University of Cape Town

School for Advanced Legal Studies – Faculty of Law

Department of Commercial Law

DATA PROTECTION: THE PROTECTION OF PERSONAL INFORMATION IN ZAMBIA

Name : **Lynn Munyebo Bwampu Syanziba**

Student Number: **SYNLYN001**

Supervisor: **Steven Ferguson**

Co Supervisor: **Prof. Alan Rycroft**

Submission date: **September 2011**

Research dissertation presented for the approval of Senate in fulfilment of part of the requirements for the degree of Master of Laws in Commercial Law in approved courses and minor dissertation. The other part of the requirements for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of Master of Laws in Commercial Law dissertations, including those relating to length and plagiarism, as contained in the rules of the University, and that this dissertation conforms to those regulations.

ACKNOWLEDGEMENTS

My sincere gratitude goes to my loving husband Moonga Habanji, my family and friends for the support rendered towards the completion this work. My gratitude also goes to my employer and sponsor, the Ministry of Lands (Government of the Republic of Zambia) for the financial support. I am also indebted to my supervisor Steve Ferguson for the invaluable advice. To the Almighty God, I thank you for strength you gave me to complete this work in spite of the loss of my sister, you are a wonder working God, to you is the glory!

DEDICATION

To my late young sister Wendy Lweendo Syanziba who died on 10th September 2011. May your soul rest in eternal peace!

TABLE OF CONTENTS

CHAPTER 1

THESIS OVERVIEW

1.1 Introduction

The recognition of the increase in potential threats to personal privacy[1] in the world today accounts for the world's grappling with ways of ensuring that personal privacy is upheld through various means. The perceived threat is being fuelled by 'pervasive deployment of computer systems together with the exponential increase in data collection, data processing, storage and exchange.'[2] One author aptly described the world we live in today as,

> *...a world of international data transmissions. Digitalization of information, combined with continuous and dazzling technological developments that has increased the flow and application of data. Information sharing now takes place on an international scale and involves a tremendous amount of data relating to individuals. Among the critical regulatory challenges raised by such international information flows is how to protect individual privacy.*[3]

The challenge for a developing nation like Zambia, which has only recently begun to feel the tremors caused by technology in the protection of personal information, is to adopt a data protection regime that will actively protect the interests of Zambians in the most effective way.

The adoption of such data protection should be undertaken the same time as taking into consideration the fact that 'privacy law has had difficulty keeping pace with advances in technology and that it's changing nature provides a continuous challenge to the law regulating its use.'[4] A growing nation is therefore left with the challenge of coming up with a data protection regime that will not only ensure adequate safeguards in the protection of personal information of its citizens but will

---

[1] Jonathan Burchel 'The Legal Protection of privacy in South Africa: A transplantable Hybrid' (2009) 13.1 Electronic journal of comparative Law at1 available at http://www.ejcl.org.

[2] Olinger et al 'Western privacy and/or ubuntu? 'Some critical comments on the influences in the forth coming privacy bill in South Africa' (2007) 39 *International information and Library review* 31 at 32.

[3] Paul M Schwartz 'European data protection law and restrictions on international data flows' (1995) 80 Iowa at 471

[4] Rachael Zimmerman 'The way the "Cookies" crumble: Internet privacy and data protection in the 21st century' (2000-200) 4 *NYUJ &Pub. Poly at* 439.

also provide an environment that encourages e commerce and the flow of transborder data.

1.2 Historical Background

The concept of privacy until recent times has been alien to those African societies which value communal interests above the interests of self. In traditional African culture[5] privacy is synonymous with secrecy and as such has not been a value worth promoting since the culture was premised on the philosophy of communitarianism which places emphasis on the good of the community[6] as a whole. Western cultures on the other hand are primarily based on the political philosophy of libertarianism, a philosophy which places emphasis on the rights of an individual in order to protect or empower them.[7] Here the rights of the individual are more important than the rights of the community as a whole.

Thus although the concept of privacy traces its origins from Western culture, it is important to note that even in Western culture the concept of privacy only began to take root in the industrialisation age around the 18th century. As a result of the converging of people in Britain and the industrialising countries of Europe in search of jobs away from their rural communities, insecurities and tensions were created as people from different backgrounds with different customs where thrown together. These people had to find a way of amicably living together. In order to do this, boundaries of personal space had to be defined and this process later found expression in the right to privacy.[8] Thus this social need, which became crystallized in the right to privacy, did not grow insistent until the great age of industrial expansion when dramatic advances in transportation and communication threatened to annihilate time and space.[9] This implies that the need for the right to privacy was triggered to a large extent by industrial and technological advancements then.

The right to privacy is today acknowledged as a human right. Depending on the ideological, cultural or social background, the right of people to privacy is defined and accepted either as a fundamental human right or seen as a human right

---

[5] In this context culture refers to values, norms and customs of a particular society.
[6] OlingerN Hanno et al (note 2) at 32.
[7] Ibid.
[8] Henderson Harry *Privacy in the Information age* revised ed. (2006) an imprint of InfoBase publishing at 6.
[9] Nizer Louise 'The right to privacy- half a centuries developments' (1940- 1944) 39 Mich L Rev. 526 at 526.

protected by law. The world today is grappling with a particular component of privacy, termed 'information privacy' in the United States of America, or 'data protection' in the countries making up the European Union.

The first serious international discussion on data protection law took place in 1968 at the United Nations International Conference on Human Rights. The state of Hesse in Germany was the first to enact a data protection statute in 1970[10], as the memory of the 'November 9, 1938 "night of the broken glass" in which the Nazi secrete police and Hitler youth swarm over Jewish businesses and homes terrorizing the helpless individuals all over the country remained only too vivid for Germans. They remembered also that extensive government records of citizens' personal information were used to identify and single out those the ruling Nazi Party deemed 'undesirable.'[11] The Germans and a generation of citizens of those European countries involved in World War ll would forever remember the atrocities in part caused by the abuse of personal information.

After the United Nations general conference flag off, data protection, privacy, and 'fair information practices' attracted widespread international and domestic debate and generated legislative action, particularly in Europe.[12] The region has been a pioneer in this crusade not so much now because of fear of the past but as a matter of principle.

In a nutshell, the trend towards data protection or data privacy has been influenced by three major rationale; firstly the desire on the part of certain countries to remedy past injustices caused or allowed by inadequate protection of personal information; Secondly, promotion of economic activity within a highly globalised market place and thirdly, and perhaps the most important one, the desire to ensure that a nation's laws are in tandem with the European Union model that is becoming so prevalent,[13] and has become the standard, so as to promote uniformity in this area.

---

[10] Fred H Cate 'The European Union data protection directive: Information privacy and the public interest' (1994-1995) 80 Iowa L Rev 431 at 431.
[11] Ryan Moshell '... And then there was one: the outlook for the self regulatory United States amidst a global trend towards comprehensive data protection' (2004-2005) *37 Tex Tech L Rev* 357 at 358.
[12] Cate (note 10) at 431.
[13] Moshell (note 11) at 364.

1.3 Objectives of the Study

The rationale of this thesis is to create a basis of the enactment of comprehensive data protection legislation in Zambia that meets the international standards with regards to data protection. It is hoped that this would lead to effective participation of Zambia in Electronic Commerce (e- commerce) and would afford its citizens a chance to exercise control over their personal information amidst increased threats to protection of this information. In order to achieve this, the thesis aims to achieve four specific objectives:

1. To determine the current status of the law relating to data protection in Zambia;
2. To look at the downside of technology as it relates to the protection of personal information
3. To make a comparative analysis of data protection models obtaining in the European Union (the standard) and the United States of America the two opposing extremes in data protection and reflect on and draw lessons from there.
4. To determine the best course of action for Zambia in terms of data protection by way of recommendations and to suggest a way forward.

1.4 Significance and value of the findings of this study

It is hoped that this study will highlight the weaknesses relating to data protection in Zambia. The recommendations coming out of this study, if implemented, will foster reform of the law on data protection by suggesting the enactment of a comprehensive data protection legislation taking into considerations the requisite international standards relating to data protection and drawing lessons from other jurisdictions in order for Zambia to effectively participate in the global economy. The results of this study will ultimately make a significant contribution in the area of cross border data transfer among handlers of information in Zambia and provide citizens a tool with which to exercise control over their personal information.

1.5 The Concept of privacy: definitions

Privacy is not a straightforward concept and therefore is very difficult to define.[14] The concept means different things to different people. It is certainly not a single interest 'but rather has several dimensions.'[15] Samuel Warren and Louise Brandeis, the major common law contributors to the right to privacy in the United States defined privacy 'as the right to be let alone.'[16] This definition has been said to be too broad and vague[17] and therefore risks being too over inclusive.

Another author attempting to define privacy in the context the United States has argued that 'when people today decry lack of privacy, what they want...is mainly quite different from seclusion: they want more power to conceal information about them that others may use to their disadvantage.'[18] These definitions suggest that while American have been known to say they want privacy, what they are interested in is conditions of solitude, the need for repose or the seclusion needed for intimacy rather than the control of facts and information about themselves.[19] On the other hand the European Union privacy is intimately tied with dignity and honour, and is therefore perceived to the core of humanity in general.

Though difficult to define, privacy can generally be divided into four categories[20];

> *1.information privacy, which concerns the control and handling of personal data; 2. bodily privacy which involves the integrity of an individual's body against violations; 3, communication privacy which covers various forms of communications; and 4 territorial privacy which limits or places boundaries against intrusion into a persons specific space or area.*[21]

The variations in the definitional accounts of privacy can be attributed to three factors '(a) variation in the use and the denotation meanings of 'privacy' (b) variation in purpose for which definition of 'privacy' is undertaken; and (c)

---

[14] 'Personal Privacy in the Information age : comparison of the internet Data Protection regulation in the United States and the European Union'(1999) 21 Loy L. A. Int'l &Comp L .J. at 663.
[15] Ibid.
[16] Samuel D Warren and Louise Brandeis 'The Right to privacy' (1890) 4 Harv. L Rev at 193 available at Web.ebscohost.com.
[17] Daniel J Solove 'I've Got Nothing To Hide" and other Misunderstandings of privacy' (2007) San Diego L.Rev 745 2007 at755.
[18] Solove note 17 citing Richard A Posner 'The economics of Justice' at 751.
[19] Anita Allen 'Privacy as a data control: Conceptual practical and Moral Limits of the paradigm' at 867.
[20] Zimmerman (note 4) at 441.
[21] Personal Privacy in the Information age' (note14) at 664.

variation in the approaches taken to the task of the definition.'[22] In other words the definition of privacy will depend on the denominator, either use, purpose or the task involved in defining the term.

This paper is centred around information privacy which was aptly defined by Alan Westin as the 'claim of individuals, groups, or institutions to determine for themselves how and when and to what extent information about them is to be communicated to others'[23] this definition is based on privacy as a data control paradigm which seeks to place the individual at the centre of decision making about personal information use.[24] The data control paradigm in the data protection definition has been said to encompass three notions;

> *...[F]irstly privacy means control or (right of control) over the use of personal information, secondly, the notion that the expression "right to privacy" means the claim to control the use of personal data or information and thirdly, the notion that the central aim to privacy regulation should be promoting individuals control (or right of control) over personal data or information.*[25]

Personal information is the core ingredient of data protection laws and information privacy legislation. Although the European Union uses the term 'data protection' whereas the United States of America favours the term 'information privacy' the two terms are in fact used interchangeably throughout this discourse. A fairly broad consensus exists that data protection laws are aimed primarily at safeguarding the 'privacy' of the individual against potentially intrusive data processing practices.[26]

Information has been said to be personal if it can be 'understood to refer to or relate to a person' and the data must facilitate identification of such a person.'[27] The Electronic Communication Transactions Act (ECT)[28] of Zambia provides a broad

---

[22] Allen (note 19) at 684.
[23] Alan F Westin 'Social and Political dimensions of Privacy' Westin 'Privacy and Freedom 1967' (2003) 59 no.2 journal of social sciences at 3 available at www.privacysummersymposium.com.
[24] Allen citing Schwartz (note 19) at 817.
[25] Allen (note 19) at 863.
[26] Lee A Bygrave *Data Protection Law, Approaching its rationale, logic and limits*, Information Law Series (2002) at 8.
[27] ibid at 42.
[28] ECT Act no 21 of 2009 s2.

definition for Personal information. The definition is a standard definition which traces its origin from the Organisation for Economic Cooperation and Development (OECD) guidelines and it is also verbatim with the definition found in the ECT Act of South Africa.

The definition will be taken from the Act in its entirety as it is the basis of this thesis and it will be referred to throughout the discussion. According to the ECT Act personal information is defined as;

> *...as information about an identifiable individual, including but not limited to — (a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual; (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved; (c) any identifying number, symbol, or other particular assigned o the individual; (d) the address, fingerprints or blood type of the individual; (e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual; (f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the individual; (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name*

> *itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years.*[29]

The underlying thread in the above definition of personal information is identifiability that is, 'the potential of the information to enable identification of a person'[30] as one will find that all the attributes of the components of the definition will in one way or another lead to the identification of an person.

Related to the term 'personal information' is the data subject. This refers to any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored. In other words the data subject is the owner of the personal information. Also related to the data subject is the 'data controller' this is the person or institution that is responsible for collating, collecting or processing of personal information.

These are the major concepts that require definition proceeding to the core of this thesis. Other important concepts associated with the issue of privacy and protection of personal information will be defined as they are introduced.

1.6 Structure

This thesis comprises of six chapters. The first chapter provides a general introduction and overview of the thesis. The main purpose of this chapter, besides introducing the research problem, is to provide an historical overview and, the aims and significance of the research in terms of contribution to data protection in Zambia.

Chapter two examines the Zambian approach to data protection by considering the various pieces of legislation that play a role in that country in data protection, as well as the common law protection of privacy, with a view to creating a foundation for assessing the adequacy of the data protection legislation in the country.

Chapter three broadly addresses the global trends in data protection in the world today. The core principles that underlie data protection legislation are

---

[29]ECT Act no. 21 of 2009 s 2.
[30] Bygrave (note 26) at 42.

considered as well as the three major international instruments that have shaped the global data protection landscape. The Chapter concludes by considering the major models of data protection. These include the comprehensive, sectoral, self- regulation and the technology enhancing data protection models. The aim of this chapter is to provide a foundation for current data protection legislation.

Chapter four considers the role of technology in the processing of personal information. It examines the advantages and challenges of technology in this context, in particular since the advent of the internet. This process leads to the conclusion that technological advancement has in fact blurred both the right to and guarantee of privacy. The chapter also looks at technological advancements as driver of commerce at and the increased risk of the violation of the right to privacy that has accompanied this.

Chapter five considers European Union data protection approaches and models in terms of being the standard for data protection globally as well as the approach of the United States to data protection, seeing the two as being at the extremes of models of data protection. The safe harbour compromise is also considered based on the outcomes of protracted negotiations between the two parties. Useful lessons in the area of data protection are drawn from the case of South Africa as the country, is in the process of enacting a piece of legislation dedicated to the protection of personal information that is in line with international standard.

Chapter six concludes the study with the argument that the data protection regime in Zambia is both fragmented and inadequate in terms of meeting the international standards which dictate data protection legislation. It ends with making recommendations for a comprehensive data protection system of legislation, one which will afford the citizens of Zambia the opportunity to exercise control over their personal information amidst technological advancement, and one which will also ultimately encourage e-commerce and transborder data flows.

