IS PART 6 OF THE COMMUNICATIONS ACT 8 OF 2009 A VIOLATION OF THE ENTRENCHED RIGHT TO PRIVACY?

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF

BACHELOR OF LAWS (HONOURS)

OF

THE UNIVERSITY OF NAMIBIA

BY

SHIMAKELENI APPOLOS. T

STUDENT NUMBER: 200712365

NOVEMBER 2011

Supervisor: Ms. EMILIA NAMWOONDE

ABSTRACT

The newly implemented Communications Act raises several constitutional questions. In trying to answer ensuing questions, focus should be given on the Communications Act, Part 6 in particular, and finding out whether the establishment of interception centres infringes upon the right to privacy as provided for in Article 13 of the The Constitution of the Republic of Namibia. Thus, the paper looks at the history and background of the right to privacy, case law on interception of communications, as well as its limitations. Furthermore, the Namibian Act is compared to the South African Act, which two Acts are more or less the same. After looking at the right to privacy and what it entails, the paper concludes that the right to privacy is enshrined, and it should be protected. However, Article 13 to some extend allows for interference for, amongst others, national security and other interests of the state. The Constitution in addition allows for some limitations on such a right through Article 22. Part 6 of the Act was enacted with the aim of combating crime and national security, as Article 13 provides for. Whether such enactment was reasonable in a democratic society or not is quite complex to decide upon, as it is subject to interpretation. Any conclusion to be reached on this matter is debatable, as aspects like determining whether a certain law is reasonable in a democratic society may be influenced by subjective elements. What the state may deem reasonable may on the other hand be regarded as unreasonable by certain sectors of the society. Nevertheless, the Communications Act falls within the bounds of the Namibian laws, unless it can otherwise be proved unreasonable in a democratic society.

Table of Contents

ACKNOWLEDGEMENT

I would like to thank my parents and siblings who have always been supporting me throughout my life. Without their support, I would not have achieved anything. I would also like to thank my friends, as well as classmates, for their kindness in always sharing ideas with me. Furthermore, I would like to thank my supervisor Ms. Emilia Namwoonde for the assistance and guidance in writing this paper. A word of thanks also goes to Professor Nico Horn for the guidelines he gave during the LLB Dissertation classes.

Declarations

"I, the undersigned hereby declare that the work contained in this dissertation for the purpose of obtaining my degree is my own work and that I have not used any other sources than those listed in the bibliography and quoted in the references."

Signature …….

Date …….

I, the undersigned hereby certify that the research and writing of this dissertation was carried out under my supervision.

Supervisor's signature ……..

Date …….....

CHAPTER ONE

1. BACKGROUND

1.1 Statement of the problem

The dissertation is going to look at the implications that the new Communications Act[1] has on the right to privacy, as enshrined in the Namibian Constitution[2], Article 13. The question would be; is allowing interceptions of personal communications a violation of ones privacy? This topic is crucial as far as democracy and the rule of law is concerned in independent Namibia. Some people, ordinary citizens and experts have lashed out through the media, saying that the newly implemented Communications Act is an infringement on people's privacy. The perception was that, every communication one makes will be viewed or listened to. Regarding this perception, does the Act, Part 6 in particular, has provisions in place addressing the issue of fulltime monitoring of all communications made? It is thus important to look into this matter, so as to make it clear what Part 6 of the Act was meant for, how it is regulated, and thereby coming to a stand, whether it infringes upon ones privacy. On the other hand, if it is to be said that Part 6 infringes upon the people's privacy, under what framework would such an infringement be permitted? Namibia is a developing country, and human rights are of significance to its people's well being, and so is the protection of the country's national security.

[1] No.8 of 2009.
[2] Act 1 of 1990: Article 13.

1.2 Introduction

When the then Communications Bill was tabled in Parliament, it was received with varied thoughts by different sections of the Namibian community. The proposers of the Bill argued that the provision for the establishment of the interception centres was because of the enhancement of national security. Furthermore, they argued that information may only be intercepted in certain circumstances, and only in accordance with a court order. To the ordinary citizen, implementing the Communication Act meant there was no more privacy, as all their calls, text messages, emails and faxes will be viewed all the time, or at certain times. It is of no doubt that the right to privacy is an internationally accredited and esteemed right that is inherent to every human being. Therefore, it is very important for any democratic country to respect and uphold such a right, thereby complying with its national laws and international instruments. Having said that, it can also not go unmentioned that, we are living in a world of ever growing technology, were technology and advanced technical systems are being used for illegal activities. For instance, one can throw a missile while seating at a computer at home. The existence of the internet which is being advanced day by day has changed many aspects of the society, and such excessive advancement has made it hard to a lot of things.[3] Thus, one can then try to reconcile the two; the right to privacy and implementing measures for national security. Consequently, this paper intent to analyse Part 6 of the Communications Act and see as to whether the establishment of the interception centres was reasonable, considering the people's right to privacy.

[3] Lloyde, I. 2000. *Legal Aspects of the Information Society*. London: Butterworths, p, 29.

