?* (2009) United Kingdom, Polity Press

Helton, A C *The Price of Indifference: Refugees and Humanitarian Action in the New Century* (2002) Oxford, United Kingdom, Oxford University Press

Holvast, Jan *The Global Encyclopaedia of Data Protection Regulation* (1999) The Hague, Kluwer

Holzgrefe, J L and Keohane, Robert *Humanitarian Interventionism: Ethical, Legal, and Political Dilemmas* (2003) New York, Cambridge University Press

Jackson, Robert H *Quasi-States: Sovereignty, International Relations and the Third World* (1990) Cambridge, Cambridge University Press

Opeskin, Brian; Perruchoud, Richard and Redpath-Cross, Jillyanne *Foundations of International Migration Law* (2012) Cambridge, Cambridge University Press

Pfleeger, Charles P *Security in Computing* (1997) Prentice Hall, New Jersey

Philpott, Daniel *Revolutions in Sovereignty: How Ideas Shaped Modern International Relations* (2001) Princeto, Princeton University Press

International Migration Programme *International Migration and Development: the ILO Perspective* (2007) Geneva, International Labour Organization

International Labour Organization *Protection of Worker's Personal Data* (1997) Geneva, International Labour Organization

Kindred, Hugh M et al *International Law: Chiefly as Interpreter and Applied in Canada* (5th Ed) (1993) Toronto, Emond Montgomery Publications Limited

Landau, Loren ed. *Exorcizing the Demons Within: Xenophobia, Violence and Statecraft in Contemporary South Africa* (2011) Johannesburg, Wits University Press

Martens, Ruzayda *IOM Data Protection Manual* (2011) Geneva, International Organization for Migration

Michael, James *Privacy and Human Rights: An International and Comparative Study, with special reference to Developments in Information Technology* (1994) England, The United Nations Educational, Scientific and Cultural Organization and Dartmouth Publishing Company Limited

Mills, Kurt *The New Sovereignty: The Changing Humanitarian Agenda in the Emerging Global Order* (1995) Notre Dame, University of Notre Dame

Mills, Kurt *Human Rights in the Emerging Global Order: A New Sovereignty?* (1998) London, MacMillan Press

Morris, L *Managing Migration: Civil Stratification and Migrant's Rights* (2002) London, Routledge

Moussalli, M *Transfrontier and Migration* (1983) Geneva, United Nations High Commissioner for Refugees

Murphy, Sean D *Humanitarian Intervention: The United Nations in an Evolving World Order* (1996) Philadelphia, University of Pennsylvania Press

Neethling, J; M Potgieter, J M and Visser P J *Neethling's Law of Personality* (2005) Durban, Butterworths

Newman, J *Protection through Participation: Young People affected by Forced Migration and Political Crises* (2005) United Kingdon, University of Oxford

Perruchoud, Richard and Redpath-Cross, Jillyanne eds. *International Migration Law: Glossary on Migration* 2nd Edition (2011) International Migration Law Series No.25, Geneva, International Organization for Migration

Perruchoud Richard, and Tömölovà, Katarina *Compendium of International Migration law instruments* (2007) The Hague, T.M.C. Asser

Plender, Richard *Basic Documents on International Migration Law* (2007) The Hague, Boston, Massachussets, M.Nijhoff.

Redpath, Jillyanne *Biometrics and International Migration* (2005) International Migration Law Series No. 5, Geneva, International Organization for Migration

Rehman, Javaid *International Human Rights Law* Second Edition (2010) London, Pearson Education Limited

Salazar, Luis *E-Commerce Best Practices: Online Privacy (Ten Keys to Latin American Data Privacy)* (2008) Standford Law School Press, Standford

Sassen, Saskia *Losing Control? Sovereignty in an Age of Globalization* (1996) New York, Columbia University Press

Sorensen, Birgitte Refslund and Vincent, Marc *Caught between Borders - Response Strategies of the Internally Displaced* (2001) London, Pluto Press in association with the Norwegian Refugee Council

Soysal, Yasemin *The Limits of Citizenship: Migrants and Post-National Membership in Europe* (1994) Chicago, University of Chicago Press

Stanley, Paul *The Law of Confidentiality: A Restatement* (2008) Oxford England, Hart Publishing

Swire Peter P and Litan, Robert E *None of Your Business: World Data Flows, Electronic Commerce and the European Privacy Directive* (1998) Washington D.C., Brookings Institution Press

United Nations *Human Rights in the Administration of Justice: A Manual on Human Rights for Judges, Prosecutors and Lawyers* (2003) New York and Geneva, United Nations Publications

United Nations Educational, Scientific and Cultural Organization *Human Rights: Major International Instruments, Status as of 31 May 2010* (2010), Paris, United Nations Educational, Scientific and Cultural Organization

United Nations High Commissioner for Refugees *Refugee Protection and Mixed Migration: The 10-Point Plan in Action* (2011) Geneva, United Nations High Commissioner for Refugees

United Nations Population Fund *Guidelines on Data Issues in Humanitarian Crisis Situations* (2010) New York, United Nations Population Fund

Waldo, James; Lin Herbert S and Millet Lynette I *Engaging Privacy and Information Technology in a Digital Age* Committee on Privacy in the Information Age, National Research Council, Washington, The National Academic Press

ARTICLES

Al Jazera 'US Promises not to Spy on the UN - UN Says it has been Assured the US Does Not and Will Not Spy on it, but Doesn't Comment on Whether it do so in the Past' 30 October 2013 <http://www.aljazeera.com/news/americas/2013/10/us-promises-not-spy-un-201310301934394770.html>

Andrijasevic, R and Walters, W 'The International Organization for Migration and the International Government of Borders" (2010) *Environment and Planning D: Society and Space* 28(6) 977 – 999