CHAPTER II

ZAMBIAN APPROACH TO DATA PROTECTION THE LEGISLATIVE AND INSTITUTIONAL FRAMEWORK

2. 1 Introduction

The sources of law in Zambia are the Constitution of Zambia which is the supreme law of the land, delegated legislation, English acts extended to Zambia by the English Law (Extension of Application) Act Cap 11 of the Laws of Zambia, English Common law and doctrines of Equity by virtue of the British Acts Extension of applications Act Cap 10 of the Laws of Zambia, Customary law of Zambia, and the public and international law that has been incorporated into domestic law.

The protection of privacy can be derived from a variety of sources, the major contributories being the Constitution of Zambia and Common law in form of the law of tort, as well as various pieces of legislation. It must be noted that policies relating to different sectors may also act as a modes for the protection of privacy in the country.

2.2 Constitutional provision for the protection of Personal Information

Data protection is not directly provided for under the constitution of Zambia. It is however protected under the right to privacy which falls within the Bill of Rights in Zambia. The Bill of Rights comprises the fundamental freedoms and rights of individuals. Article 11(d) of the Constitution[31] provides for the protection of privacy of an individual as regards his home and other property, and from deprivation of the property without compensation.

Further, article 17[32] of the Constitution provides for the protection of privacy regarding an individual's home or property unless he/she gives his/her consent to invasion of his/her privacy or to deprivation of his/her property. Since the protection of personal information is a component of the individual's right to privacy one can always invoke the constitutional right to privacy in the event of violation of the said right.

---

[31] Chapter 1 of the laws of Zambia.
[32] Ibid.

The 'entrenchment of fundamental rights,' which includes the right to privacy, strengthens the protection function of these rights and affords them a higher status in the sense that they are applicable to all law and are binding on the state as well as on natural and juristic persons.'[33] However, like every right contained in the Bill of Rights, the right to privacy is not absolute therefore capable of limitation. It must be balanced with other rights entrenched in the Constitution.[34] An individual may only enjoy their right to privacy as long as it does not violate another person's rights.

2.3 Legislative provisions for protection of Personal Information in Zambia

Personal data in Zambia is protected through the right to privacy. The said data is protected through a number of legislative provisions relating to different sectors constituting 'the right to privacy'. The following are some of these pieces of legislation:

a) The Electronic Transactions Act no 21 of 2009

b) The Information and Communications Technologies no 15 of 2009

c) The Banking and Financial services Act

d) The Postal Services Act no. 22 of 2009

The aims, functions and scope of each of these pieces of legislation will be outlined in detail.

2.3.1 The Electronic Communications and Transactions Act of 2009

The aim of the Act is to provide a safe and secure environment in the country when electronic communications are used in order to provide legal certainty in this relatively new area of the law. The ECT Act is the most comprehensive piece of legislation relating to the protection of personal information in Zambia. The whole of Chapter VII of the ECT Act is dedicated to the protection of personal information. The chapter provides principles that must be employed when dealing electronically with the collection of personal information:

---

[33] Denys Reitz 'Protection of personal information' (2009) Seminar paper on protection of personal information available at http://www.dp/org/za accessed on 27/07/11

[34] Chapter I Article 17 ss 2 a- d

1. *Consent; the first principle requires the data controller to have express written consent from the data subject before collecting, collation, processing or disclosure of personal information except where the law provides an exception. Here the data subject should be accorded a chance to either accept or refuse to give their personal information depending on their reasons.*
2. *Lawful purpose Limitation, this principle implies that the data controller should only collect personal information for a lawful purpose as such personal information should not be collected for an unlawful purpose, for example for purposes of committing a crime.*
3. *Specific purpose limitation, here the data controller is obliged to disclose in writing to the data subject the specific purpose for which the personal information is being collected. This implies that before the data subject provides their personal information they should be clear as to the purpose of their personal information being collected so that they can make an informed decision.*
4. *Use Limitation principle, this principle obliges the data controller not to use the personal information collected for any purpose other than that for which the information was originally intended without the express permission from the data subject, except where the law provides an exception.*
5. *Where the personal information was kept for a period longer than one year, the data controller is required to keep a record of the information and also the original purpose for which the information was collected.*
6. *The data controller is not at liberty to divulge personal information in their custody to a third party unless the law permits them to do so or the data controller has secured permission in writing from the data subject.*
7. *Where the personal information was kept for a period longer than a year by a data controller, a data controller should keep a record of all the third parties who accessed that personal information. The data controller is obliged to indicate the date and the specific purpose for which the information was accessed.*

8. *The data controller is obliged to destroy or destroy personal information collected under the act unless where the law provides otherwise.*
9. *The data controller may use any personal information for statistical purposes and may trade with that data as long as it does not link to a specific person. For example the data controller may provide information such as there were a thousand people who purchased so many things in the previous year or for a certain number of months depending on what their compilation indicates.*[35]

These principles unfortunately limit the amount of information that can be protected as they relate only to information that is collected through electronic means.[36] Subscription to the principles is voluntary,[37] which is perhaps one of it shortfalls as people can easily contract out of it and continue to conduct transactions as if the legislation did not exist, there being no incentive for subscription. However once the parties choose to contract into the ECT Act, subscription to the principles is not optional.[38] The biggest challenge to the Act is that of enforcement of the Act as it does not provide an enforcement mechanism other than the option of suing the defaulting party under the law for breach of contract.

Further, chapter eleven of the ECT Act[39] provides for the interception of communication. This has serious implications for the privacy of an individual in terms of communication privacy. The act provides for the protection of privacy in so far as it prohibits attempts and intercepting communications through the use of electronic or mechanical devices.[40] However the act provides exceptions under which communications may be intercepted.[41] The ECT Act also provides for the protection of privacy in so far as it restricts access and disclosure of stored communication, except under circumstances as provided and stipulated by the law.[42] These provisions are very important as they play a significant role of protecting people's privacy in this age of advanced technologies where the use of email is very prevalent.

---

[35] ECT Act no. 21 of 2009
[36] ECT Act no 21 of 2009 s.41(1)
[37] ECT Act no 21 of 2009 s 41(2)
[38] ECT Act no 21 of 2009 s 41(3)
[39] No 21 of 2009
[40] ECT 21 of 2009 s 64
[41] No 21 of 2009 s 66
[42] ECT Act no 21 of 2009 s.80

The ECT Act prohibits 'spam' the transmission of any unsolicited electronic messages for either commercial or illegal activities[43] The act does not use the word bulk as such one can imply that even one unsolicited electronic message may amount to spam as such implying an opt in regime of protection against spam. In this case the law has been blatantly ignored as many cell phone owners continue to receive electronic messages from different sources mostly commercial in nature indiscriminately.

2.3.2 The Information and Communications Technologies no 15 of 2009

This piece of legislation provides for the establishment of the Zambia Information and Communications Technology Authority (ZICTA) which is intended to provide for the regulation of information and communication technology and to facilitate access to technology in the country. This regulatory authority, among other functions and responsibilities serves to promote the interests of consumers, purchasers and other users of information with respect to accessibility, quality amongst a variety of other services.

The regulator has the mandate for specifying the minimum standards and the quality of service that will be provided to the consumers in this case data. The act also empowers the regulator to provide guidelines for processing complaints where necessary. Section 68 alludes particularly to the protection of consumer information which may include personal information and as such this section of the act also contributes to a large extent to the protection of personal information.

2.3.3 The Banking and Financial Services Act CAP 387

The Banking and Financial Services Act regulates the conduct of banking and financial institutions in order to provide safe guards for both customers and investors in the industry. Because of the fiduciary nature of relations between the banking institutions and the client, the Act makes provision for all confidential information provided by clients in the course of the bank's providing a service to a client shall be

[43] ECT Act 21 of 2009 s 105.

confidential, thereby providing protection for this category of personal information. The Act further provides instances where the information may be divulged, for instance, with the consent of the customer or by court order or where the law provides for the information to be divulged.[44] Confidential information refers to information that is not in the public domain.

According to the Act confidential information includes; the nature, amount or purpose made by or to the person, the recipient of the payment by the person, assets, liabilities, financial liabilities or the financial condition of a person or any matter that the customer has disclosed in confidence to the finance service provider. Based on this piece of legislation the banking and financial sector has contributed to the protection of personal information Zambia. Coupled with the ECT act a measure of protection is provided for Zambians. This act provides protection of personal information to the extent that a financial institution may not divulge personal details of the client in the course of transactions to a third party without a clients consent.

2.3.4 The Postal Services Act no. 22 of 2009

The Act regulates the postal and courier services in the country and the operation of postal banking services. The Act also has a role to play in protection of information privacy in the handling of mail which includes or contains personal information. Section 82[45] makes it unlawful to communicate, divulge or access mail without authority, and as such it makes it an offence to do so. In Section 92, the operation of the postal service in terms of electronic mail is bound by an obligation to abide by the Electronic Transactions Act of 2009.

The above mentioned pieces are some of the important pieces of legislation that protect privacy in Zambia. This was intended to show that protection of personal information is provided through a number of legislations, the ECT act at the centre.

---

[44] Banking and Financial services Act Chapter 387 s 50
[45] Postal Services Act no. 22 of 2009.

2.4 Privacy and the Common law in Zambia

Zambian law is based on the English common law. There is currently no free standing right or overriding tort of privacy in common law. In the absence of a tort of privacy, the equitable remedy of confidence and a variety of torts, linked to intentional infliction of harm to a person, are used.[46] For instance '[t]he privacy of a home has been protected by torts such as trespass and nuisance; the privacy of the body was protected by torts such as assault, battery, intentional infliction and nervous shock and negligence.'[47] These protections hinge on the protection of bodily privacy as well as on intrusion of a private property or premises. The application of this multiplicity of different remedies has been accompanied by frequent and emphatic assertions that no general rights of privacy exist in English law.[48]

Under the common law, the infringement of the right to privacy was enforced through the law of tort (delict) as a consequence of a duty of care. The person whose right had been infringed had to prove that the conduct at issue was wrongful, intentional and that it caused injury to him or her. In some instances there was a need to apply the 'but' for test in order to apply the principle of causation implying that if a particular event had not occurred then probably the injury or harm may not have occurred.

It has been stated that the common law torts are inadequate to protect privacy or indeed the right to information privacy. The common law protection of privacy shows 'limitations of an approach that relies upon adequate existing remedies to protect privacy'[49] by trying to fit protection of privacy into the straight jacket of the English common law tort. Common law torts of trespass imply physical entry upon a property or physical contact in the case of assault or battery. These torts are inadequate in protection of personal information as violations in this area may not necessarily entail physical entry upon a property or physical contact. For instance in the case of hacking a computer because there is no physical entry onto a computer system as a virus may be used. In a nutshell the common law is not adequate for

---

[46] Basil Markesinisi et al 'Concerns and Ideas about the Developing English law of tort (how knowledge of Foreign law may help' (2004) 52 1 American journal of comparative law 133 at 137.
[47]Roos A 'Personal Data protection in New Zealand: Lessons for South Africa' (2008) 4.
[48] In the case of Wainwright v Home office (2001) EWCA Civ 2081, the law lords refused to recognise a separate and free standing tort of privacy, relying upon the progressive extension of the existing breach of confidence action to protect privacy interests.
[49]Markesinisi et al (note 46) at 138.

purposes of protection of personal information as such must be complimented with legislative provisions.

2.5 Legal Precedent

The Zambian courts of law essentially recognise the constitutional right to privacy. Although no case has been reported where an individual was particularly challenging a violation of the right to privacy per se, some cases like Patel Vs the Attorney General,[50] Zinka Vs Attorney General,[51] and Edith Nawakwi vs Attorney General,[52] have in their obiter dictum given recognition to fundamental rights and freedoms including the right to privacy.

It must however be noted that in the area of data protection there has been no case to date. This could be attributed to that fact that the ECT Act is a relatively a new piece of legislation and as such not yet tested. Perhaps the closest the Act has come to being tested is through a widely reported case in Zambia where ZICTA, the regulator of information and communications technology, was ordered by a judge to divulge the name of the author of an article that was deemed contemptuous in that it was analyzing evidence in a case before court. A ZICTA official was therefore summoned and testified that the paper that had published the article was hosted in Houston, United States of America by one Anthony Mwamba using a computer registered to William.[53]

2.6 The Constitution Review Commission

The then republican president of Zambia His Excellency Dr Patrick Levy Mwanawasa, in exercise of his power under the Inquiries Act,[54] appointed a commission that was chaired by Wila D Mungamba for purposes of reviewing the constitution of Zambia. The terms of reference of the Commission included, among others, to recommend a constitution that should exalt and effectively entrench and

---

[50] Z R (1968) 99
[51] ZR (1990-1992) 73 HC
[52] ZR 112 (1990-1992) 112 HC
[53] Judge Finds Mwamba with a case to Answer dated 29th Dec.2010 available at www.zambianwatchdog.com accessed on 30th August 2011
[54] No 41 of the laws of Zambia

promote the protection of fundamental human rights that would stand the test of time.[55]

During the proceedings of the commission a lot of issues where laboured at length, including the Bill of Rights, which took precedence over a number of other matters. In spite of the constitution review commission being in the unique position of being able to propose an express constitutional provision of data protection, the issue of data protection was not even tabled, indicating the general feeling in the country. Perhaps this feeling was one of indifference, or a feeling that Zambia has an adequate data protection regime, or even that the protection of personal information is not a subject fit for constitutional protection.

[55] Mungomba Constitution Review Commission final report available at www.ncczambia.org accessed on 27/04/11

CHAPTER III

GLOBAL TRENDS TOWARDS THE PROTECTION OF PERSONAL INFORMATION

3.1 Introduction

The emergence of data protection laws is quite recent. The trend globally is the enactment of comprehensive data protection legislation, which has been spurred by the Pan European law, the EU directive in particular.[56] Business analysts point to the push to promote electronic commerce as the key driver toward comprehensive laws. It has been argued that electronic commerce demands particular standards and effective protection of data and this requires the confidence of consumers before e-commerce can fulfil its promise as the engine of the new economy.[57] The list of countries enacting data protection legislation is growing. These countries are developing privacy laws as packages of laws intended to facilitate electronic commerce by harmonizing and synchronising data protection laws.

The data protection landscape has been generally influenced or shaped by three international instruments: (1) the OECD guidelines governing the protection of privacy and transborder flows of personal information adopted by the OECD[58] in 1980, (2) the 1981 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data at the Strasbourg Convention and would be binding to its signatories. Finally the cherry on the top came in 1995 in the form of a directive on the protection of personal information and free movement of such data. These data protection instruments have been said to contain a relatively clear distillation of data protection principles which should be present in most domestic data protection laws and they have been serving as influential models for

---

[56] William J Long and Marc P Quek 'Personal data privacy protection in an age of globalisation : the US-EU Safe Harbour compromise' (2002) Journal of European public policy 225 at 331.

[57] Ibid.

[58] The Organisation for Economic Cooperation and Development (OECD) is a group of 29 member countries, including the United States, Canada, Japan and most European countries. According to a statement on its Web site, it is an organisation that, most importantly, provides governments a setting in which to discuss, develop and perfect economic and social policy. The member states compare experiences; seek answers to common problems and work to coordinate domestic and international policies that will create a level playing field in the global arena.

national and international data protection initiatives.[59] The following section will describe in detail the core data protection principles which emerged from the initiatives described above.

3.2 Introduction on the Core Principles of Data protection Laws

There are basically eight data protection principles that are common to most data protection legislation. These form the backbone of data legislation today and have come to be embodied in most international and domestic data protection legislation. Similar words in the various instruments in which they are embodied may not be used but the spirit of the principles is fundamentally the same. The said principles trace their origins from the above mentioned data protection instruments;

3.2.1 Principle 1 Fair and Lawful processing

The Fair and Lawful Processing principle is considered to be the primary data protection principle. It is considered a primary principle because it 'embraces and generates the other core principles of data protection laws... the twin criteria of fairness and lawfulness are manifest in all the core principles.'[60] This principle requires data processors, in striving to achieve their data processing goals, to take into account the interests and reasonable expectations of the data subjects[61] and for this to be achieved requires that personal information be collected directly from the data subject.

The data collected must only be processed with the consent of the data subject except where the information is being collected for purposes of complying with the law, either a public law duty or contractual obligation. Further, personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3.2.2 Principle 2: Minimality

The second core principle of data protection laws is that the amount of personal data collected should be limited to what it is intended to achieve and the purpose[s]for which the data was gathered and further processed The principle should in fact be

---

[59] Bygrave (note 26) at 30.
[60] Ibid at 58.
[61] Ibid.

summed up in terms of 'minimality', 'proportionality', and 'frugility'.[62] This principle requires that Personal information must not be excessive in relation to the purpose for which it was intended. Here the data controller is obligated to collect only the information that is sufficient for the requisite purpose.

3.2.3 Principle 3: Purpose Specification

This data protection principle implies that personal information may only be collected for a specific, explicitly defined and legitimate purpose, and not subsequently processed for any other reason other than that for which it was originally intended. This principle has been said to form a cluster of three principles,: '1. The purpose for which data are collected shall be defined, 2. The purpose shall be lawful and legitimate; and 3.the purpose for which the data is further processed shall not be incompatible with the purpose for which the data was first collected.'[63] In other words, the purpose for which the information is collected need not only be specific but also legitimate and should not be used for any other purpose than that for which it was originally intended.

3.2.4 Principle 4: Information quality

This principle seeks to ensure that the personal data being kept by the data controller should be valid with respect to what it intends to describe, or it must be relevant and complete with respect to its intended purpose. In other words the data processor or controller should ensure that the information is complete, not misleading, up to date and accurate. The principle of information quality is especially important in that decisions may be made that might have far reaching consequences for the data subject and be to his or her detriment.

3.2.5 Principle 5: Data Subject Participation and Control

This principle requires that persons be able to participate in, and have a measure of influence over, the processing of data on them by other individuals or institutions.[64] A data subject is entitled to the particulars of his or her personal information held by any institution or person, as well as to the identity of any person who has had access to his or her personal information. The data subject is also entitled to request the

[62] Bygrave (note 26) at 60.
[63] Ibid at 61.
[64] Ibid at 63.

correction of any information held by another party. This ultimately implies that the data controller has to collect the personal information directly from the data subject and that the intended purpose will have to be disclosed by the data controller in order for the individual to attain some level of control over his or her personal information.

3.2.6 Principle 6: Disclosure Limitation

This principle restricts disclosure of personal information to a third party except with consent of the data subject or indeed as a requirement of the law. This principle is normally incorporated in the principles of fair and lawful processing and of purpose specification as outlined in 3.2.3.

3.2.7 Principle 7: Information Security

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data. The data controller must take care to implement technical and organisational measures to secure the integrity of personal information, and to guard against the risk of loss, damage or destruction of personal information. Here the data controller could employ certain technologies, for instance encryption or software to prevent the abuse of the information.

3.2.8 Principle 8 Sensitivity

This principle holds that certain types of information categorized as sensitive for data subjects should be subject to more stringent controls beyond the controls over general personal information, for instance, information relating to religious beliefs, sexual preferences as well as medical records. Sensitive information can easily be used to discriminate and stigmatise against data subjects because of their preferences or medical records. This goes against the spirit of data protection.

In conclusion, data protection core principles are embodied in many data protection instruments.[65] In fact they could be referred to as the threads that hold the present day data protection regimes together. The said principles trace their roots to the three major tributaries of data protection instruments which have greatly influenced the current trend in data protection. In the following section the three major international instruments that have shaped the data protection principles will be described:

[65] For example, ECT Act of Zambia and the South African ECT act.

3.3 OECD Guidelines

In 1980 the OECD, in its quest to create a common standard in the area of protection of privacy and Trans border flows of personal data, issued what was then the most comprehensive data protection and privacy statements. In its guidelines the OECD set forth those basic principles for data protection which have been very influential in the development of data protection models in the world today.[66] The OECD embodies the following principles and criteria: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, and accountability. While these OECD Guidelines were not intended to be binding, they have been and remain highly influential and form the threshold that is used by the European Union for purposes of attaining degrees of adequate data protection. The OECD guidelines have also formed the backbone of many data protection regimes in the world today.

3.4 The Convention for the Protection of individuals with regard to Automatic Processing of Personal data (CoE)

The convention is a treaty dealing specifically with data protection in the European Community member states. The convention came into force in 1981 with the intention of providing standard and consistent principles for the protection of personal information. The main aim of the Convention was to 'secure in the territory of each party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular the right to privacy, with regard to automatic processing of personal data.'[67] The convention was not successful because not self executing and it did not create a body to enforce its implementation. It simply obliged the member states to incorporate its principles into their data protection legislation. The Convention, like the OECD guidelines, embodies some data protection principles such as data quality[68] and data security.[69] The Convention proceeds to provide for special categories of data[70] in article 6. This category includes information relating to a persons's sex, race, beliefs, health and sexual life..

---

[66] Bygrave (note 26) at 32.
[67] Convention no. 108/1981 Art. 1.
[68] Convention no. 108/1981 Art 5.
[69] Convention no 108/1981 Art. 7.
[70] Convention no 108/1981 Art. 6.

3.5 EU Directive

While the OECD guidelines and the CoE have a special place in the protection of personal information, the challenge lay in the fact that these guidelines were not legally binding. Thus in the area of data protection the greatest achievement was the adoption of the European Union Directive[71] herein after referred to as the Directive. The said Directive is the most complex and comprehensive of the three instruments that have been influential in the data protection landscape as described above.

The Directive will be discussed in greater detail under the European Union approach to data protection. For the present suffice it to say that, in addition to data protection, the Directive provides principles relating to data quality.[72] This requires that personal information be processed fairly and lawfully, collected for a specific and legitimate purpose, not be excessive in relation to the purposes for which it was originally collected, and must be accurate and kept in a form that permits identification of data subjects within a period that is not unnecessarily long. The Directive also makes provision for the individual or data subject to give his consent or in accordance with the exceptions provided.[73] In other words the Directive embodies all the data protection principles in the OECD guidelines as well as those in the Coe but goes beyond the provisions in the above two documents in that it provides an enforcement mechanism for data protection.

It must be born in mind that, although the Directive provides the minimum threshold for data protection, it does not place a ceiling on data protection standards. Unlike the other two instruments, the Directive is legally binding in terms of enforcement by the member states. Failure to enact legislation among the member states carries the possibility of opening erring members to a law suit for non compliance with the directive. The Directive also exerts an influence[74] on non European Union member states or third countries in that it requires them to provide adequate data protection safeguards or risk blockage by the European Union of the flow of personal information from the European Union to that country.

---

[71] Directive 95/46 of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[72]Dir 95/46/EC Art 6.
[73]Dir 95/46/EC Art 7.
[74]Dir 95/46/EC Art 25.

The extent of incorporation of data protection principles in a data regulatory regime will normally determine the type of model that a particular country or union or federation chooses to adopt.

3.6 Introduction to Models for Privacy Protection

There are basically four models for data protection generally used by countries. These models are chosen by a country or group of countries depending on what ideologies underpin a particular type of social, cultural, or political or data regulatory regime. In other words the choice of a particular model for data protection would depend on the historical background or ideological orientation of a particular people or nation.

3.6.1 Comprehensive Laws Model

The Comprehensive Laws model is comprised of 'omnibus legislation establishing broad standards seeking to provide the best legal protection governing the collection, use and dissemination of personal information by both the public and the private sectors.'[75] This model considers data protection to be a fundamental and inalienable human right. It is the preferred model for most countries adopting data protection laws because it is currently favoured by Europe in order to ensure compliance with its new data protection regime.

The Comprehensive Data Protection model presupposes an oversight enforcement agency. In terms of this model adherence to data protection legislation is mandatory and failure to comply with this legislation could result in an investigation being launched by the commissioner, ombudsman, or registrar for purposes of ensuring compliance. The said official is usually responsible for education and international liaison in data protection and data transfer.

This model has been criticised for being rigid and characterised as favouring bureaucratic procedures, therefore carrying with it the threat of lagging behind in terms of regulation when dealing with technology. However a variation of this model, which has been described as the 'co-regulatory' model, is emerging and being adopted in Australia and Canada.[76] Using this model, industry develops enforceable

---

[75]Long and Quek (note 56) at 330.

[76] David Banisar 'Privacy and Data protection around the world' available at http://www.pcpd.org.hk.

standards for protection of privacy which are then enforced by the industry and supervised by a privacy agency.

3.6.2 Sectorial Laws Model

This model does not involve general laws instead it enacts privacy laws targeting only those specific industries shown to be a threat to privacy.[77] In comparison with the comprehensive model, the legislation under the sectoral model is more narrowly defined in that it regulates specific sectors of government, business, or civic activity. The United States of America is one of the proponents of this model, having avoided comprehensive data protection rules in favour of specific sectoral laws governing, for example, video rental records and financial privacy. The sectoral approach has been said to be a more flexible approach to data protection as it allows different sectors to regulate themselves.

Although effective when complementing and detailing comprehensive law, if used on its own this model tends to result in excessive time lag[78] as it requires that new legislation be introduced with each new technology, irrespective of the need for the law to be technology-neutral. Thus with this model, protection measures frequently lag behind technological developments. Unlike the Comprehensive data protection model, enforcement is achieved through a range of mechanisms since there is a lack of an oversight agency.

3.6.3 Industry Self Regulation Model

Data protection can also be achieved, at least in theory, through various forms of self regulation, in terms of which companies and industry bodies establish codes of practice. Self regulation allows companies and industry bodies a freer rein to establish their own codes of practice. Advocates for this model of regulation argue that this model is less costly and more flexible in terms of meeting individual preferences and needs for privacy.[79] However, the record of these efforts has been disappointing, with little evidence that the aims of the codes are regularly or consistently fulfilled, for instance '[i]n regard to online privacy protection, despite numerous online businesses establishing their own private guidelines, the

---

[77] Moshel (note 11) citing 'Privacy International and Human rights 2003' at 367.
[78] Ibid at 367.
[79] Long and Quek (note 56) at 330.

government, internet users and many online businesses agree that the industry efforts fall "far short" of what is needed to protect users'[80]Adequacy and enforcement are the major disadvantages of these approaches. Industry codes in many countries have tended to provide only weak protection systems and have not been able to effectively enforce these. At best self regulation has been said to be a public relations tool.[81] The promotion of the model is currently the policy of the governments of the United States, Japan, and Singapore.

It has been argued that, in order, 'to be effective, self regulation should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress).'[82] In self regulated privacy protection systems and policies, it is suggested that mechanisms for compliance will include making acceptance of compliance with a code of fair information practices a condition of membership in an industry or association: external audits to verify compliance and certification of entities that have complied with the code at issue.[83] This model is closely related to the sectoral approach model in that each of them addresses specific areas and do not provide comprehensive data legislation.

3.6.4 Privacy Enhancing Technologies Model

This model is usually used to compliment the other three models of data protection. The model employs the use of commercially available privacy enhancing technologies such as encryption and digital cash to protect personal information. The platform for privacy preferences (P3P), developed by the Wide Web Consortium, may also be used as it 'allows the internet users to decide the level of disclosure of personal information they are willing to accept when they are using the internet.

---

[80] Personal Privacy in the information age (note 14) at 674.
[81] Joel R Redeinberg 'E-Commerce and Transatlantic privacy' (2001-2002) 38 Hous L. Rev 726.
[82]Jordan M Blanke '"Safe Harbour" and the European Unions Directive on Data Protection' (2000-2001) Vol. 11 Alb. L J Sci. & Tech. 57 also available http://heinonline.org accessed on 20th April 2011 at 721.
[83]Ibid at 722.

Reservations however remain about the security, trustworthiness of these systems.'[84] These technologies have been said to place the protection of personal information in the hands of an individual and as such the degrees of security may vary depending on the kind of program being used. These programmes include encryption, anonymous remailers, proxy servers, and digital cash or smart cards.

3.7 Conclusion

The above mentioned principles and data protection models are at the centre of most modern data protection legislation. These principles have been employed for purposes of determining the adequacy of data protection in various privacy regimes based on the European Union directive, which appears to be yardstick according to which adequacy of data protection is measured and determined. In terms of data protection models, different jurisdictions may favour different models. There is no rule that is cast in stone with regards to the model that a particular country should follow. In fact ideally one should be able to borrow from all the models of data protection.

[84]Long and Quek (note 56) at330.

CHAPTER IV

DATA PROTECTION, TECHNOLOGY AND E-COMMERCE TOWARDS TRANS-BORDER DATA FLOWS

4.1 Introduction

Record keeping dates back to the beginning of civilisation before even the paper mediums were used. With the advent of the paper medium came the challenge of storage and space as they took up a lot of space unlike like the electronic files of today. This further implied that only a limited amount of information could be kept at a given time and for a limited period of time. The longer the information or the data was kept, the more expensive it was to maintain a registry. Maintenance of a large filing system also translated into a mammoth challenge relating to retrieval which could only be accomplished by experts, this was time-consuming and inefficient. Further processing of the information stored was an even bigger challenge which meant physically accessing and cross referencing the information stored.

With the dawn of the information age, many of these physical limitations have changed tremendously. The use of advanced technologies mean that there are virtually no physical limitations in terms of the volume of information that may be stored, the length of time the information may be stored, or the cost of this storage space. Access is at the click of the mouse and so is cross referencing of the files. Search engines satellites, sensor networks, security agencies and marketers are processing terabytes of information per day.[85]

This large amount of processed information includes information about ourselves – the information users – which is derived from the web of today's technology-based infrastructure systems and communication networks. These have greatly increased in number and sophistication over recent time, resulting in a greater capacity to collect, share and process information. These technologies include closed circuit television networks (CCTV), radio frequency identifiers (RFIDs), mobile phones, the internet, minute microphones, satellite imagery, and telecommunications

---

[85] Jeroem Van Den Hoven *Information Technology and Moral Philosophy: Information Technology, Privacy and the Protection of Personal information* (2008) at 301.

systems and social sites like face book. The data being collected covers our movements, characteristics, finances, health etc. These data can in turn, and not always with our knowledge, be profiled and used to structure and influence the personal decision-making framework, often with far reaching consequences. This scenario is captured by Kafka's '[t]he Trial'(1925) which depicts a bureaucracy with inscrutable purposes that uses peoples information to make important decisions about them yet denies the people the ability to participate in how their information is used.'[86] The problems captured by Kafka are problems of information processing, the storage, use and analysis of data rather than the information collection.

4.2 Information Technology and Privacy

The 'information age' characterised by the introduction of computers into every sphere of life threatens individual privacy in ways that were unimaginable a decade ago.[87] With the increasing rate of advancement of technologies and their application in the world, the right to privacy is becoming more complex and difficult to protect. The tremendous and the continuous growth of our information and communications systems coupled with the internet web 2.0, the multiplication of digital identities, the convergence of all infrastructures and finally the ubiquitous computing[88] are the major cause of the new challenges related to the right to information privacy.

The internet has made a unique contribution to the gathering and processing of personal information in this era hence it being 'the most novel and striking aspect of our age [is] the exponential growth of information, not only available but often thrust upon us whether we want it or not.'[89]

4.3 Privacy and the Internet

The gathering of information in our age has exploded through the use of the internet, it continues at an astronomical rate. The prominence of the Internet with respect to data protection is evidenced by a tendency by some countries passing data protection laws that target electronic data collection and transactions without addressing paper

---

[86] Franz Kafka *The Trial* Translated by David Wyllie (1925) at 50-58 available at free book at planet ebook.com accessed on 20/07/11.