Annan, Kofi 'Two Concepts of Sovereignty,' Former UN Secretary-General, The Economist 352, 18 September 1999

Bailliet, C M 'Responsibilities of the Destination Country, *Forced Migration Review 25*, May 200

Bargiotas, Theodoros and Maganaris, Emmanuel 'Privacy Under Attack?: The Surveillance Phenomenon in Europe, the Legitimacy of Workplace Monitoring and the Greek Paradigm' (2006) *European Review of Public Law* London, Esperia Publications 18 (3) automne 2006: 1037-1082

Bechtold, Stefan 'Digital Rights Management in the United States and Europe' (2004) *American Journal of Comparative Law* 52 (2) Spring 2004: 323-382

Belair, Robert R and Coy, Kevin 'United States Privacy Law and Policy' (2010) in *The Future of Financial Privacy: Private Choices versus Political Rules*

Bernhardt, R 'Human Rights and the Individual in International Law" (1985) *Encyclopedia of Public International Law*, volume 8, Amsterdam, New York, North-Holland Publishing Company

Bignami, Francesca 'The Case of Tolerant Constitutional Patriotism: the Right to Privacy before the European Courts" (2008) *Cornell International Law Journal* 41(2) 2008: 211-249

Burchell, Jonathan 'The Legal Protection of Privacy in South Africa: A Transplantable Hybrid" in *Electronic Journal of Comparative Law*, vol 13:1, March 2009

Bygrave, Lee A 'An International Data Protection Stocktake at 2000: Part 1: Regulatory Trends' (2000) 6 *Privacy Law & Policy Reporter* 129

Bygrave, Lee A 'Privacy and Data Protection in an International Perspective' (2010) 56 *Scandinavian Studies in Law* 165

Bygrave, Lee A 'Privacy Protection in a Global Context-A Comparative Overview' Scandinavian Studies in Law, 2004, Vol. 47

Buthelezi, Mangosuthu, 'After Amnesty: The Future of Foreign Migrants in South Africa,' Keynote Address, 20 June 1997

Cholewinski, Ryszard 'Human Rights of Migrants: The Dawn of a New Era? ' (2010), in *Georgetown Immigration Law Journal* [Vol. 24:585), Georgetown University Law Centre

Congo Watch 'ICC - France Arrests Rwandan Rebel Leader Callixte Mbarushimana in Paris for War Crimes Committed in DR Congo's Kivu Province in 2009' 31 October 2010 <http://congowatch.blogspot.com/2010/10/icc-france-arrests-rwandan-rebel-leader.html?m=1>

Cowen, Zelman 'The Private Man' The Boyer Lectures, Australian Broadcasting Commission (1969) in Malcolm Crompton, Federal Privacy Commissioner *What is privacy?* Privacy and Security in the Information Age Conference, Melbourne, 16-17 August 2001 <http://www.docstoc.com/docs/2253786/What-is-privacy>

Currie, Iain 'The Protection of Personal Information Act and Its Impact on Freedom of Information' (2010) University of Witwatersrand, Johannesburg

Currie, Iain and Allan, Kate 'Enforcing Access to Information and Privacy Rights: Evaluating Proposals for an Information Protection Regulator for South Africa (2007) 23 *South African Journal on Human Rights (SAJHR)* 3: 527-586.

Currie, Iain and Klaaren, Jonathan 'Evaluating the Information Bills: A Briefing Paper on the Protection of Information Bill' prepared on behalf of the Centre of Memory at the Nelson Mandela Foundation, 17 June 2011.

Danziger, Richard; Martens, Jonathan and Guajardo, Mariela 'Human Trafficking and Migration Management (2009) in Friesendorf, Cornelius *Strategies against Human Trafficking: The Role of the Security Sector* Vienna, National Defence Academy and Austrian Ministry of Defence and Sports

David, Anne-Sophie 'Le nouvelles technologies au service del'aide humanitaire' French weekly Le Novel Economiste, 12 April 2012

De Kock, Emmie 'Data Protection in South Africa' December 2005 <http://www.dekock.co.za/data-protection-in-south-africa/>

De Villenfagne, Florence and Gayrel, Claire 'Data Protection at ICPO-Interpol: Assessments, Issues and Outlook' (2011) Belgium, Notre Dame de la Paix University

De Vos, Pierre (2012) 'Balancing Independence and Accountability: The Role of Chapter 9 Institutions in South Africa's constitutional democracy' in Chirwa, Danwood and Nijzink, Lia eds. *Accountable Government in Africa: Perspectives from Public Law and Political Studies* Cape Town, UCT Press

European Commission 'LIBE Committee Vote Backs New EU Data Protection Rules' European Commission Press Release, 22 October 2013 <http://europa.eu/rapid/press-release_IP-12-46_en.htm>

European Commission 'Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of their Data and to Cut Costs for

Businesses' European Commission Press Release, 25 January 2013 <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en>

Farer, Tom J 'How the International System Copes with Involuntary Migration: Norms, Institutions and State Practice' (1995) *Human Rights Quarterly* 17(1) February 1995: 72-100, Ohio, Urban Morgan Institute for Human Rights

February, Judith 'Border Controls May Cross Boundaries' The Cape Times, 29 July 2003
<http://www.queensu.ca/samp/sampresources/migrationdocuments/commentaries/2003/cross.htm>

The Freedom of Information website 'South African to create Information Regulator' 10 December 2012 <http://www.freedominfo.org/2012/12/south-africa-to-create-information-regulator/>

Higgins, Rosalyn 'Derogations under Human Rights Treaties' (1978) 48 British Yearbook of International Law 286

Hondius, Frits W 'A Decade of International Data Protection' (1983) *Netherlands International Law Review* 30(2) 1983: 103-128