[87] David Filvaroff 'Privacy, computers and the Commercial dissemination of personal information' (1986-1987) 65 Tex L Rev at 1395 available at http://heinonline.org accessed on 20/07/11.

[88] Yves Poullet 'Data Protection Legislation: What is at Stake for our society and Democracy' (2009) 25 Computer at 211.

[89] Phaedon John Kozyris *Regulating the Internet Abuses: Invasion of privacy* (2007) at 1.

based practices.[90] The internet not only allows for faster collection of personal information it also has the ability to collect very detailed information beyond the name, address, sex, date of birth or internet browsing habits. This detailed information is primarily collected when individuals are increasingly asked to provide personal information in order to gain access to a particular internet-based service or application.[91] The internet can also collect information on people's perceptions, attitudes, preferences and even moods through the use of interactive tools such as reel com's mood matcher which helps people find movies depending on their moods.[92]

Paradoxically, as the internet can function to collect specific information on a user, it can also provide anonymity. For example, one would purchase a particular item from the internet believing no one has access to the record or it may be a case of contributing to a discourse anonymously due to the fear of an oppressive government. Thus irrespective of one's nationality, location one can enter anonymously or pseudonymously at will into this virtual space since identity, location and source can easily be disguised with the use of cheap or free technologies.[93] In this miraculous new world, in this endless space there is virtually free entry worldwide[94] at minimum cost and no need for a passport or a visa. The interplay of the main functions of the internet which include the enhanced disclosure of information, access and the freedom of anonymity are central to the issue of privacy in the information age.

4.4 The Challenges of the Internet

Along with the immense social benefits that the internet brings comes vast potential for privacy violations.[95] The use of the internet is a long way from what was envisaged by commentators using the metaphor of Gorge Orwell's '1984' to describe the problems that have been created by the collection and use of personal information.[96] Against the background of technological advancements depicting 'big

---

[90]Moshell (note 11) at 361.
[91] Edgar A whitley 'International Privacy, Consent, the "Control" of personal data' (2009) EnCoRe publication also available at http://www.encore-project.infor accessed on 27 August 2011 at 2.
[92] Kalinda Basho 'Licensing of our personal information; is it a solution to Internet Privacy' (2000) 88Cal L Rev 1507 at 1512.
[93]Kozyris (note 89) at 2.
[94] Ibid.
[95] Zimmerman (note 4) at 440.
[96] Daniel J Slove (note 17) at 755.

brother' and the all seeing eye of the big brother,[97] the internet has seen the introduction of a swarm of 'kid brothers who constantly watch and interrupt our lives.'[98] These kid brothers can be anybody and their activities manifest in form of 'internet or local unauthorised access to information systems, illegal dissemination for commercial purposes, unauthorised disclosure, modification and loss of use.'[99]

4.4.1 Publishing personal data

Publishing of personal information on the internet raises a number of challenges which are unique to that medium unlike in the case of a hard copy. If information relating to a particular person is published on the internet the material will immediately become available to the world as long as they have access to the internet. Although publications locally in a hard copy may have resulted in material being taken to another jurisdiction, publication on the webs site have different consequences regarding for instance, restrictions on transborder data flows.[100] Further, publication on the Internet implies a greater reach as it transcends geographical borders. Virtually anybody who has access to the internet can have access to that particular information. Personal privacy can be violated in this way, for instance personal data might be volunteered for publication in a small circulation magazine having a defined audience with a common interest - publishing the same online even if for the same audience exposes the personal information to a vastly wider readership than that which might have been contemplated.[101]

Publishing of personal information also exposes a particular computer network to security concerns depending on what those who gain access to the network hope to achieve. Some hackers will hack into a computer network just for the fun of it. As if this was not enough the internet has also introduced novel forms of publication for example web cams, face book, and twitter. These entail vast amounts of information being placed on the sites as part of the networking. All these are vulnerable channels of information that make the protection of personal information a challenge on the internet.

---

[97] Henderson (note 8) citing George Orwell at 11.
[98] Simpson Garfinkel ' Privacy and the New Technology: What they do not Know can hurt you,' (2000) 270 The Nation at 11.
[99] Ambrosia Totaval et al 'Legal requirement Reuse: A critical success factor for requirement quality and personal data protection' (2000) Computer society
[100] Graham J H Smith, Bird & Bird *Internet Law and Regulation* (2002) 3rd ed London at 367.
[101] Ibid at 367.

4.4.2 Holding material on an internal data base or computer system with internet connectivity.

Most internal corporate computer systems have internet connectivity to allow employees to access the internet for purposes of carrying out their duties. This in itself poses security challenges as unauthorised agents may access the system. Where personal data is incorporated into material held on an internet site available for public access, or access to a closed group, different considerations have to apply for purposes of securing the site. Unless access is restricted by encryption and a firewall any person with access to the internet may visit the site and extract information. This will expose the data subjects to the risk that information relating to them may be acquired by strangers within or in other countries and may be used for unregulated purposes which were not in contemplation when the information in question was originally obtained from the data subjects concerned.[102]

4.4.3 Sending information Via the internet e-mail

Internet email raises security issues as to whether the information can be intercepted during transmission at any point at which the email might be stored. An internet connection may be routed through different countries and the email may be potentially 'sniffed'(examined) or accessed during transmission this may raise data protection concerns in that the data subject is robbed of a chance to consent to their personal information being accessed. However, email differs in often being stored in mail boxes hosted by intermediaries pending being accessed by the recipient, whereas a web or a file download session is conducted in real time between the servers and the user's PC.'[103] When the email is being hosted by an intermediary that might provide a weak link for the unauthorized access in cases where the intermediary is not well protected or intermediary may well decide to harvest personal information it is hosting for purposes of selling to direct marketing companies.

4.4.4 Cookies

The internet makes one realise that the computer screen is not a mirror but rather a window, so that as the user searches for information and makes selections, data bout

[102] Smith (note 100) at 368.
[103] Ibid.

that individual are moving outward where they are accumulated in data bases through the use of cookies.[104] Cookies can betray an internet user in two primary ways. Firstly, cookies are stored in the user's hard drive and when accessed they reveal a detailed list of electronic footprints of the internet user.

The trail of transactional data left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce and it will show the websites visited by the user within the relevant time.[105] When aggregated, these digital fingerprints have value because they provide businesses a glimpse of your life that might indicate your attitudes and preferences respective to services and products,[106] and therefore make you a target for personalized advertising. The cookie files may reveal personal information about the user password, email address or indeed any other information that was entered at the site.

The second way in which the cookies may affect privacy is that the servers who send cookies also receive information stored in a particular cookie when a user makes a return visit to the same site.'[107] For example it is very common for Website operators or banner advertisement companies to acquire data about the visitors to their websites. This may be overtly done through a visitor completing a questionnaire or covertly through cookies. Depending on what the website is offering or how much the visitor wants the service being provided, a visitor will be forced to provide personal information by completing a questionnaire or be unable to proceed to the next level of the website. In fact most successful websites such as hotmail, yahoo and Gmail provide individuals with free services in exchange for information about the viewer, for instance free email.[108] Cookies rob an internet user of the choice to consent to their personal information being accessed and also the opportunity to have a say on how the information will be used.

---

[104]Henderson (note 8) at p4.
[105]A testimony of Ari Shwartz Policy analyst before Government reform Sub Committee on available at http;//www.cdt.or.
[106] Willam Fendrich 'Common Law protection to individuals right to personal information' (1995-1997) 65 fordham L Rev p 952 available at http://www.law.nyu.ed accessed 27/07/11.
[107] Zimmerman (note4) at 443.
[108] Basho (note 92) at 1515.

4.4.5 Data Mining

Data mining has been defined as a set of automated techniques used to extract buried or previously unknown pieces of information from a large database.[109] Using data mining techniques it is possible to come up with a wide range of information, including on relationships and behavioural patterns through the revealed preferences of users' activities. In the broadest sense, data mining has been said to be 'a process of finding patterns or correlations in data for records stored in large data bases and analysing that data from different perspectives, categorising and summarising it to come up with useful information.'[110] In other words data mining is a process for making sense of or finding patterns in data.

In data mining there are potentially two ways in which the right to informational privacy can be violated. Firstly, in some instances data mining is used to collect information about a data subject without their awareness – therefore no consent is gained from the individuals or data subjects involved. Secondly, in instances where permission was originally secured to collect information about data subjects in the processing of the data, data mining affords certain data processors a chance to use it for purposes other than for which it was intended.

Data mining also violates the data protection principle of 'purpose specification' because data mining programs by their design reveal information that would have been extremely difficult to foresee and therefore secure the necessary consent.[111] Further because data mining operates on implicit patterns of association and responds to open-end user queries, its software makes it possible for terabytes of data containing personal information to be examined for detection of meaningful patterns in response to the open ended questions. However, 'since data mining is based on the extractions of unknown patterns of information from data bases...users of data mining techniques cannot predict what type of potentially valuable personal information or what kind of relationships in the data will emerge'[112] therefore it becomes a challenge to conform with the minimality, and use principle.

---

[109] Cauvokian A 'Data Mining: Staking your Claim on Your Privacy Data information and Privacy Report' (1998), Ontorio Canada.
[110] Herman T Tovani 'Information Privacy Data mining and the internet' (1999) Kluwer Academic publishers Netherlands at 137.
[111] Ibid at 140.
[112] Tovani (note 110) at 114.

4.4.6 Profiling

'Profiling' is the process where data from different sources or the same data base are processed layer upon layer to come up with a profile or description of characteristics pertaining to a data subject. This kind of information has proven to be gold for marketers who buy it for purposes of direct marketing and also sell it to other agencies. This has been augmented by the drop in the cost of storage of information, the level of sophistication of the analytical tools and the sheer processing power available in modern computers. These capabilities enable rapid sorts and searches that are able to construct a profile based on many sources of data, many of which are suspect, 'in short, a man on the street finds his profile based on data that has little connection to him and less connection to the use made of his information and whose existence he is largely unaware of'[113] contrary to data protection principles relating to choice and consent.

The challenge is that the information in these data bases may be outdated and inaccurate. Since the data subject may not be aware of its existence, not only is he or she deprived of choice, he or she will not be able to contribute to the quality of their personal information. The consequences may be far reaching in that, for instance one may not be offered accommodation or a loan based on a profile whose existence they may not be aware of. Should an individual find out about the said profile, the onus will be on the individual to prove that the profile is inaccurate and not vice-versa.

4.4.7 Social Networks

Social network sites have become very common modes of interaction especially among students and youths in general. What attracts users to these sites is the ability to converse with friends, share digital cultural artefacts, ideas and connect to vast networks of people at almost zero cost.[114] Despite these potential benefits to the general populace, scholars, privacy advocates and the media have raised concerns over the risks associated with the disclosure of personal information on these sites,[115] as people continue to willing divulge information on these sites believing that they have control over their personal information after reading the security settings.

---

[113]Tovani (note 110) at 114.
[114] Alyson L Young and Anable Quan-Haase Information Revelation and internet privacy concerns on social network sites: A case study of face book (2009) citing 'Boyed and Heer (2006)' at 1 .
[115] Ibid at 1.

The truth is that the users to these social networks actually have no control over their personal information.[116] Simple member ship of either face book or my space permits access to more fields than anticipated at the point of registration. For instance, the common chain of friends provides a channel for publishing personal information to other parties beyond the scope envisaged by the user. One wonders how far the chain of friends of friends goes in terms of sharing information. This provides a window for publishing personal information to other parties beyond the scope envisaged by the user.

The other challenge is that even after one cancels subscription to a particular network site the site keeps those individuals personal information for unknown periods of time. Networking sites are actually gold mines ripe for harvesting of personal information as people utilizing these tools can end up divulging more information that what they would ordinarily divulge if they were aware of the potential for others acquiring this information.

4.4.8 Ubiquitous or pervasive Computing

The reality of ubiquitous or pervasive computing refers to the services provided through countless invisible devises imbedded in the users' environment. These may be work-related or personal. Pervasive computing provides numerous opportunities for the violation of privacy. Of particular relevance is the proliferation of use of ambience intelligence technologies in the form of Radio Frequency Identification tags (RFIDs) which track users and transmit information as they move around. This includes information on the person's behaviour, habits preferences, aversions and associations. The challenge of pervasive computing is its requirement to be non obtrusive hence its need to be embedded in the everyday objects that transmit and receive information. The embedding reduces visibility of the pervasive computing environment making it more user friendly and acceptable, 'ironically the same characteristic makes it possible to violate the privacy of the user.'[117]

Through ubiquitous technology, a world was envisaged in 2005;

> *...a world of smart dust with networked sensors and activators so small as to be virtually invisible where the clothes you wear , the paint on your wall, the carpets on your floors, the paper money in your pocket*

[116] Poullet (note 88) at 212
[117] Pankaj Bhaska and Sheiki Ahamed 'Privacy in Pervasive Computing open issues'(2007) 1EEE at 2.

> *have a computer communication ability. It's a 4 G world were today's phone is transformed into a terminal capable of receiving television, accessing the internet, downloading music, reading RFIds, taking pictures enabling interactive video telephony and much more. It's a world of heterogeneous devices are able to communicate seamlessly across today's disparate networks, it's a world of machine ... where computers will decide our activities, routines, behaviours and predict what we will do next...a world where we will never have to worry about losing granny or junior because he will have a location device implanted under the skin, if they are squeamish one in their watch.*[118]

The smart world as it was then imagined is already upon us. A silent revolution is occurring in the retail surveillance technology unbeknownst. RFIDs 'technology provides enormous economic benefits for both the businesses and consumers while simultaneously potentially constituting one of the most invasive surveillance technologies threatening consumer privacy.'[119] In fact, RFID technology can enable the tracing of the life circle of a product from the production line all the way to the recycling centre such is the extend of intrusion enabled by this technology.[120]

The use of ubiquitous technologies is not only being used in retail, it is steadily on the increase in emergency services as well. The company 'Applied Digital Solutions' has designed an RFID chip called the 'verichip' which can be implanted under the skin. The chip will provide a way of tracking children, the disabled and Alzheimer patients. Surely this proves the existence and well being of Big Brother[121] who appears to be watching at all times.

The fact that ambience technologies will deliver personalised services means that somewhere, a large amount of personalised data will have to be stored. It has been stated that compared to the current computing technology, pervasive computing [heavily] relies on an increased amount of, quality, accuracy of the data generated.[122] The challenge still remains as to whether the information will be safe from abuse by those who are the gate keepers or indeed those who will manage to access these data bases.

---

[118] Davide Write 'The Dark Side of Ambient Intelligence' (2005) 7 no. 6 33 at 51 available at http://www.top100net accessed 27/0711.
[119] Eileen P Kelly and G Scott Erickson 'RFID Tags: Commercial applications vs Privacy Rights' www.emaraldinsight.com/researchregister accessed on at 1.
[120] Ibid
[121] Ibid
[122] Bhaska and Ahamed (note 117) at 3.

4.5 Information Technology and the Privacy of Workers

From an employment law perspective, the right to privacy is of particular relevance in relation to internet and email use. The new information technologies in the work place present new ways of processing vast amounts of information in ways that it was not thought possible not too long ago.

The collection of information from employees is not unusual, in fact the employer can access a huge amount of information of the employee long before the person is employed. The sources of information include the application letter, the curriculum vitae, medical records and criminal records if any. After the person is awarded employment the employer continues to gather and keep personal and other kinds of information for purposes of appraisal, evidence of misconduct, compliance with tax and the conditions of employment, and collective bargaining (wages, medical aid, social benefits).

Now more than ever the employer is able to compile vast amounts of information especially with today's' computer systems that automatically store traffic records, these include the time of transmission of every email along with the content of its subject line and the details of recipient or recipients.[123] As if that was not enough no information deleted by the employee is completely deleted as it remains on the server for as long as the employer wants the record there.

The fact that an employer can amass huge amounts of information and employ surveillance of the employee (whatever the justification) brings with it a huge risk with regards to violation of the right to privacy of employees, especially considering that 'more and more, the line between 'personal' and 'professional' is being blurred as workers conduct personal businesses in the office and professional business at home.'[124] The question is, considering that the use of new information technologies have resulted in a big erosion of the privacy of each employee, whether the individual employee should be able to expect privacy in the place of work?

Unfortunately, generally workers do not have an expectation of privacy in the office and employers can monitor activities of the employee including email as long

---

[123] Mark Jeffery 'Information Technology and workers privacy' (2005) 2351 Comp. Labour law and Policy Journal at 251.

[124] Lara Hartman 'Technology in the workplace' (2001) 106:1 business and society review at 8.

as the monitoring has a reasonable, business-related purpose,[125] however in the case of Copeland v United Kingdom in the European Union, monitoring of an employee's email was held to be in violation of the employees right to privacy.[126] Many employers point to the legal system as to the reasons why they monitor the employee's e mail and web usage[127] arguing they could be held vicariously liable for offences committed by employees in the course of their work.

However in terms of protection of personal information in the work place, The International Labour Organisation ("the ILO") adopted a Code of Practice on Protection of Workers' Personal Data ("the ILO Code") approximately 10 years ago. The Code identifies the following principles that should govern and limit the collection of information in the workplace:

> *1. The information collected must be directly* ***relevant*** *to the employee's employment 2. The information should be* ***obtained from the employee.*** *Any information obtained from third parties must be done so with the* ***employee's consent.*** *3. The information must be* ***used for the purpose for which it was collected.*** *If it is required for another purpose, consent must be obtained first. 4. The employee must be* ***informed*** *about the nature of the information being collected, its purpose and the manner of collection. 5. The use must be* ***proportional*** *and the method used must be the least intrusive.*[128]

Employers in whose countries these codes have been adopted are required to take steps to ensure that the personal information relating to employees is secure and protected from unauthorised access. Access will only be authorised if there is employee consent or it is necessary to prevent imminent and serious harm to health and safety or if the information is necessary for the conduct of the employment relationship or it is necessary for criminal or civil litigation.

In a nutshell, in terms of the use of email and the internet the employee cannot be guaranteed privacy but in terms of protection of personal information the employee enjoys some level of protection. This is however being applied unevenly in the world.

---

[125] Henderson (note 8) at 31

[126] 626117/00 [2007]ECHR 253 can be accessed

[127] Henderson (note 8) at 31

[128] Available http//www denysreit.om.za and www.ilo.org.safework/normative/codes/lang--en/doc/NameWCMS_107797/index.thml.

4. 6 The Internet as an E-commerce Driver and Data privacy

Electronic commerce (e-commerce) as a general concept includes 'any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct contact.'[129] It can also be said to be the use of electronic means to exchange information and to carry out activities and transactions.[130] The underlying thread in both definitions is the use of electronic means to transact, mostly through the internet to conduct business.

E –Commerce has a broad range of financial and other applications such as dissemination and exchange of digital data, electronic funds transfer, electronic stock exchange activities, commercial auctions, electronic bidding, and direct consumer sales to mention a few.[131] These transactions can occur between business to business, governments to business, business to consumer. For the purposes of this discourse, of particular interest is the scenario of business to consumer transactions, where there is a large difference in bargaining strength between the parties and therefore the abuse of personal information is more likely to occur.

The Internet is an exciting tool that has redefined ecommerce. With the click of the mouse one can buy an air ticket, send flowers, send or receive money, work anywhere, communicate in real time etc. The internet therefore is particularly important when considering the issue of the protection of personal information as it has introduced a whole range of ways people do business and communicate, resulting in a number of areas in which protection of personal information is important. For instance the internet has introduced virtual markets where you can get almost all kinds of products and services without physical contact with the suppliers and will probably never meet the employees of that virtual enterprise.[132] However, in these markets for the purposes of completion of the transaction, an individual would have to divulge personal information. One would have to provide, at minimum, his or her name, address, and credit card details. A good example of a virtual enterprise is

---

[129] Karen Alboukrek 'Adapting to New World of Electronic Commerce: The need for Uniform Consumer protection in the International Electronic Market Place' (2003) 35 Geo. Wash. Int'l L. Rev 425 at 427.

[130] Louise A Lefebvre and Elizabeth Lefebvre 'E-commerce and virtual Enterprises: issues and challenges for the Transition Economies' (2002) 22 Technovation at 313.

[131] Ibid.

[132] ibid at 312.

Amazon which has no physical point of sale but it has become of the United State's largest book and media sellers.

The internet has also given birth to an entirely new market entailing the organisation and sale of personal information.[133] For example, cyber click a marketing company recently purchased by Google operates by placing cookies on your computer when you visit one of their clients' websites, and collects information through the cookies placed on the hard disk and establishes consumer profiles that adapt and personalize the publicity banner.[134] The challenge is that as '[technologies] replace face to face contact the individual receives no compensating increase in control over the use and disclosure of his personal information.'[135]

4.7 The Benefits of Electronic Commerce

E-Commerce has changed the economic landscape of the global economy. The importance of e-commerce cannot be over emphasized, and this greatly informs the discussion of protection of personal information, as this must be seen in the context of the functions of e-commerce in supporting the global economy. Trade is happening at unprecedented levels as the world becomes more interconnected. The following are some of the benefits that come with the advent of e-commerce;

4.7.1 Worldwide Access and Greater Choice

E commerce transcends physical borders and knows no limit as the world is its market place. This is possible as 'through global net works like the internet, world wide Web, both businesses and consumers are able to transcend global barriers.'[136] As a result of these global networks, commercial entities need not worry about physical location as they can be everywhere and are accessible any time of day as time and distance cease to be a constraining factor e-commerce. This translates into unlimited access by consumers as well as greater choice for consumers due to businesses which are no longer inhibited by physical location. In other words, 'e-commerce offers businesses world visibility, direct, inexpensive access over the market to international markets.'[137]

---

[133] Moshel (note 11) at 360.
[134] Poullet (note 88) at 212.
[135] Filvaroff (note 87) at 1403.
[136] Alboukrek (note 129) at 429 .
[137] Lefebvre and Lefebvre (note 130) at 313.

4.7.2 Enhanced Competitiveness and Quality Service

Once the challenges of distance and time zones are eliminated, businesses are able to concentrate on improving their businesses and products. This frees businesses from worrying about physical infrastructure and things incidental to a physical business. This ultimately translates into more time for businesses to concentrate on customer satisfaction and improving their products. E-commerce has also seen the introduction of new ways of advertising as millions of adverts can be sent at the click of the button though bulk electronic messages. This is a very cheap and efficient way of advertising. Because of the borderless nature of the internet and the low cost of internet services, businesses are able to have worldwide exposure in terms of advertising. This kind of advertisement, if done indiscriminately without due regard for the law is what comes to be known as spam – the unsolicited bulk electronic commercial or non commercial messages which can easily become a nuisance to clients, with vast potential for violating consumer rights to privacy.

4.7.3 Mass Customization and Customized Products and Services

With the new players on the global market (those who deal in buying and selling of personal information), businesses are now able to collect detailed personal information and can cater to the specific needs of the customer. This is the positive side of the intrusive technologies such as data profiling of personal information. The result is 'customised products to those offered by specialised supplies but at mass market prices.'[138] The customer is happy as they do not have to sift through a lot of adverts to get to the things that are of interest to them. Businesses also make more sales as a result of these personalized services.

4.7.4 Elimination of the Intermediary and Product Availability

Unlike in the non electronic realm, in e-commerce there is no need for intermediaries like the retailers or wholesalers as products are sold directly to the consumers in most cases. The internet now makes it possible for goods to move from the manufactures to consumers, this implies large profit margins for the manufactures and cheaper and more readily available goods for the consumers due to the cutting of the chain of supply.

---

[138] Alboukrek (note 129) at 430.

4.7.5 Greater Efficiency and Lower costs

E commerce provides for greater efficiency in the global market place due to the lower costs of communicating information electronically and processing transactions. It allows for the efficient harnessing of smaller and more geographically dispersed vendors. Not only does e-commerce increase vendor participation it reduces transaction costs for both the vendor and the purchaser. A good example is eBay an internet bidding site were virtually any one of contractual age can transact.

4. 8 The argument for measures to protect personal information

The above are some of the benefits at the instance of e-commerce. It has been argued that 'the opportunities e-commerce offers are so great that it appears there is no going back.'[139] However e-commerce has also created new opportunities for the abuse of personal information, as it leaves 'an extensive trail of personal information' in the process of conducting business.[140] This information may be compiled through the use of intrusive technologies and subsequently sold off without the data subjects knowledge and consent. When information is sold as a consequence of e-commerce we have the birth of a new method of advertising 'spam.' Spam can be a nuisance as, not only does it violate individual privacy, it may also prove to be costly on the part of the consumer in terms of time spent on deleting spam or requiring the purchase and installing of software to fight spam.

Other challenges that may arise include, 'using the world wide web [to] place sellers beyond the reach of national courts increasing consumer exposure to unfair marketing practices, unsafe products, insecure payments systems and loss of personal information.'[141] This creates a challenge relating to dispute resolution as the consumer may be exposed to a foreign dispute resolution forum which will imply huge costs and if successful challenges of judgement recognition and or enforcement. On the other hand the business entities will potentially have to comply with hundreds of consumer protection laws hence need for uniformity or harmonisation of consumer and data protection regulatory framework in the regulation of e-commerce globally.

---

[139] Lefebvre and Lefebvre (note 130) at 313.
[140] Reidenburg (note 81) at 719.
[141] Alboukrek (note130) at 433.

It must however be noted that E-commerce does not particularly raise new data privacy issues, it just increases the level of complexity when dealing with interests of citizens in fair treatment of their personal information[142] hence the need of standard data protection laws to provide legal certainty and confidence for purposes of e-commerce.

4.8.1 The case of Electronic Commerce (E Commerce) and Trans-border Data Flows

Technology has made it possible for multinational firms to establish electronic links for organisational data transfers with strategic partners to promote global integration of their businesses. They have also enabled seamless flow of real time digital information across international boundaries in support of business operations.[143] Therefore as cross border exchanges or transactions over the internet increase, legal issues come to the fore inter alia, the applicable law between transacting parties, contractual relationship and capacity, the disputes resolution mechanism to be employed and indeed the forum. Because of these concerns it becomes important to regulate trans-border data flows in order to create legal certainty as well as promote global trade.

The underlying principle for restriction or regulation of trans-border flows of data lie in the need to set international standards for data protection while promoting free flow of information across boundaries.[144] To this end, all international data protection instruments had two primary goals; (i) The setting of standards at the national level for the protection of personal data and (ii) The reconciliation of this goal with the idea of allowing the free flow of information across national boundaries.[145] The rationale was to bring uniformity between national rules and consequently greater legal certainty. These were to be rigorously enforced in the area of cross border data flows so as to prevent data havens and making of a mockery of those countries that have achieved milestones in data protection.

---

[142]Redeinberg (note 81) at 719.

[143] AtlaVanishree Rudraswami and david A Vance 'Transborder data Flows: Adoption and diffusion of Protection Legislation in the global electronic environmen' (2001) 14 at 127.Available at http://www.soc.napier.ac.uk and http://www.emerald-library.com.fic accessed on 3/08/1.

[144] Dir 95/46/EC no 8 preamble.

[145] Annelise Roos 'Data protection; Explaining the international backdrop and evaluation the current south African position' (2003) SLJ 400 at 404 citing the Discussion paper project 109 available at http//salawrform.justice.gov.za.

The European Union was the first to take a stand in the transfer of personal information to third countries through its Directive on data protection.[146] The Directive only permits the transfer of personal information to third countries if the recipient country has an adequate level of data protection based on all the factors surrounding a data transfer operation, particularly taking into consideration the nature of the data, the proposed processing operations duration and the existence of data protection laws and security measures in that third country.[147] The concern was understandable given the borderless nature of the internet[148] and the fact that permitting the abuse of the European Union's Citizen's information outside of Europe would make a mockery of the decades of effort expended on creating high levels of data protection.[149]

Non adherence or failure to meet the adequate threshold can have far reaching consequences, for example Nedbank South Africa has been forced, at great extra cost, to set up processing centres in Europe, in order to meet European information protection legislative requirements because it cannot transfer information about its customers from its branches in Europe and Hong Kong (China) to its headquarters here in South Africa.[150]

4.9 Conclusion

Advances in information and communication technologies during the 'Information Age' have transformed the way information is collected, stored, analysed and used. As the pace of innovation and pervasiveness of these technologies has increased, so the issue of privacy of users' information has come under scrutiny on a number of fronts. Huge amounts of data pertaining to individuals derive from multiple sources, are processed continuously and are often universally available. This can affect the way institutions and others relate to individuals, and have far-reaching consequences.

---

[146] Dir 95/46 EC art 25
[147] Dir 95/46 ECArt 25 para 2.
[148] Ida Madieha 'E-commerce and Privacy Issues of the personal data Protection Bill' (2002) Amsterdam available at http://www.bileta.ac.uk.02Papers/madieha.html accessed on 3/08/11 at 8.
[149] Shwartz (note 3) at 72.
[150] Roos (note 145) citing The South African law review commission paper para.7.19 at 421.

Privacy is a particularly critical issue for the growth of electronic commerce, which is a critical component of modern economy and life.[151] While embracing the benefits accruing from the advent of e-commerce it is important to bear in mind increased risk of privacy violation that accompany the technology. There is a need to find a balance between the protection of personal information and the need to promote e-commerce. Accordingly I argue that consumer confidence must be boosted by putting up measures that protect consumers against abuse of their personal information thereby giving them some control over their personal information. If the challenges relating to technology and privacy are not addressed people will be afraid to engage in e-commerce, which will have negative effects.

[151] Joel Reidenburg 'Restoring Americas privacy in electronic commerce' (1999) 14 Berckley Tech. L J 777 at 772.

CHAPTER V

COMPARATIVE ANALYSIS OF THE APPROACHES TO DATA PROTECTION THE UNITED STATES OF AMERICA AND EUROPEAN UNION

5.1 Introduction

The European Union and the United States of America approach data protection from different perspectives. In the European Union privacy is considered a fundamental human right, deserving rigorous and comprehensive legislative safeguards. It is intimately tied to the protection of honour and dignity,[152] However in the United States privacy is traditionally conceived of as a 'right to be left alone,'[153] is treated as commercial property and not specifically provided for by the United States of America Constitution. The Americans tend to view privacy as an interest that is mainly, if not exclusively, of value to the individual person qua individual persons and therefore exists in tension with the wider society.[154]

Thus, given the American approach to privacy, legislative safeguards are less stringent and 'provide very little protection for personal data,'[155] and while some specifics law may provide protection for some of this information these laws generally apply to the public rather than to private institutions. The Americans tend to see privacy as important primarily for ensuring freedom from government intrusion.[156]

> *The relative laxity of the United States legislative safeguards for privacy is not just a symptom of cultural difference in the way privacy is valued; it reflects numerous factors, not least paucity of first hand domestic experience of totalitarian oppression in the USA, at least for the bulk of white society. In contrast European legislative policy reflects the traumas from firsthand experience of such oppression. The traumas' impact on that policy and anxiety is largely missing in the United States of America.*[157]

---

[152]Lee Bygrave 'International agreements to protect personal data' edited by James B Rule and Graham Greenleaf *Global Privacy Protection: The First generation* (2008) Edward Elgar Publishing Limited Cheltenham Northampton at 16.