Hornung, G 'Regulating Privacy Enhancing Technologies: Seizing the Opportunity of the Future European Data Protection Framework" (2013) 26 *The European Journal of Social Science Research* 181

International Organization for Migration 'IOM Publishes Data Protection Manual' IOM Press Briefing, Geneva, Switzerland, 27 January 2012 <http://www.iom.int/jahia/Jahia/media/press-briefing-notes/pbnEU/cache/offonce?entryId=31191>

Kajevic, Belhira 'Biometrics: A New Mean of Surveillance and Migration Control' Malmö University, 2 June 2006

Klaaren, Jonathan 'PAIA Through the Courts: Case Law and Important Developments in PAIA Litigation 2005-2009: A Paper Prepared for Democracy Advice Centre' (2010) Johannesburg, School of Law, University of Witwatersrand

Ki-moon, Ban 'Secretary-General's Message for 2012 on International Migrants Day18 December' <http://www.un.org/en/events/migrantsday/2012/sgmessage.shtml>

Knoppers, Bartha Maria (2000) 'Confidentiality of Health Information: International Comparative Approaches' in *Protecting Data Privacy in Health Services Research* National Academy of Sciences, Washington DC
< http://www.nap.edu/openbook.php?record_id=9952&page=173 > (accessed XX)

Kranenborg, Herke 'Access to Documents and Data Protection in the European Union: on the Public Nature of Personal Data' (2008) *Common Market Law Review* 45(4) August 2008: 1079-1114

Krutskikh, Andrei and Fedorov, Aleksandr 'International Information Security' (2000) *International Affairs (Moscow)* 46(2) 2000: 170-182

Kuner, Christopher 'An International Legal Framework for Data Protection: Issues and Prospects' *Computer Law & Security Review*, Vol.25, 307-317, 2009

Kuner, Christopher 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future' TILT Law & Technology Working Paper No. 016/2010, Tilburg Law School, 1 October 2010

Martens, Jonathan 'Moving Freely on the African Continent: The Experiences of ECOWAS and SADC with Free Movement Protocols in Ryszard Cholewinski, Perruchoud, Richard and MacDonald, Euan; eds. *International Migration Law: Developing Paradigms and Key Challenges* The Hague, TMC Accer

Massey, Douglas S 'International Migration at the Dawn of the Twenty-first Century: The role of the State' (1999) *Population and Development Review* 25(2) June 1999: 303-322, New York, The Population Council

'Media Statement on the Validation Workshop of SADC Harmonized Cyber Security Legal Framework' Gabrone, 27 February to 2 March 2012 <http://tis.sadc.int/files/1813/3232/7429/media_statement_cyber_security_version_2.pdf>

Mendel, Toby 'National Security vs. Openness: An Overview and Status Report on the Johannesburg Principles' in Campbell Public Affairs Institute (2003) *National Security and Open Government: Striking the Right Balance* Maxwell School of Citizenship and Public Affairs Syracuse University, New York

Meier, Patrick 'What is Crisis Mapping? An Update on the Field and Looking Ahead' iRevolution, 20 January 2011 <http://irevolution.net/2011/01/20/what-is-crisis-mapping/>

Meier, Patrick 'On Crowdsourcing, Crisis Mapping and Data Protection Standards' iRevolution, 5 February 2012 <http://irevolution.net/2012/02/05/iom-data-protection/>

Moeckli, Daniel 'Discriminatory Profiles: Law Enforcement After 9/11 and 7/7' (2005) *European Human Rights Law Review* No. 5 2005: 517-532

Ngandwe, Phazha Jimmy 'The Paradox of Migration and the Interests of the Atomistic Nation-States: The Southern African Perspective' (2013) *Potchefstroom Electronic Law Journal* Vol. 6 (1) 2013

Olinger, H N; Britz, J J; and Olivier, M S 'Western Privacy and Ubuntu - Influences in the forthcoming Data Privacy Bill' in *Ethics of New Information Technology - Proceedings of the Sixth International Conference of Computer Ethics: Philosophical*

Enquiry (CEPE2005), Brey, P., Grodzinsky, F., **and** Introna, L. (eds), Enschede, The Netherlands, 291-306, July 2005 <http://mo.co.za/open/ubuntu.pdf>

O'Neil, Robert M 'Privacy in the New Millennium: Virtual Trespass and Other Concepts' <http://www.abanet.org >

Open Rights Group 'Data Protection' <https://www.openrightsgroup.org/issues/data-protection>

Oriola Taiwo A 'Electronic Database Protection and the Limits of Copyright: What Options for Developing Countries' (2004) *Journal of World Intellectual Property* 7 (2) March 2004: 201-228

Oucho, John O (2007) 'Migration in Southern Africa: Migration Management Initiatives for SADC Member States' Institute for Security Studies (ISS) Paper 157 <http://www.iss.co.za/pgcontent.php?UID=29462>

Parliamentary Monitoring Group (PMG) 'Protection of Personal Information Bill: Departmental and Public representations' <http://www.pmg.org.za>

Parliamentary Monitoring Group (PMG) 'Protection of Personal Information Bill; Constitution 17th Amendment Bill: briefing; UN Security Council proclamations in respect of entities involved with terrorist activities' Recent Meetings for NCOP Security and Constitutional Development, 15 November 2012 <http://www.pmg.org.za/report/20121114-department-justice-and-constitutional-development-protection-state-in>

Pendleton, Wade 'Migration and Xenophobia in South Africa <http://www.iiz-dvv.de/index.php?article_id=725&clang=1>

Peston, Julia 'Obama Lifts a Ban on Entry into US by HIV Positive People' The New York Times, 30 October 2009 <http://www.nytimes.com/2009/10/31/us/politics/31travel.html>

Potakkis, Andreas 'Administration without Frontiers? European Migration Law: case study' (2009) *European Review of Public Law* 21(1) printemps 2009: 637-659, London Esperia Publications

Privacy International 'Privacy & Human Rights' 28 May 2007 <http://www.privacyinternational.org >

Prosser, William L (1960) 'Privacy' 48 *California Law Review* 383

Raab, Charles D 'From Balancing to Steering: New Directions for Data Protection' in Colin Bennet and Rebecca Grand, eds. *Visions of Privacy: Policy Choices in the Digital Age* (1999) Canada, University of Toronto Press

Reuters 'UN Worker Arrested Over Genocide' 13 April 2001 <http://tvnz.co.nz/view/page/425822/36358>

Roos, Anneliese 'Data Protection' in Van der Merwe, D; Roos, A; Pistorius, T; and Eiselen, S (2008) *Information & communication technology law* Durban, LexisNexis

Roos, Anneliese 'Data Protection for South Africa: Expectations Created by the Open Democracy Bill' in the Report of the Conference *The Constitutional Right to Access to Information* Pretoria, 2000

Roos, Anneliese 'The Law of Data (Privacy) Protection: A Comparative and Theoretical Study' (2009) UNISA Theses and Dissertations, Pretoria

Rooseveld, Eleanor 'Address to the United Nations General Assembly on the Adoption of the Universal Declaration of Human Right' Paris, 9 December 1984 in Rehman, Javaid (2010) *International Human Rights Law*

Saul, Heather 'Angela Merkel calls for Tighter Internet Data Protection Rules for Websites Registered in the UK Amid Allegations of US Surveillance' The Independent, 15 July 2013 <http://www.independent.co.uk/news/world/europe/angela-merkel-calls-for-tighter-internet-data-protection-rules-for-websites-registered-in-the-uk-amid-allegations-of-us-surveillance-8708975.html>

Schindlmayr, Thomas 'Sovereignty, Legal Regimes and International Migration' (2003) *International Migration* 41(2) 2003: 109-123, Geneva

Shaffer, Gregory 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Privacy Standards' (2000) *Yale Journal of International Law* 25(1) Winter 2000: 1-88, New Haven, Yale Law School

Stein, Ginny 'Rwanda – Questions of Murder' SBS Dateline, 21 February 2007 <http://www.sbs.com.au/dateline/story/transcript/id/130743/n/Rwanda-Questions-of-Murder>

Steinberg, Jonny 'Generous Judgment Instils Stigma' Business Day 24 April 2007 <http://www.businessday.co.za/articles/topstories.aspx?ID=BD4A445289>

Steiner 'Securing Human Rights: The First Half Century of the UNDH', Harvard Magazine, September – October 1998 in *International Human Rights Law*

Southern African Development Community (SADC) website <http://www.sadc.int/english/about-sadc/>

Sivakumaran, Sandesh 'The Rights of Migrant Workers One Year On: Transformation or Consolidation?' (2004) *Georgetown Journal of International Law* 36 (1) Fall 2004: 113-153, Washington D.C., Georgetown University Law Centre

Tan, Domingo R 'Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and European Union" (1999) *Loyola Angeles International and Comparative Law Journal* 21(4) August 1999: 661-684

Thomas ,Rebekah 'Biometrics, International Migration and Human Rights' *European Journal on Migration and Law* 7: 377-411, The Netherlands, Koninkilijke Brill NV

United Nations News Centre 'Interview with William Lacy Swing, 'Director General of the International Organization of Migration (IOM)' New York, 6 December 2011 <http://www.un.org/apps/news/newsmakers.asp?NewsID=46>

United Nations News Centre 'Number of international migrants rises above 232 million' UN News Centre, New York, 11 September 2013 <http://www.un.org/en/development/desa/news/population/number-of-international-migrants-rises.html>

United Nations Office of the High Commissioner for Human Rights 'Commission on Human Rights Resolution 1999/44'

<http://www.ohchr.org/EN/Issues/Migration/SRMigrants/Pages/SRMigrantsIndex.aspx>

United Nations Office of the High Commission for Human Rights 'Migration and Development: A Human Rights Approach' <http://www2.ohchr.org/english/bodies/cmw/docs/HLMigration/MigrationDevelopmentHC'spaper.pdf>

United Nations Office of the High Commissioner for Human Rights 'Migration and Human Rights' <http://www.ohchr.org/EN/Issues/Migration/Pages/MigrationAndHumanRightsIndex.aspx >

United Nations Office of the High Commissioner for Human Rights 'Landmark Statement on Protecting the Human Rights of Migrants' Global Migration Group, 30 September 2010 <http://www.ohchr.org/EN/NewsEvents/Pages/MigrantsInIrregularSituation.aspx>

Vassilaki, Irini 'The Constitutional Background of Privacy Protection within European Communities: Basic Principles for Interpretation and Implementation of the EC Data Protection Directive" (1994) *European Review of Public Law* London, Esperia Publications.