[153] John D R Craig citing Warren and Brandeis the 'right to privacy in Invasion of privacy and Charter values: the common law tort awakens' (1997) McGill L J 193 at 196.

[154]Bygrave (note152) at 16.

[155]Blanke (note 82) at 58.

[156] (note152) at 16.

[157] (note 152) at 16.

The differences exist even at terminology level. Whereas the United States of America uses words like 'information privacy,' the definition of this being very broad, the European Union uses terms like 'data protection,' which is more specific. In addition the former has also got a separate tort of privacy whereas the latter has been resisting this and ensures that, through various case laws,[158] that no such tort exists.

5.2 Data Protection in European Union

Data protection in the European Union is regulated by the European Union's Directive on data protection. The approach is grounded in the concept of privacy as a fundamental human right. The European Union Convention on Human Rights (ECHR) in article 8 provides for the right to the respect for privacy and for family life. This right has been upheld in a number of cases,[159] for instance the Court of Human Rights has recently held that telephone calls and e mails from a business fall under 'private life' and 'correspondence' and are subject to a reasonable expectation of privacy on the part of those using these as a means of communication and any monitoring of these communications constitutes a breach of Article 8 of the ECHR.[160] According to this principle, only when individuals are able to interact with self determination and dignity can there be a just and free society.[161]

The fact that the European Union favours the Comprehensive model of data protection is clear from the EU directive on data protection. Though it must be noted that this directive only prescribes the floor threshold for the signatories and its general thrust is to establish a set of rules capable of broad application and impact.[162] The directive is very comprehensive and complex in nature. It exercises some political and legal influence over other countries outside the European Union in the sense that it prohibits the transfer of data to these countries unless they meet the adequate data protection levels.

The thrust of the Directive[163] is in articles 6 and 7. These provide principles for processing personal information. In a nutshell the Directive provides a

---

[158] Waynright V Home office (2003) U K H L 53, 16 2003
[159] For instance in the cases of Dimitrov V. Bulgaria (Applications no. 37358/97, 37988 and 39365/98) and in the case of S. Marper V UK [2008] ECHR 1581
[160] Copland V UK [2007] ECHR 253
[161] Long and Quek (note 56) at 331.
[162] Bygrave (note 26) at 31.
[163] Dir 95/46 EC

requirement for personal data to be, 1. Processed lawfully and fairly, 2. Collected for a specific and legitimate purpose and not further processed in a way incompatible with the original purpose, 3. Adequate, relevant and not excessive for the purpose for which it was originally collected, 4. Accurate and up to date in terms of the information, 5. Kept no longer than necessary in any form in which it is possible to identify the data subjects or in a form in which they are further processed.

Article 6 addresses issues relating to consent and provides that personal information shall only be processed with the consent of the data subject, which consent should not be ambiguous. In the absence of such consent personal information may be processed where there is a need for the performance of a contract, or when the processing is for purposes of compliance with the law, or where the processing is for purposes of protecting the interests of the data subject, in the interests of the public or. The Directive, under article 8, also provides for a stricter requirement for so-called 'sensitive data.' This is data that refers to an individual's racial or ethnic origins, beliefs, or trade union affiliation. This category of personal information requires a higher level of safeguards.

Articles 25 and 26 provide for the transfer of personal information to a third country. These transfers can only be made if that third country meets the adequate level of protection as prescribed by the European Union Directive. The adequacy of a particular level of protection is assessed on a case by case basis. In an assessment of the level of adequacy the circumstances surrounding the transfer of data operation are considered, in addition to the nature of the data, the purpose and the length of that data processing operation, the country of origin and the country of final destination, the rules of law, both general and sectoral-, and the professional rules and security measures. Section 26 provides derogations to the general rule since to every general rule there are exceptions. These derogations unfortunately have the potential to compromise the standards of data protection

The Directive also provides for the creation of an independent national supervisory authority which will be responsible for oversight and enforcement of the privacy protections provided by the Directive.[164] Citizens are at liberty to complain to the Authority and seek redress in case of violations personal information. The

[164] Dir 95/46/EC,Art 28(1).

Authority may also of its volition commence investigations into perceived violations of the privacy of the citizens' personal information.

Although the European Union Directive creates a strong baseline of data protection across Europe, divergences and ambiguities will inevitably occur because different supervisory agencies of member states will interpret the data protection principles in different ways.[165] Although it could be argued that this could the negative side of the European approach, the European system also provides extra legal administrative support for purposes of data regulation. The working party[166] offers a formal channel for data protection officials to consult each other and reach consensus on critical interpretive issues.[167] To some extent this process provides consensus on the understanding and interpretation of the principles in the Directive.

5.3 Data protection in the United States of America

American legal and philosophical thinking about privacy begins with Samuel Warren and Louise Brandeis's 1890 Harvard Law Review article, in which they argued that the common law protects the 'right to privacy', which implies 'the right to be let alone.'[168] They anchored the right to privacy on the common law protection for intellectual and artistic property, arguing that the right was not based on the property right but on the inviolable personality. Others have however argued that the United States legal system treats privacy as a personal property right that may be disposed of as one sees best, rather than as an unassailable human right.[169] In other words, according to this definition, privacy is essentially commercial in nature. Thus it is no surprise that Americans tend to be more trusting of the private sector and the free market than of the state to protect personal privacy, fearing more invasion of privacy from the state than from the free market.

The second major milestone in the American discourse around privacy was attained by William Prosser in his 1960 article 'Privacy'[170] who argued that the right to privacy in one form or another was recognised in four different tort protections,

---

[165] Redeinburg (note 81) at 734.
[166] The working party is composed largely of representatives from each member states data protection Authority. The chief task is to provide independent advice to the European Union on a range of issues including uniformity of application of measures on data protection.
[167] Redeinburg (note 81) at 734.
[168] John D R Craig (note153) at 196.
[169] Long and Quek (note 56) at 332.
[170] Edward J Bloustein 'Privacy as an aspect of Human dignity, An Answer to Dean Prosser' (1964) 39 N. Y. U. L. Rev 162 at 965.

unlike the case of the European Union which does not recognise an independent tort of privacy. These tort protections include intrusion, disclosure, false light and appropriation. In other words, Prosser's view of privacy extended beyond the right to be let alone to ways in which it could be invaded.[171] In terms of intrusion the right to privacy could be violated by a physical entry upon that space considered personal. In the case of disclosure this 'intrusion' meant making public that personal information which the owner considers to be private, although this right did not extend to that information that is held by a public entity. False light refers to the publication of personal information that is highly offensive but not necessarily defamatory in nature. Public disclosure refers to the publication of embarrassing private information that is not newsworthy but would be highly offensive to a reasonable person.

In the United States there is no comprehensive or generally applicable data protection legislation, nor does the Constitution provide an express provision for the right to privacy. However it is important to note that over time the Supreme Court has recognized a number of privacy rights deriving from the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments. These constitutional protections only apply to government action and exclude the private sector,[172] thus reinforcing the argument that Americans are more trusting of the private sector.

On the basis of the First Amendment which implies freedom of expression, and the due clause of the Fifth and the Fourteenth, the court upheld a number of privacy interests including association privacy,[173] and political privacy.[174] The Fourth Amendment, which provides 'the right of the people to be secure in their houses, papers, and effects against unreasonable searches and seizures' is an important basis for privacy protection. The leading case tried under the Fourth Amendment is the case of Katz V United States,[175] a wire tapping case in which the court ruled that the Fourth Amendment protected people and not places, and did not require physical trespass or seizure of property in the course of investigation.

---

[171] Priscilla M Regan 'The United States' *Global privacy: The first generation* (2008) ed. By James B Rule and Graham Greanleaf at 51.
[172]Regan (note 171) at 51.
[173] NAACP V Alabama 357 US (1958)
[174] Watkins V US 354 US 178 (1957) an d Sweezy V Hampshire 354 US 234 (1957)
[175]389 US 347 (1967)

The Fifth Amendment protection against self incrimination also protects privacy. Courts have interpreted it to prohibit compelling anyone from disclosing incriminating information about themselves in criminal proceedings. It must however be noted that the court has limited the protection of personal information to that information which is the possession of an individual, as in the case of Couch V United States.[176] This was a case where petitioner challenged the Internal Revenue service directing ac accountant to produce records of accounts. The court held that the Fifth Amendment held no bar to produce the accounts records as there was no personal compulsion for the petitioner to divulge his books of accounts since he had willingly surrendered them to his accountant.

Because of its piecemeal and fragmented data protection approach the United States makes use of a mixture of disparate data protection models, such as the sector regulation, self regulation of the private sector and the use of technology. This fragmented system does not resemble the United States' European Union counterpart, which has a comprehensive and coherent data protection regime. Professor Redeinberg has pointed out that the American legal system responds incoherently and incompletely to privacy issues raised by existing information activities.[177] Realising how inadequate this incoherent response to data protection is, a number of proponents of comprehensive data legislation in the United States have been advocating for more comprehensive data protection legislation. However there is always a vocal and well financed opposition to privacy protection generally, from business and government bureaucrats who do not want to restrict access to personal information. Opposition from these groups usually takes the form of weakening the proposed privacy protections and further narrowing the scope of such protection[178] and placing more emphasis on the protection of freedom of expression afforded by the First Amendment.

Because of the United States federal system of government, there are basically two levels of legislative protection in terms of data protection; the federal level and the state level. In terms of protection of personal information the federal legislation is more important because it cuts across state lines. It is important to note

---

[176] 409 US 322 (1973)
[177] 'Business Information and " personal Data" some common law observations' (1994) 95 hein Online Iowa L R 95[accessed on April 27], 2011 at 621.
[178] Regan (note 171) at 51.

that federal legislation in terms of privacy protection laws is sector or industry driven. For instance in the area of consumer privacy at the federal level there are; Fair Credit Reporting Act,[179] Fair Credit Billing,[180] Fair Debt collection Practices Act,[181] Debt Collection Act.[182]

In the area of Financial Privacy, in the case of US V Miller,[183] the Supreme Court held that an individual has no constitutional legitimate right to privacy in records of financial transactions. A number of laws have since been enacted to remedy that situation, although obviously in piece meal fashion. These laws include the Bank secrecy Act,[184] enacted before the miller case. The Electronic Funds Transfer Act,[185] the Right to Financial privacy Act,[186] and the Gramm-Leach-Bililey Act[187] were enacted after the Miller case. This implies that now a person has a legitimate right to privacy of his financial transactions.

In the area of identity theft obviously an extreme example of loss of personal information privacy, there are the pieces of legislation at the federal level which protect personal information include the Identity Theft and Assumption Deterrence Act[188] which makes it a crime for anyone to knowingly transfer or use without lawful authority as a means of identification the means of identification of another person with intent to commit, aid or abet any unlawful activity that constitutes a violation of federal or state law. There is also the Identity Theft Enhancement Act[189] and the Fair Credit Reporting Act Amendment.[190]

In terms of the protection of Government records, there is the Privacy Records Act,[191] the Freedom and Information Act, the Electronic Freedom of Information Act,[192]and the Computer Matching Privacy Protection Act.[193]

---

[179] 15 U.S.C s. 1681 (1970)
[180] 15 U.S.C s. 1666 (1975)
[181] 15 U.S.C 1692-1692o(1977)
[182] public Law97-365 as amended (1982)
[183] 425 US 435 (1976)
[184]12 U.S.C. s.1970
[185]15 U.S.C. s. 1693-169r(1978)
[186]12 USC (1978)
[187] 15 USC s.6801 (1999)
[188]18 USC s.1028 (1998)
[189]18 USC s.. 1028 (2002)
[190] 2003
[191] 1974
[192]5 USC s 552 (1986)
[193]5 USC s 552 as amended(1988)

The Omnibus crime control and safe streets, Wiretap Act,[194] prohibits intentional unauthorized, interception, use and disclosure of communication by government agencies but also provided exceptions. The act extended the Fourth Amendment against unjustified searches and seizure of information being communicated via a telephone line. Under the said omnibus crime control act, the 1986 Electronic Communications Privacy Act (ECPA) was enacted take care of those technological advancements which were not covered under the wire tap law. The ECPA fills in the gap covering the protection of privacy from radio-paging devices, electronic mail, cellular phones, computer data transmissions etc. Meanwhile the United States' Patriot Act[195] was a quick response to the September 11terrorist attack. It was meant to expand government powers in the investigation of terrorism.

The approach to spam regulation, as with other privacy protection legislation, was also piecemeal until the CAN SPAM Act.[196] The Act does not ban spam as such but is based on the 'opt out' regime. An individual is therefore not precluded from receiving one unsolicited message but once he or she received of the message and 'opts out' it will be an offence for the sender to continue to send these unsolicited messages to that individual. The act has been criticised for this but this notion obviously originates in the belief of the United States in the freedom of speech as applied to the field of commerce.

The salient features of the CAN SPAM Act are its focus on marketing commercial messages and its provision for criminal sanctions for the use of false headers and false information[197]. It also provides for the use of specific subject line labels for messages containing explicit materials. In addition it prohibits dictionary attacks and the harvesting of emails. The primary responsibility for the enforcement of the CAN SPAM Act lies with the Federal Trade Commission (FTC), and various other federal agents, which are charged with maintaining a 'do not-email' list.[198] The do not send list means that before advertisers send any electronic spam they would have to check the list, and would be precluded from sending spam to all those people

---

[194] 1968
[195] Officially called the Unity and Strengthening America by Providing Appropriate tools Required to Intercept and Obstruct Terrorism, H. R. 3162 (2001).
[196] 15 U.S.C. 103 (2003).
[197] 15 U.S.C. 103 s. 7705.
[198] 15 U.S.C. 103 s.7708.

whose names appear on the list failure to which they would be committing an offence.

The Act also provides a private right of action to Internet Service Providers (ISPs) to bring actions against spammers and gives latitude to the ISPs to develop their own private policies for the handling of spam which may extend beyond the scope of the Act. Unfortunately the Act does not make provision for the right of action for private individuals and business against spammers, but there is a bounty that is provided for whistle blowers who help provide information leading to the discovery of the identities of these illegal spammers.

The above are some of the pieces of legislation that protect privacy at the federal level in the United States. At the state level there is also an array of data protection laws with various states falling under different sectors or groups and further underlining the major difference in the approach to data protection between the United States and the European Union.

In stark contrast to the coherent system dictated by the European Union Directive, there is no single central United States government agency that supervises privacy protection.[199] Instead the Office of Management and Budget (OMB) and the Federal Trade Commission (FTC) enforce specific private laws. Unfortunately the FTC can only enforce those laws relating to consumer credit and to unfair trade practices,

> *but has no authority to enforce privacy rights other than those arising from fraudulent trade practices. Self regulation is an important element of the American data protection regime. The high tech industry believes that the bureaucracy lacks the 'capability and the flexibility to deal with the rapid pace of change and innovation of the information economy.* [200]

On the whole the US business community supports the layered approach to data protection which assumes that 'private-public regulation, publicly announced corporate policies and industry codes of conduct are backed by the FTC and state

---

[199] Julia M Framholz 'The European Union data privacy Directive' (2000) 15 Berk Tech L J 471 at 473.

[200] Thomas Olsen 'European union Data protection regulation and automatic processing of information on the internet' (2001-2002) University of Southampton also available at http://.jus.uio.no.

level enforcement in response to private civil actions for damages or injunction relief.'[201]

To conclude, in terms of data protection regimes, the United States of America and the European Union are definitely at opposite ends of the spectrum of data protection and hence the need for a compromise.