Van Wasshnova, Mathew R 'Data Protection Conflicts between the United States and the European Union in the War on Terror: Lessons Learned from the Existing System of Financial Information Exchange" (2008) *Case Western Reserve Journal of*

International Law 39 (3) 2007-2008 pgs 827-865 Ohio, Case Wesertn Reserve University School of Law

Wakan, Joanne M 'The Future of Online Privacy: A Proposal for International Legislation" (2003) *Loyola of Los Angeles International and Comparative Law Series* 26(1) Fall 2003: 151-179

Walden, I N and Savage, R N 'Data Protection and Privacy Laws: Should Organizations be Protected?' (1988) *International and Comparative Law Quarterly* 37 (2) April 1988: 337-347

Warren, Adam; et al 'Sources of Literature on Data Protection and Human Rights' (2001) (2) *The Journal of Information, Law and Technology*

Warren A et al 'Sources of Literature on Data Protection and Human Rights', 2001 (2) *The Journal of Information, Law and Technology* <http://elj.warwick.ac.uk/jilt/01-2/warren.html>

Williams, Christopher 'UN Issues Call for International Privacy Statement' The Register, 20 January 2010 <http://www.theregister.co.uk/2010/01/20/un_terror/>

REPORTS

Action Research on AIDS and Mobility, Global Alliance against Traffic in Women and International Women's Rights Action 'Report on Roundtable on using CEDAW to Protect the Rights of Women Migrant Workers and Trafficked Women in South and Southeast Asia' 6-9 May 2009, Kuala Lumpur, Malaysia <http://www.iwraw-ap.org/publications/doc/Roundtable_on_Migration_and_Trafficking_report.pdf >

Banisar, D and Davies, S (2000) 'Privacy and Human Rights: An International Survey of Privacy Laws and Developments' Electronic Privacy Information Centre, Washington <http://gilc.org/privacy/survey/intro.html>

Bustamante, Jorge A 'Human Rights of Migrants' *Report of the Special Rapporteur on the Human Rights of Migrants* (A/65/222) 3 August 2010 <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/474/88/PDF/N1047488.pdf?OpenElement>

Crépeau, François 'Preparing for the 2013 High-level Dialogue: A Human Rights Perspective' *Presentation by Professor François Crépeau Special Rapporteur on Human Rights of Migrants* Tenth Coordination Meeting on International Migration, New York, 9-10 February 2012 <http://www.un.org/esa/population/meetings/tenthcoord2012/SRM%20Final%20statement.pdf>

Crush, Jonathan; Williams, Vincent and Peberdy, Sally 'Migration in Southern African' A Paper Prepared for Policy Analysis and Research Programme of the Global Commission of International Migration, September 2005 <http://lastradainternational.org/?main=documentation&document=2276>

Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions 'A Comprehensive Approach on Personal Data Protection in the European Union' COM (2010) 609 final 9, Brussels, 4 November 2010 <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf>

Council of Europe Commissioner for Human Rights 'Protecting the Right to Privacy in the Fight against Terrorism' Strasbourg, CommDH/IssuePaper (2008) 3

Department of Homeland and Security 'Comments by the DHS Privacy Office and the Staff of the U.S. Federal Trade Commissioner on the Joint Proposal for International Standards on the Protection of Privacy with regard to the Processing of Personal Data' 10 August 2010

Directorate General of Human Rights and Legal Affairs 'Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data' (2005) in *Data Protection: Compilation of Council of Europe Texts*, Strasbourg, November 2010 <http://www.coe.int/t/dghl/standardsetting/dataprotection/dataprotcompli_en.pdf >

European Data Protection Supervisor 'Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on Migration' (2012/C 34/02), 9 July 2011, *Official Journal of the European Union* <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:034:0018:0026:EN:PDF>

European Commission Working Party on the Protection of Individuals with regard to the Processing of Personal Data 'Working Document: Transfers of Personal Data to Third Countries: Applying Articles 2 and 26 of the EU Data Protection Directive' (1998) WP 12
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf>

European Council, Communication from the Commissioner to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on Migration 'A Comprehensive Approach on Personal Data Protection in the European Union' COM (2010) 609 final, 9 November 2010

European Union Agency for Fundamental Human Rights 'Data Protection in the European Union: The Role of National Data Protection Authorities' 2010

Global Commission for International Migration 'Migrating in an Interconnected World: new directions for action, Geneva, 2005

Grant, Stefanie 'International Migration and Human Rights' A Paper Prepared for the Policy Analysis and Research Programme of the Global Commission on International Migration, September 2005

Hammarberg, Thomas 'Protecting the Right to Privacy in the Fight against Terrorism' Council of Europe Commissioner for Human Rights, Strasbourg, CommDH/IssuePaper (2008) 3 <https://wcd.coe.int/ViewDoc.jsp?id=1469161>

Homeland Security, Biometric Identification & Personal Detection Ethics (HIDE) 'Project Report on Policy Forum on Body Issues' <http://www.hideproject.org/downloads/deliverables/D4.2aPolicy_Forum_Report_on_Body_Issues.pdf>

Hosein, Gus and Nyst, Carly (2013) *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries* Privacy International, London

International Civil Aviation Organization 'Accelerating a Worldwide Approach to Biometric Identity Confirmation in MRTD's as the Key Token of Entitlement for Simplified Passenger Travel' Twelfth Report, Cairo, Egypt, 22 March 2004 to 2 April 2004 <http://www.icao.int/icao/en/atb/fal/fal12/docu- mentation/fal12ip007_en.pdf>

Inter-Action Protection Working Group 'Data Collection in Humanitarian Response: A Guide for incorporating Protection'<http://www.jointokyo.org/images/cms/Data_Collection_in_Humanitarian_Response.pdf>

Joint United Nations Programme on HIV/AIDS (UNAIDS) (2007) 'Guidelines on Protecting the Confidentiality and Security of HIV Information' Proceedings from a Workshop, 15-17 May 2006, Geneva

Knopjes, Fons 'Total Identity: Latest Developments ICAO' ID Management Centre <http://www.idmanagement-centre.com/>

Lehman, Julian 'Limits to Counter-Terrorism: Comparing Derogation from the International Covenant on Civil and Political Rights and the European Convention on Human Rights' <http://projects.essex.ac.uk/ehrr/V8N1/Lehmann.pdf >