5.4 Safe Harbour Compromise

The United States, which prefers to leave regulation to industry, views the data protection Directive as a classic demonstration of the European fondness for bureaucracy and regulatory overkill.[202] A face-off between the data protection positions of the European Union and the United States in 1995 presented an interesting scenario at a time when the world's largest consumer market, and the world's largest economies, respectively occupied extreme ends of the data protection spectrum.[203] This gave rise to a protracted set of negotiations and an eventual compromise known as the 'safe harbour' agreement. The agreement is based on 'safe harbour' principles which would allow United States industry to conduct business under the European privacy conditions.[204]

The dispute between the United States and the EU over data protection regulation erupted because of the European Union's sweeping Directive. The Directive had the effect of harmonizing data protection among the EU member states and also held non member countries to a standard equivalent to an 'adequate' level of data protection.[205]

At the time of the passage of the above mentioned directive the United States did not meet the required threshold of data protection. Firms in the United States that do business with Europe had to pay to pay entities in Europe to process their information or risk being blockaded. The immediate solution for the United States was to ask for the suspension of the directive while a negotiated settlement was attempted. There followed the protracted negotiations between the European Union

---

[201]Long and Quek (note 56) at 333.
[202] Micheal Chissick and Allistir Kelman *Electronic Commerce Law and Practice* 2nd ed (2000) at 199.
[203]Moshell (note11) at359.
[204]Chissick and Kelman (note 202) at 199.
[205]Long and Quek (note 56) at 326.

Commission and the FTC of the United States. The result of these negotiations was the Safe Harbour Compromise.

The Safe Harbour compromise became a short-term solution for a compromise between the two regional economic giants. Though it was a solution to the immediate problem the safe harbour has been 'said to have weakened the European standard for redress of data privacy violations'[206] because of the derogations allowed under the Safe Harbour. A compromise between the worlds' two most powerful, and highly interdependent, economic entities was being put to the test and the result would impact significantly on global trade. The EU is the United States' largest trading partner and was therefore the most vulnerable to the potential restriction on the transborder data flow.[207]

In a nutshell, if the relationship between the European Union and United States is the engine of the world economy and information flow is the oil that that keeps the machinery running,[208] it follows that at whatever cost the engine had to be kept running, and thus a compromise needed to be reached.

5.5 Safe Harbour Principles

The safe harbour agreement includes a statement of safe harbour principles and a set of frequently asked questions (FAQs). These documents are collectively referred to as the 'Principles.'[209] The FTC makes specific reference to the OECD guidelines and the Directive. It identified five core principles of privacy protection and what it termed 'fair information practices.' The most fundamental principle was held to be the principle of Notice. According to this principle consumers have to be given notice of the entity which is collecting data, the uses the data would be put to, the potential recipients, the nature of the data and the means which would be used in the collection of the data.

The second principle was the choice or consent principle. At its simplest, according to this principle consumers should be given options in terms of how their information will be collected and used. This choice relates specifically to secondary uses of personal information, for instance, uses beyond those necessary to the

---

[206] Redeinberg (note 81) at 744.
[207] Long and Quek (note 56) at 326.
[208] Long and Quek (note 56) citing Hirst and Thomson in the 'The Tyrany of Gloabalization: Myth or Reality' (1999) at 326.
[209] Blanke (note 82) at 78.

contemplated transaction for example, the placing of a consumer on a mailing list in order to market additional products or promotions.[210] Traditionally there are two types of choice/ consent regimes: the opt-in and opt-out regimes. Opt-in regimes require affirmative steps by the consumer in the process of allowing the collection and/or use of information, whereas the opt-out regimes require affirmative steps to prevent the collection and or/use of information.[211] In the opt in regime a business would need express consent for the customer before engaging the customer, not even silence would amount to consent, whereas in the opt out a business would engage a customer while in the opt out the customer would have to actively say no to whatever is being offered.

The third principle, the principle of Access /Participation refers to an individual's ability to both access his or her personal information and contests its accuracy and completeness. To be meaningful the exercise must be neither too costly nor too time consuming for the data subject. The fourth principle is that of Integrity / Security. According to this principle data needs to be accurate and secure. To assure data integrity, data collectors must take reasonable steps such as using reputable sources and destroying information that is incomplete or dated. In terms of security both managerial and technical measures must be put in place to ensure unauthorized access, destruction, use or disclosure of data.

Finally the fifth principle that was agreed upon was that of Enforcement or Redress. This principle was perhaps the most important in that it would defeat the whole purpose of data protection if there was no way of enforcing or guaranteeing the individual's right to data protection. The parties further agreed on the criteria necessary for inclusion in the list of companies in the safe harbour scheme and on sanctions to be applied for violations of the European Union Data Protection Laws.[212] The idea was that companies in the United states would self certify to adhere to the safe harbour principles. A company would then be presumed to provide adequate privacy protection and could continue to receive personal data from the European Union.[213]

---

[210] Ibid at 71.
[211] Ibid.
[212] Chissack and Allistir (note 202) at 199.
[213] Roos (note 145) at 416.

The safe harbour agreement signifies the importance of enacting a data protection regime that meets international standards and the consequences of falling short of these would be to be subjected to a blockade of the flow of data. The lesson to be learnt is that if America, being as big an economic sphere as it is, and as dedicated as it is to the notion of self regulation, was forced to negotiate a compromise, a small third world country would undoubtedly be expected to tow the line.

5.6 A Case for South Africa and the upcoming protection of personal information bill

The South African government is in the process of enacting a piece a legislation that will be comprehensive and particularly dedicated to the protection of personal information that is processed by the private and public sector. This piece of legislation will be giving effect to the constitutional right to privacy in South Africa and will regulate data protection in accordance with international standards.

The right to privacy has long been acknowledged in the South African courts. In the case of National Media Limited Vs Jooste, Neethling's definition of privacy was accepted as being 'an individual condition of life characterized by exclusion from publicity, which condition includes all those facts which a person himself (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.'[214] This means that an individual need not labour on the understanding of right to privacy in the context of the South African context as the jurisprudence will attest to that in forma a number of cases that have been decided.

5.7.1 Right to Privacy in Common Law

In terms of the Common law, the right to privacy was recognised as 'an independent right of personality'. Infringement of the right to privacy under the common law was enforced through delict (tort) as a consequence of a duty of care. The person whose right had been infringed had to prove that the conduct at issue was wrongful, intentional and that it caused injury to him or her.

---

[214] 1993 (3) SA 262 (A) at 271

Although South Africa has a well developed level of protection of the right to privacy and identity in the law of delict, it was realised by the courts that it was not sufficient to provide adequate data protection since the traditional principles do not give active data control of personal information.[215] Like any other right, the right to privacy is not absolute, as a common law right, it is limited by the legitimate interests of others and by the public interest.

5.7.2 Statutory protection of the Right to Privacy

In terms of statutory law, the Constitution,[216] which is the supreme law of South Africa, provides for the right to privacy under section 14, Chapter 2. The right to privacy is entrenched in the Bill of Rights. It is therefore a fundamental human right so that any conduct which is inconsistent with it is invalid. The entrenchment of privacy as a fundamental right in the South African Constitution strengthens the protection of the right to privacy and gives it a higher status in the sense that it becomes applicable to all laws and becomes binding on the state as well as on natural and juristic persons.[217] As is the case under the common law, the constitutional right to privacy is not an absolute right and is capable of limitation.[218]

In South Africa there are a number of pieces of legislation that play a role in the protection of personal information. These include the Electronic Commercial Transactions (ECT) Act,[219] The Promotion of Access to Information Act,[220] which provides for individuals who want to gain access to their personal information that is held by private or public bodies. The Credit Act[221] also provides for confidentiality of personal information and consumer credit records. For purposes of protection of personal information the ECT Act will be considered in greater detail than the other pieces of legislation as it relatively comprehensive in terms of data protection and embodies data processing principles.

---

[215] Roos (note at 47).
[216] Constitution of South Africa no.108 of 1996.
[217] Constitution of South Africa no 108 of 1996 s 8 ss2.
[218] S. 36 of the Constitution of South Africa provides that the right to privacy is not absolute, it can be limited by a general application to the extent that the limitation is reasonable and justifiable in open democratic societies based on human dignity and freedoms.
[219] ECT Act no. 25 of 2002.
[220] Act no.2 of 2000.
[221] National Credit Act no.34 of 2005.

5.7.3 Electronic Communications Transactions Act

The ECT act of 2002 was primarily enacted for purposes of regulation of e-commerce as most of the laws in the country did not make provisions for e-commerce or indeed take it into consideration. The process to determine an electronic commerce policy for South Africa started in September 1998, when research started which led to the drafting of a Discussion Paper on e-commerce[222] based on the OECD guidelines on Governing the Protection of Privacy and Transborder Flows of Personal information. The passing of the ECT Act in South Africa was recognised by as the most significant legal step taken to log on to the world of electronic communications and e-commerce.

Like the ECT act of Zambia (Chapter VII), Chapter VIII of the ECT act of South Africa aims at addressing the privacy concerns of consumers by enumerating the principles that must be adhered to when electronically collecting personal information. However, unfortunately subscription by the data controller and the data subject to the said principles is voluntary as stated in the Zambian case.

5.7. 4 Data Protection from the ECT Act towards the Protection of Personal Information Act

As a response to the call by the European Union Directive to provide adequate data protection legislation, South Africa has set the wheels in motion for the enactment of more comprehensive data protection legislation, hence the birth of the Data Protection Bill. This process commenced when, in '[o]ctober 2005, the South African Law Reform Commission (SALRC) published a Discussion Paper on privacy and data protection containing a draft Bill on the protection of personal information.'[223] This was supposed to be the foundation for the discussions and contributions to the enactment of the protection of personal information Act.

The Protection of Personal Information Bill is an attempt by the government of South Africa to provide comprehensive data protection legislation for the processing of data by both the public and private entities. The bill aims to provide

---

[222] Green paper available at www.polity.org.za/govdocs/green_papers/green.
[223] Roos (note 145) at 400.

and ensure the constitutional right to privacy as well as to regulate personal information in accordance with international standards of information processing.[224]

The provisions ECT Act of South Africa and the protection of personal information bill in South Africa will be compared and contrasted for purposes of drawing useful lessons for Zambia, bearing in mind that the ECT acts of the two countries are almost similar. This implies that the shortfalls under the South African ECT act will apply to the Zambian case.

Both the ECT Act and the Bill are premised on the OECD guidelines and as such embody similar data protection principles. However the differences between the two lie in the scope. In terms of scope of application, the Bill goes beyond the scope of the ECT Act, in that it and extends to data which is electronically or manually collected by both public and private bodies[225]. This takes care of the challenge of protection of information that is manually collected.

Both the ECT act and the Bill embody similar principles though the scope of the principles under the Bill is wider, for instance, the purpose of limitation principle, S. 51 (1) which requires disclosure to the data subject of the purpose for which the information is collected[226] is similar to the provisions in Sections 8 to 11 of the Bill,[227] which provides for the need for express consent, lawfulness of processing, minimality and that the collection be done directly from the data subject.

Both the ECT act and the Bill contain the principle of specific purpose sections 51 (3) and (4) of the Act[228] and sections 12 and 13 of the bill Act. These sections aim to address the transparency principle by requiring that the data controller disclose in writing to the data subject the specific purpose(s) for which any personal information is being requested, collected, collated, processed or stored. Clearly the requirements under the bill are more comprehensive than those in the

---

[224] Preamble of the Protection of personal information bill
[225] Section 3 of the Bill (PPI B 9-2009) provides that the bill applies to the processing of information entered into a record by or for a responsible party domiciled in the republic or not but by using automated or non automated means subject to section exceptions as provided in section 4 of the said bill.
[226] ECT Act no 25 of 2009.
[227] PPI Bill B9-2009.
[228] ECT Act no 25 of 2009.

ECT act. The Bill will encompass the further processing principle, which the ECT Act does not seem to have under section 15 of the Bill.[229]

In terms of the principle relating to quality, the requirement of the ECT Act that the data controller delete or destroy all personal information that has become obsolete, constitutes a limited attempt to address the data quality and proportionality principle and as such the provision cannot be said to be similar to section 16 of the Bill.[230] The Act is lacking in principles which address issues such as the accuracy of the data, that they must be kept up to date, adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

The Openness Principle under section 17 of the Bill[231] is another provision that is being introduced by the Bill and as such does not accord with a similar provision in the ECT Act. This requires the data controller to allow data subjects access to the data base to enable the data subject have a say over the quality of data. In fact this is one of the major differences between the provisions of the Act and those of the Bill. The data regulator and the concept of notification are also unique to the Bill in this regard.

The Bill has included the principle of Security Safeguards as provided for under section 18 to 20.[232] This principle is lacking under the ECT act, it therefore introduces the principle of security which implies that the Bill will add to the protection of personal information in the sense that it requires data processors to ensure adequate security of personal information in their custody use of whatever means at their disposal. This principle imposes an obligation on the part of a responsible person to provide security measures for the maintenance of the integrity of information. A responsible party must take reasonable technical and organisational measures to secure the integrity of information in order to prevent, inter alia, loss, damage, or unlawful access to the information. The Bill further provides for the need by the responsible party to notify the regulator in case of compromise of the security system.

In addition, the strength of the Bill lies in the fact that subscription to mechanisms of data protection of personal information is mandatory, unlike the ECT

[229]PPI bill
[230]PPI Bill B 9-2009.
[231]PPI Bill B 9-2009.
[232]PPI Bill B 9-2009.

Act where this is voluntary,[233] although, once the parties' subscribe to the data protection principles, they are obligated to subscribe to all of them.[234]

In terms of Supervision and Enforcement, the Bill again goes beyond the scope of the ECT Act,[235] which provides for the establishment of an Information Protection regulator, an external supervisory body which shall be responsible for ensuring compliance in terms of the Bill and also provide for criminal or penal sanctions under Chapter 11 of the Bill, unlike the ECT Act.

The bill further provides a complaints mechanism where a data subject can lodge a complaint against the processor where he or she believes there is an infringement under section 71 of the Bill[236] as a part of the enforcement mechanism this allows an individual to enforce his or her rights rapidly and effectively, again this is not the case under the ECT Act. The Regulator will receive and deal with complaints, and may lodge investigations where non-compliance is suspected. There is an obligation to notify the Regulator before any personal information is collected or processed. In certain instances (e.g. where the processing of information may affect an individual's rights or freedoms) the Regulator may initiate an investigation. In such cases processing may not commence while the investigation is ongoing.

The Bill makes specific reference to the transfer of personal information s. 69 of the Bill in a bid to meet the international dictates of data protection legislation. This has clearly not been provided for under the ECT Act.

To sum up, the Bill goes a long way towards meeting the international standards for data protection as provided for by the European Union Directive and as such, once enacted will mean that South Africa stands a very good chance of benefitting from the data flows from the European Union thus contributing not only to e-commerce, but also providing its citizens with a substantial level of control of their personal information: compliance will mean compliance with the highest standards of data protection, higher even than those of the United States.[237]

---

[233] ECT Act no 2002 s50 ss2.
[234] ECT Act no 2002 s50 ss3 -4.
[235]ECT Act no 2002 s 35.
[236]PP I Bill B9-2009.
[237]Roose (note 145) at 406.

5.8 Future Reforms: a lesson for Zambia

Since the ECT Act of South Africa is almost verbatim with the ECT act of Zambia, the short comings of the South African ECT Act also apply to the Zambian ECT Act and it would be prudent attempt to emulate South Africa in moving towards the enactment of a comprehensive Personal Information Act.