Makhema, Mpho 'Social Protection for Refugees and Asylum Seekers in the Southern Africa Development Community (SADC)' (2009) Discussion Paper No. 0906, Social Protection and Labour, the World Bank < http://siteresources.worldbank.org/SOCIALPROTECTION/Resources/SP-Discussion-papers/Labor-Market-DP/0906.pdf>

Mokgoro J *Ubuntu and the Law in South Africa* Paper delivered at the first Colloquium Constitution and Law, Potchefstroom, 31 October 1997 <http://www.ajol.info/index.php/pelj/article/viewFile/43567/27090>

Olinger H N, Britz JJ and Olivier MS (2005) 'Western Privacy and Ubuntu - Influences in the Forthcoming Data Privacy Bill' <http://mo.co.za/open/ubuntu.pdf>

Oucha, John O 'Migration in Southern Africa: Migration Management Initiatives for SADC Member States' ISS Paper 157, 1 December 2007

Permanent Bureau (2010) 'Cross-border Data Flows and Protection of Privacy' Note submitted by the Permanent Bureau, Hague Conference on Private International Law <http://www.hcch.net/upload/wop/genaff2010pd13e.pdf>

Searle, Louise and Wynn-Pope, Phoebe 'Crisis Mapping, Humanitarian Principles and the application of Protection Standards: A Dialogue between Crisis Mappers and Operational Humanitarian Agencies' Meeting Record, 17 November 2011, Geneva <http://irevolution.files.wordpress.com/2012/02/world-vision-geneva-report.pdf>

Sehmer, Carolin 'Report of the Parallel Event Third Generation' Human Rights – Reflections on the Collective Dimension of Human Rights, Palais des Nations, 22 March 2007, Geneva <http://www.academia.edu/1140272/_Third_Generation_Human_Rights>

Scheinin, Martin 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while countering Terrorism, Ten Areas of Best Practices in Countering Terrorism' (A/HRC/16/51), 14 February 2010 at<http://www.ohchr.org/EN/Issues/Terrorism/Pages/Annual.aspx>

Simonovic, Ivan *Report of the United Nations High Commissioner for Human Rights to the ECOSOC General Segment 2010, Item 14(g)* Assistant Secretary-General for Human Rights, 22 July 2010 <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=10231&LangID=E>

South African Law Reform Commission 'Privacy and Data Protection' Discussion Paper 109: Project 124 (2005) Pretoria, South African Law Commission

South African Law Reform Commission 'Project 124: Privacy and Data Protection Report' (2009) Pretoria, South African Law Commission

United Nations 'Human Rights and Scientific and Technonogical Developments: Guidelines for the regulation of computerized personal data files' *Report of the Secretary-General* [A/44/606] 24 October 1989

United Nations 'Promotion and Protection of Human Rights, Including Ways and Means to Promote the Human Rights of Migrants' *Report of the Secretary-General*

(A/64/156), 21 July 2010 <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/459/22/PDF/N1045922.pdf?OpenElement>

United Nations Office of the High Commission for Human Rights: (OHCHR) 'Special Rapporteur on the Human Rights of Migrants' <http://www.ohchr.org/EN/Issues/Migration/SRMigrants/Pages/SRMigrantsIndex.aspx>

United Nations High Commissioner for Refugees 'Asylum Processes (Fair and Efficient Asylum Procedures), Global Consultations on International Protection' Third Track – Executive Committee Meetings, EC/GC/01/12, 31 May 2001.

United Nations High Commission for Refugees (UNHCR) 'Comments on the Source Country Information Systems (SCIS) of the International Centre for Migration Policy Development (ICMPD)' Department of International Protection (2003) Geneva, United Nations High Commission for Refugees

United Nations High Commission for Refugees (UNHCR) 'UNCHR Guidelines on Determining the Best Interests of the Child' (2008) Geneva, United Nations High Commission for Refugees

United Nations High Commission for Refugees (UNHCR) 'UNHCR Regional Conference on Refugee Protection and International Migration: Mixed Movements and Irregular Migration from East Africa and the Great Lakes to Southern African Dar es Salaam' Tanzania, 6-7 September 2011, Summary Report <http://www.unhcr.org/4d7f7ef711.pdf>

The Working Party on the Protection of Individuals with regard to the Protection of Personal Data, 'Opinion 3/2012 on Developments in Biometric Technologies' (WP193), 27 April 2012 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf>

LEGAL INSTRUMENTS AND SOFT LAW ON HUMAN RIGHTS AND DATA PROTECTION

African Charter on the Rights and Welfare of the Child Rights, 1999 (entered into force 29 November 1999) OAU Doc. CAB/LEG/24.9/49 (1990), available at: http://www.au.int/en/sites/default/files/Charter_En_African_Charter_on_the_Rights_and_Welfare_of_the_Child_AddisAbaba_July1990.pdf

African Charter on Human and People's Rights, 1981 (adopted 27 June 27 1981) OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), *entered into force* 21 October 1986, available at: http://www1.umn.edu/humanrts/instree/z1afchar.htm

Cairo Declaration on Human Rights in Islam Aug. 5, 1990, U.N. GAOR, World Conference on Human Rights, 4th Session, Agenda Item 5, U.N. Doc. A/CONF.157/PC/62/Add.18 (1993), available at: http://www1.umn.edu/humanrts/instree/cairodeclaration.html

American Convention on Human Rights, 1969 (entry into force 18 July 1978) [1114 U.N.T.S. 123], available at: http://www.oas.org/juridico/english/treaties/b-32.html

American Declaration of the Rights and Duties of Man, 1948 (adopted on 2 May 1948), available at: https://www.cidh.oas.org/Basicos/English/Basic2.American%20Declaration.htm

Asia-Pacific Economic Cooperation (APEC) Privacy Framework, 2005 (endorsed by the APEC economies), available at: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

Charter of Fundamental Rights of the European Union, 2000 [Official Journal C 364, 18/12/2000 P. 0001 – 0022], available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000X1218(01):EN:NOT

Commission Decision on Standard Contractual Clauses for the transfer of personal data to third countries under Directive 95/46/EC, 2001 of the European Parliament and of the Council (2010/87/EU), available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:039:0005:0018:EN:PDF

Convention on the Elimination of All Forms of Discrimination against Women, 1979 (entry into force 3 September 1981) [1249 U.N.T.S. 13], available at: http://www2.ohchr.org/english/law/cedaw.htm

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, Council of Europe (adopted on 28 January 1981) [ETS No. 108, Strasbourg, 28.1.1981], available at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) allowing the European Communities to accede, 1999, Council of Europe (adopted on 15 June 1999), available at: http://conventions.coe.int/Treaty/en/Treaties/Html/108-1.htm

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No. 108] regarding supervisory authorities and transborder data flows, 2001 [ETS No. 181, Strasbourg, 08.11.01], available at: http://conventions.coe.int/Treaty/EN/treaties/html/181.htm

Convention on the Rights of the Child, 1989 (entry into force 2 September 1990) [A/RES/44/25], available at: http://www2.ohchr.org/english/law/crc.htm

Committee on the Rights of the Child (CRC), General Comment No. 6 (2005) 'Treatment of Unaccompanied and Separated Children outside their country of origin',' 1 September 2005 [CRC/GC/2005/6], available at: http://www.unhchr.ch/tbs/doc.nsf/(symbol)/CRC.GC.2005.6.En?OpenDocument

Declaration on the Human Rights of Individuals who are Not Nationals in the Countries in which they live, (A/RES/40/144), 13 December 1985, available at: http://www.un.org/documents/ga/res/40/a40r144.htm

Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (adopted by the European Parliament and the Council on 24 October 1995) [Official Journal L 281, 23-11-1995, P. 0031 – 0050], available at: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

Directive 2006/24/EC on the Retention of Data generated or processed in connection with the provision publicly available electronic communications services or of public communications networks_and amending Directive 2002/58/EC (adopted by the European Parliament and the Council on 15 March 2006) [Official Journal L 105 , 13/04/2006 P. 0054 – 0063*], available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML*

European Convention for the Protection of Human Rights and Fundamental Freedoms, 1950 (entry into force 3 September 1953)) [78 U.N.T.S. 222], available at: http://conventions.coe.int/treaty/en/treaties/html/005.htm

Guidelines Concerning Computerized Personal Data Files, adopted by the UN General Assembly Resolution, 14 December 1990, United Nations [A/RES/45/95], available at: http://www.un.org/documents/ga/res/45/a45r095.htm

International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990 (entry into force 1 July 2003) [A/RES/45/158], available at: http://www2.ohchr.org/english/law/cmw.htm

International Covenant on Civil and Political Rights, 1966 (entry into force 23 March 1976) [99 U.N.T.S 171], available at: http://www2.ohchr.org/english/law/ccpr.htm

Organization for Economic Co-operation and Development (OECD) Guidelines

on the Protection of Privacy and Transborder Flows of Personal Data (adopted on 23 September 1980, available at:
http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html

Organization for Economic Co-operation and Development (OECD) Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (adopted on 25 July 2002), available at:
http://www.oecd.org/dataoecd/16/22/15582260.pdf

Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention Against Transnational Organized Crime, Annex II, 2000 [G.A. res. A/RES/55/25], (entry into force 25 December 2003), available at: http://www2.ohchr.org/english/law/protocoltraffic.htm

The Protection of Human Rights in the context of HIV and AIDS, C.H.R. res. 1997/33, ESCOR Supp. (No.3) at 115, U.N. Doc. E/CN.4/1997/33 (1997), available at: http://www1.umn.edu/humanrts/instree/HIV-AIDS.htm

The Protection of Human Rights in the Context of Human Immunodeficiency Virus (HIV) and Acquired Immune Deficiency Syndrome (AIDS), C.H.R. res. 1999/49, U.N. Doc. E/CN.4/RES/1999/49 (1999), available at: http://www1.umn.edu/humanrts/instree/aidsresolution.html

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community Institutions and Bodies and on the free movement of such data, European Parliament and Council [Official Journal L 008, 12/01/2001 P. 0001 – 0022], http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Reg_45-2001_EN.pdf/

The Right to Privacy in the Digital Age, 2013 [G.A. res. 68/167], available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

Universal Declaration of Human Rights, 1948 [G.A. res. 217A (III)], available at: http://www.un.org/en/documents/udhr/index.shtml

Universal Declaration on Bioethics and Human Rights, adopted by acclamation on 19 October 2005 by the 33rd session of the General Conference of United Nations Educational, Scientific and Cultural Organization (UNESCO), available at: <http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/bioethics-and-human-rights/>

United Nations Human Rights Committee (HRC), CCPR General Comment No 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988, http://www2.ohchr.org/english/bodies/hrc/comments.htm

United Nations Children's Fund (UNICEF), The Paris Principles: Principles and Guidelines on Children Associated With Armed Forces or Armed Groups, February 2007, available at: http://www.unicef.org/emerg/files/ParisPrinciples310107English.pdf

United Nations General Assembly 'Declaration of the High-Level Dialogue on International Migration and Development' (A/86/L.5) 1 October 2013

United Nations General Assembly 'Human Rights and Scientific and Technonogical Developments: Guidelines for the Regulation of Computerized Personal Data Files' Report of the Secretary-General [A/44/606] 24 October 1989

United Nations General Assembly 'Proclamation of 18 December as International Migrants Day' (A/RES/55/93) 28 February 2001