One of the lessons the Zambian government can learn from South Africa is that, in spite of information privacy being a fundamental human right expressly provided by the Bill of Rights, the South African government is in the process of designing and enacting a comprehensive data protection regime. This suggests the level of seriousness attached to data protection in the country. One cannot emphasise enough the benefits that come from an adequate data protection. An adequate data protection regime will not only enable the country meet the international dictates for data protection but will ultimately reduce the cost of doing business in the country and of promoting e-commerce by instilling confidence in the consumer who will be secure in the knowledge that her or his personal information is being adequately protected.

Currently a country with a growing economy such as Zambia cannot afford to ignore the global trend towards the designing and enactment of comprehensive omnibus data protection legislation. Thus, if the country is interested in contributing to and benefiting from e-commerce and free data flows, it should not be content with fragmented legislation relating to the protection of personal information. One reason for this is that lack of privacy protection may seriously hinder economic development, firstly because there will be a reluctance on the part of consumers in the uptake of online services, and secondly because the inability of commerce to access certain foreign markets thus be to the detriment of economic growth.[238]

For a long time in Zambia the challenges posed by technologies that had been posed in developed countries had not been experienced or overcome in Zambia as the country lagged behind in terms of technological advancement due to inadequate infrastructure. Owning a computer until recently was considered to be a luxury. A few people had access to the internet in the 1980s and 1990s when the challenges and pitfalls of data protection where still being debated in Europe and the United States.

---

[238] Delrae Goodburn and Martha Ngoye *Cyber law @SA II The Law of the Internet In South Africa*, (2004) at 171 available at http://www.cyberlawsa.co.za .

The technological challenges, that before seemed still to be at a distant removed, have now arrived in Zambia with the influx of cheap computers from China and an increase in internet services[239] which are being provided at a relatively low cost.

Zambia's lack of interest in and sensitivity towards, the protection of personal information may be attributed to the prevailing traditional culture. However this argument is not a useful or valid one, as technology is advancing rapidly whether a people like it or not. Whether we like it or not the world is becoming a global village and a people must subscribe to certain standards and regulations in order to advance economically.

[239] Patrick Ngulube 'The Nature and accessibility of E-government in Subsaharan Africa' (2007) 7 International review of information ethic at 4.

CHAPTER VI

CONCLUSIONS AND RECOMMENDATION

6.1 Conclusions

In conclusion, technological advancements in the 21st century have greatly increased the possibility of violation of our personal information so that the only way to effectively protect one's personal privacy is to leave no transactional trace as one lives one's life which is almost impossible.[240] Now one fears not only intrusion from 'Big Brother' but from 'a swam of little brothers who spend 24 hours a day gossiping with one another'[241] while they gather and exchange our personal information for whatever purpose. Thus, in order for Zambians to be able to gain control over the use and dissemination of their personal information, and in turn to promote e-commerce and free transborder data flows, it is important for the country to come up with a comprehensive data protection regime.

Zambia's piecemeal and fragmented as evidenced by the few pieces of data protection law not even as detailed as the United States case leaves a lot of its citizens vulnerable to violations of their personal information, especially in the areas not covered by the ECT Act, such as manual records. A fragmented data protection regime does not meet the current global trend in data protection which shows a shift towards a comprehensive privacy protection system of legislation. The various pieces of legislation that protect personal information are primarily sectoral. In addition the common law does not provide adequate data protection as it the traditional torts do not accommodate the challenges arising from the rapid development of technology.

Lack of adequate data protection can hinder economic development, firstly because there may be a degree of hesitancy regarding the uptake of online services by consumers, and secondly because of the inability to access certain foreign markets and consumers due to privacy concerns.[242] Our concerns relating to the potential abuse of our personal information are real, as Carole Lane, author of a book about finding personal information online, boasts;

---

[240]Fenrich (note 106) at 955.
[241]Henderson (supra note 8) at 16.
[242] Goodburn and Ngoye (note 238) at 171.

> *...in a few hours , sitting at my computer beginning with no more than your name and address ,i can find out what you do for a living, the names and ages of your spouse and children, what kind of a car, house and how much you pay in taxes on it. From what i learn about your house and the demographics of your neighbourhood, i can make a good guess at your income. I can recover the forgotten drug bust in college*[243]

Although the ECT Act embodies some of the core principles of data protection, it is inadequate as it only relates to electronically processed information and excludes the bulk of personal information that is manually recorded, taking into consideration that the biggest challenges for privacy protection lies with electronically processed information. In addition, the fact that subscription to the Act is voluntary, serves as another reason for enacting a piece of legislation which makes it mandatory to subscribe to all the data protection principles. This omnibus legislation should also make provision for a regulatory body which would be responsible for sensitization and for enforcement breaches in cases of violations of personal information.

Although it has been argued that countries that have attempted to regulate electronic commerce allegedly face the penalty of capital flight,[244] it would be folly for a developing nation like Zambia, which is still in its infancy in the area of e-commerce, to leave the regulation of e-commerce to the market.

Though the trend in terms of data protection is to use the European Union Directive as model, it has been suggested that it would be prudent to look beyond the standard established by the Directive as one can argue that the Directive was meant to deal with the problems of processing data which were present in 1995[245]when the challenges of ambience technologies were not yet pressing.

One must also be alive to the fact that, despite the theoretical appeal of the legislative solution to the protection of personal information, individuals should not wait for legislative action but try to legislate the issues in courts of law as well as using privacy enhancing technologies. It would perhaps be useful to explore the new 'co regulatory model' of data protection.

---

[243] Carole A Lane, Naked in Cyberspace: How to find personal information online. Wilton,Conn.:Pembaton Press 1997 p 3 in Privacy in the information age p 18 also available at http://kaslab.net accessed 5/18/11.

[244] Long and Quek supra note (56) at 327

[245]Poullet (note 88) at 214

6.2 Recommendations

- There is need for the sensitization of the general populace through print, television and radio, as well as the electronic media, such as social networks, to the significance of data protection in the country, viewing it against the background of the failure of data protection to gain some prominence during the deliberations of the latest Constitution Review Commission. This would be in order to make it possible for information privacy to be specifically incorporated not only in the general right to privacy but also under fundamental human rights.
- There is also need for massive sensitization with regards to the challenges and the both the benefits and the dangers of technologies in the area of protection of personal information.
- Sensitization of the people to their right to privacy, educating them about the remedies available in order to build on our case law with regards to the right to privacy.
- Enactment of comprehensive system of data protection legislation premised on the European Union model, and which will encompass all the data protection principles, extend the scope of application of the rules and principles as well as make the subscription mandatory.
- The comprehensive legislation should be augmented by technologies that enhance security.

BIBLIOGRAPHY

Primary Sources

STATUTES

Republic of Zambia

The Constitution Chapter 1

Banking and Financial Services Act, CAP 387.

Electronic Transactions Act, No.21 of 2009.

Information and Communications Technologies Act, 15 of 2009.

Postal Services Act, No.22 of 2009.

Republic of South Africa

Constitution No. 108 of 1996.

Electronic Communications Transactions Act no.25 of 2002.

National Credit act no. 34 of 2005.

Promotion of Access to Personal Information Act no 70 of 2002.

Protection of Personal Information Bill available at www.polity.org.za.

European Union

Directive 95/46/ EC of the European council and Parliament and of the Council of 24 October 1995 available at http://eur.europa/eu.

Convention For the protection of Human rights and Fundamental Freedoms as amended by Protocols 11 and 14.

Convention for the Protection of Individuals with regard to automatic processing of personal Information. Strausboug 28/1/81 available at http://Conventions.coe.int/Treaty/en/Treaties /Html/108.

The United States of America

Bank Secretary Act, No.12U.S.C. of 1970.

Computer Matching Privacy Act, No. 5 U.S.C. 552 of 1988.

Controlling the assault of Non-solicited-Pornography and Marketing Act no.15 U.S.C. s 7701 (SPAM ACT 2003).

Debit Collection Act, No. 15 U.S.C.1692 of 1977.

Electronic Communications Act, No. 18 USC of 1986.

Electronic Freedom of Information Act, No. 15 U.S.C.1693 of 1978.

Fair Credit Reporting Act, No. 15 U.S.C. of 1970.

Fair Credit Billing Act, No. 15 U.S.C.1666 of 1975.

Fair Debit Collection Practices Act, No. 15 USC 1601 of 1982.

Financial Privacy Act, No.12 U.S.C. of 1978.

Gramm-Leach-Bliley Act, No. 15 U.S.C. of 1999.

Identity Theft Enhancement Act, No HR 5588 of 2002.

Privacy Records Act, No. 5 U.S.C. 55 of 1974.

Patriot Act, Public Law HR 3162 107-56 2001.

Theft and Assumption Detection Act, No. 18 U.S.C. 1028 of 1998.

Wire Tap Act, No. 18USC s. 2510-22 of 1968.

COURT CASES

Couch v. United States, 409 U.S. 322 (1973).

Copeland v.UK, ECHR.253 (2007).

Dimitrov V. Bulgaria (App. 37358/97,37988, 39365/98).

Katz v. United States, 398 U.S. 347 (1967).

Marper, S v. UK ECHR, 1581 (2008).

Nawakwi v. Attorney General, ZR 112HR, 112 (1990).

National Media Ltd vsJooste, 3 S.A. 262 (1993).

NAAC v. Alabama, 357 U.S. 4449 (1958).

Patel v. Attorney General, ZR 99 (1969).

Sweezy v. Hemispher, 354 U.S. 234 (1957).

United States v. Miller, 4252 U.S. 234 (1976).

Waynright v. Home Office, UKLH:16 (2003).

Zanka v. Attorney General, ZR HC.73 (1990-1992).

Secondary Sources

Alboukrek K 'Adapting to New World of Electronic Commerce: The need for Uniform Consumer protection in the International Electronic Market Place' (2003)35 Geo. Wash. Int'l L. Rev 425.

Allen A 'Privacy as a data control : Conceptual practical and moral limits of the paradigm.'

Bhaskar P, and Sheik I 'Privacy in pervasive computing and open issues' (2007) IEEE

Blanke J M '"Safe Harbour" and the European Unions Directive on data protection' (2000-2001) 11 Alb. L J Sci. & Tech. 57.

Bloustein E J 'Privacy as an aspect of human dignity, An answer to Dean Prosser' (1964) 39 N. Y. U. L. Rev 162.

Bygrave, L. *A data protection law, approaching its rationale, logic and limts: information law series.* (2000) Kluwer Law International, The Hague.

Cate, FH 'Information privacy and the public interest' (1994-1995) 80 Iowa L Rev 431.

Cauvokian A 'Data mining: Staking your claim on your privacy data information and Privacy Report'(1998) Ontorio Canada.

Chissick M and Kelman A, *Electronic commerce law and practice* 2nd ed. (2000) Sweet & Maxwell publishers,London.

David B 'Privacy and data protection around the world' available at http://www.pcpd.org.hk.

Fenrich W J, 'Common law protection of individuals rights to Privacy' (1996-1997) 65 FordadL.Rev.

Filvaroff DB 'Privacy computers and the commercial dissemination of personal information' (1986-1987) 65 Tex L Rev 1395

Garfinkel, S 'Privacy and the new technology: What they do not know can hurt you', (2000) 270 The Nation available.

Goodburn D and Ngoye M *Cyber law in the law of internet in South Africa II* 2nd ed edited by Buys R and Cronge F (2004) Van Schaik Publishers.

Henderson, H. *Privacy in the information age* Revised ed. (2007) An imprint of Inforbase publishing, New York.

Kalinda B 'Licensing of our personal information; is it a solution to internet privacy' (2000) 88Cal L Rev 1507

Kafka F *The Trial* (1925)Translated by Wylie D, Free Books at Planet eBook

Kelly, E. P and Erickson, G 'RFID Tags: Commercial applications vs Privacy Rights' www.emaraldinsight.com/researchregister

Kozyris, P. J. *Regulating the internet abuses: invasion of privacy (*2007) Walter Kluwer Internationa, Law and Business, The Netherlands.

Lane C A, 'Naked in Cyberspace: How to find personal information online' (1997) Wilton,Conn.:pembaton press in privacy in the information age

Lefebvre L A and Lefebvre E 'E Commerce and virtual enterprises: issues and challenges for the transition economies', (2002) 22 Technovation

Long W J & Quek M P 'Personal data privacy protection in an age of Globalisation: the US-EU Safe Harbour compromise' (2002) Journal of European public policy 325

Madieha, Ida 'E-Commerce and Privacy issues of the personal data Protection bill April 5-6 '(2002) Amsterdam available at http://www.bileta.ac.uk.02Papers/madieha.html accessed on 3/08/11

Markesinisi Basil et al 'Concerns and Ideas about the developing English law of tort (how knowledge of Foreign law may help)' (2004) 52 1 American journal of comparative law

Moshel, R'...And then there was one: the outlook for the self regulatory United States amidst a global trend towards comprehensive data protection' (2004-200) 37 *Tex Tech L Rev* 357

Ngulube, P 'The Nature and accessibility of E-government in Subsaharan Africa' (2007) 7 International review of information ethic.

Nizer, Louise 'The Right to Privacy- Half a century developments' (1940-1944) 39 Mich L Rev. 526

Olinger et al 'Western Privacy and/or Ubuntu? Some critical comments on the influences in the forth coming privacy bill in South Africa' (2007) International information and Library review.

Denys Reitz 'Protection of personal information' (2009) Seminar paper on Protection of personal information available at http://www.dp/org/za

Poullet Yves 'Data protection legislation: What is at Stake for our society and Democracy' (2009) 25 Computer law Rev.

Redeinberg, J 'E-Commerce and transatlantic privacy' (2001-20012) Houston L. J.

Redeinburg J 'Restoring American privacy in electronic commerce' (1999) 14 Berklay Tech. L J 771

Roose A 'Personal Data protection in New Zealand; Lessons for South Africa' (2008) vol. 4

Roose 'Data protection; Explaining the international backdrop and evaluation the current south African position' (2003) SLJ 400.

Rudraswami, A and Vance D 'A Transborder data flows: Adoption and diffusion of protection legislation in the global electronic environment' (2001) 14 no. ½.

Rule, J.B. & Greenleaf, G *Global privacy: the first generation* (2008), Edward Elgar publishing inc, Cheltenham.

Schwart, P M 'European data protection law and restrictions on international data flows'(1995) 80 Iowa.

Smith, G. & Bird, J.H .*International law and regulation.* 3rd ed (2002) London: Sweet & Maxwell, London.

Solove, D J "I've got nothing to hide" and other Misunderstandings of privacy' (2007) San Diego L. Rev 745.

Tovani, HT 'Information privacy data mining and the internet' (1999) Kluwer Academic, publishers Netherlands

Van den Hoven, J. *Information technology and moral philosophy: information technology, privacy and protection of personal information* (2008) Cambridge University press. New York.

Westin, A F 'Social and political dimensions of privacy' (2003) 59 no 2 available at www.privacysummersymposium.com.

Whitley, E A 'International privacy, consent, the "Control" of personal data' (2009) EnCoRe publication

Write, D 'The dark side of ambient intelligence' (2005) 7 no. 6 Emerald group

Young, A L and Quan-Haase A 'Information revelation and internet privacy concerns on social network sites: A case study of face book' (2009)

Zimmerman R 'The Way the "cookies" Crumble: Internet privacy and data Protection in the 21st Century' (2000-20001) 4 NYU J Legis & Poly.

Business Information and "personal Data" some common law observations (1994) hein Online Iowa L R 19194 95 (accessed on April 27)

Personal privacy in the nformation age : comparison of the internet Data Protection regulation in the United States and the European Union heinonline 21 Loy L. A. Int'l &Comp L .J.1 1999