United Nations Human Rights Committee 'General Comment No. 16: *The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Article 17), 04/08/1988, CCPR General Comment No. 16 (General Comments)*' Office of the High Commissioner for Human Rights, available at: http://hria.equalit.ie/pdf/en/5/GC%2016%20-%20privacy%20EN.pdf

United Nations Human Rights Committee 'General Comment No 29: *States of Emergency (Article 4)*' U.N.Doc CCPR/C/21/Rev.1/Add.11 (2001) Office of the High Commissioner for Human Rights, available at: http://www1.umn.edu/humanrts/gencomm/hrc29.html

United Nations Human Rights Committee (HRC) General Comment No. 31 (2004) 'The Nature of the General Legal Obligation Imposed on States Parties' 26 May 2004 [CCPR/C/21/Rev.1/Add. 13] Office of the High Commissioner for Human Rights, available at: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G04/419/56/PDF/G0441956.pdf?OpenElement

International Conference of Data Protection and Privacy Commissioners

2009 The Madrid Resolution: International Standards on the Protection of Personal Data and Privacy, International Conference of Data Protection and Privacy Commissioners, 5 November 2009, available at: http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

2005a The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities ("Montreux Declaration"), 16 September 2005, available at: http://www.privacydataprotection.co.uk/documents/montreux_declaration.pdf

2005b Resolution on the Use of Biometrics in Passports, Identity Cards and Travel Documents, 27th International Conference of Data Protection and Privacy Commissioners, Montreux, 2005, available at: http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2005_Montreux/MONTREUX-EN4.pdf

2005c Resolution on the Use of Personal Data for Political Communication, Montreux, 2005, available at: http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2005_Montreux/MONTREUX-EN3.pdf

TABLE OF CASES

Europe

European Court of Human Rights, *Case of Leander v. Sweden* (Application no. 9248/81), Judgement, Strasboug, 26 March 1987 at 33. *Osman v The United Kingdom* (2000) 29 EHRR 245

European Court of Human Rights, *Case of Rotaru v. Romania* (Application no. 2834/95) Judgement, Strasbourg, 4 May 2000.

European Court of Human Rights (Chamber) Case of Z b. Finland (Application no. 22009/93), Judgment, Strasbourg, 25 February 1997

Osman v The United Kingdom (2000) 29 EHRR 245

S and Marper v United Kingdom, [2008] ECHR 1581

South Africa

Certification of the Constitution of the Republic of South Africa 1996 (10) BCLR 1253 (CC)

Bernstein v Bester NO 1996 (2) SA 751 (CC).

Fose v Minister of Safety and Security 1997 (3) SA 786 (CC)

Islamic Unity Convention and Others v Independent Broadcasting Authority and Others 2002 (4) SA 294 (CC)

Khumalo and Others v Holomisa 2002 (5) SA 401 (CC)

*Jansen van Vuuren and Another NNO v Kruger*1993 (4) SA 842 (A)

Laugh it Off Promotions CC v SAB International (Finance) BV t/a SabMark International (Freedom of Expression Institute as Amicus Curiae) 2006 (1) SA 144 (CC)

Mail and Guardian Media Limited and Others v Chipu N.O. and Others Case CCT 136/12 (2013) ZACC 32 ; 2013 (11) BCLR 1259 (CC)

Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC).

NM and Others v Smith and Others 2007 (5) SA 250 (CC).

National Media Ltd v Bogoshi 1998 (4) SA 1196 (SCA).

*Phillips and Another v Director of Public Prosecutions, Witwatersrand Local Division, and Others*2003 (3) SA 345 (CC).

S v Makwanyane and Another 1995 (6) BCLR 665 (CC)

S v Mamabolo (E TV and Others Intervening) 2001 (3) SA 409 (CC)

South African Broadcasting Corporation v National Director of Public Prosecutions and Others 2007 (2) BCLR 167 (CC)

South African National Defense Union v Minister of Defence and Another 1999 (4) SA 469 (CC)

United States of America

Arakawa v. Sakata 133 F.Supp.2d 1223 (D. Haw. 2001)

Denius v. Dunlap 209 F. 3d 944 (7th Cir. 2000)

Doe v. City of New York 15 F.3d 264 (2d Cir. 1994)

Doe v. Coughlin 697 F.Supp. 1234 (N.D.N.Y.1998)

Doe v. Town of Plymouth 825 F.Supp. 1102, 1107 (D.Mass. 1993)

Doe v. City of New York 15 F.3d 264 (2d Cir. 1994)

Estate of Behringer v. Medical Center 249 N.J.Super. 597 (1991)

Griswold v. Connecticut 381 U.S. 479 (1965)

Mason v. Regional Medical Center of Hopkins Cty, 121 F.R.D. 300 (W.Dist. Ky 1988)

*Multimedia WMAZ, Inc. v. Kuba*212 Ga. App. 707, 443 S.E.2d 491 (Ga. App. 1994)

Schaill v. Tippecanoe County Sch. Corp., 864 F.2d 1309, 1322 n.19 (7th Cir. 1989)

Whalen v Roe 429 U.S 589 (1977)

United States v Westinghouse Elec. Corp. 638 F.2d 570 (3rd Cir. 1980)

Urbaniak v. Newton 226 Cal.App.3d 1128 (1991)

TABLE OF STATUTES

South Africa

Electoral Act of 1998

Electronic Communications and Transactions Act of 2002

Equality Act of 2000

Promotion of Access to Information Act of 2000

Protection of Personal Information Act of 2013

Refugees Act of 1998

Refugees Amendment Act of 2011

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

Other countries

Morocco - Law No. 09-08 Relative to the Protection of Individuals with regards to their Personal Data of 2009

Senegal - Law No. 2008-12 of 2008 on the Protection of Personal Data

United Kingdom of Great Britain and Northern Ireland - Data Protection Act of 1998