1.3 Research Significance

Although the right to privacy may still be ambiguous, it is of no doubt that it is a very important right, which if taken away, renders other rights ineffective. The ever growing world of technology cannot be separated from privacy nowadays. A lot of devices and equipment are being manufactured daily, and it is through their use that it has become easy for ones privacy to be violated. The right to privacy can be violated in instances were a thief for example enters someone's premises illegally, or hacks into their email accounts. This is obviously unlawful and not allowed by law. Alternatively however, one ought to consider that due to technology, illegal acts have been made easier and it would be better if one deals with that problem using technology. Criminals may use the internet to communicate, and for any state to be able to track them down, certain communications ought to be intercepted. For any interceptions to be allowed, a law has to provide for such lawful interception. Such a law would have to be reasonable to ensure that the important right to privacy is not violated. This research is necessary and is of great importance, as it aims at looking at the section in the Namibian law, which provides for lawful interception. The research seeks to analyse whether provisions are in place to avoid abuse, and moreover, looking at the right to privacy, and under what circumstances it may be limited. The right to privacy is significant to every human being, and it is upon this that it should be ensured that any limitation on such a right are in compliance with the law, and do not lead to a nation where the country's inhabitants feel unsafe.

1.4 Methodological framework

Research was done from several books, academic articles, Journals, case law, internet sources, mostly dealing with the right to privacy. The Communications Act is

also consulted, Part 6 in particular. Furthermore, international law instruments are utilised, as well as laws enacted by several countries. I will be guided by several authors, focusing on the right to privacy, limitation of rights and interception of communications. Research is based on qualitative research, and no empirical study was carried out.

1.5 Research objectives

The objectives of the research are:

1.5.1 To explain what Part 6 provides for/ and what it does not provide for.

1.5.2 To deduce the legislators intention to enact such legislation.

1.5.3 To try and make out whether Part 6 of the Act is a violation of the right to privacy or not.

1.5.4 Compare the provisions of Part 6 to other jurisdictions, and glimpse whether the provisions were warranted.

1.6 Research questions

1.6.1 How can Part 6 of the Act be interpreted?

1.6.2 What was the legislator's intention in enacting Part 6 in the Act?

1.6.3 Is Part 6 establishing the interception centres a violation of privacy or not?

1.6.4 With reference to different authorities, was enacting Part 6 justified?

1.7 Literature Review

While the main aim of this paper is to provide arguments and the discussed relevant law on the topic, the literature review is to summarize the ideas and arguments of authors on the topic. The review in short, seeks to give an insight on the background of the topic, on an author's perspective. The literature review serves as a guide to

the writer, so that one would be able to determine which fields of the law have been previously addressed, and what has been laid down. Moreover, recommendations may be drawn from looking at what other author's had to say, and comparing it to the paper's objectives. It is well known that International law serves as the main guideline in most countries, and the running of those countries in relation to other states. For that reason, the literature review will look at International law, and then domestic laws and what authors or instruments provide for.

Author Barendt[4] focuses on the right to privacy entirely. He looks at why privacy is valuable in a democratic society, and hence the reason to maintain it. He further looks at the definition and scope of privacy. The author quotes other author's views on privacy, in their bid to try and come up with a definition of privacy, which despite its importance, has no fixed definition. The lack of definition is seen as capable of leading to uncertainty of the right. Fenwick[5] in Civil Liberties and Human Rights starts off with an introduction of where the rights derive from, before going into detail of specific rights. Part VI considers to what extend the agents of government have the power to interfere with individual liberty and freedom.

Author Michael discusses the nature and significance of the right to privacy. In addition, the author looks at the impact of technology on privacy, and the international standards of international human rights. Several international human rights instruments providing for the right to privacy are also discussed.

Part 6 of the Communications Act provides for the establishment of Interception centres. The President is vested with the power of creating such centres as he

[4] Barendt, E. 2001. *The International Library of Essays In Law & Legal Theory: Privacy*. Aldershot: Dartmount Publishing Company, p, xiii.
[5] Fenwick, H. 2002. *Civil Liberties and Human Rights*. Cavendinish Publishing: London, p. 670.

deems fit in the interest of the state. Part 6 provides which people may be employed, their duties, and to a certain extent, how they should go about their interception duties. The Act also gives out instances were one would be deemed to have violated the provisions of the Act, and the consequent penalty thereof. Other author's are also referred to in the paper, as well as case law dealing with interception of communications and the right to privacy, as well as limitation of rights.

CHAPTER ONE: *Background.* This Chapter consists of the research proposal, were the framework of the research is laid out, and focus given on how and why the research is to be conducted.

CHAPTER TWO: *Background and development of right to privacy.* This Chapter will deal with the right to privacy, its development and why it is important. Reference will also be made to case law in a few jurisdictions, and see how their laws handle issues of interceptions and privacy.

CHAPTER THREE: *Privacy as a fundamental right and its limitations.* This Chapter looks at the general limitations of rights as provided for by the Namibian Constitution. It further looks at case law dealing with limitations, and then discusses the extent to which the rights may be limited.

CHAPTER FOUR: *The Act in detail*. In this Chapter, focus will be given to the provisions of Part 6 of the Act. The provisions will be interpreted, explained and reflecting on how they are to be implemented. Comparison will also be made to other similar statutes, for example, the South African Communications Act.

CHAPTER FIVE: *Conclusion and recommendations.* The final chapter will provide a conclusion and shed more light to the problem, and give possible recommendations.

CHAPTER TWO

2. Background and development of right to privacy

2.1 Its basis and protection

Many if not all legal systems in the world protect the right to privacy. Privacy is one of the most respected human rights in the world, and ought to be upheld by all individuals and states that respect human rights. Such right is recognised by domestic laws, as well as International legal instruments.

In *Olmstead v United* States[6] Louis J stated that, "the makers of our Constitution..recognised the significance of man's spiritual nature, of his feelings and his intellect. They knew that only a part of life is to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government the right to be let alone-the most comprehensive of rights and the right most valued by civilised men."[7]

Author Bobbio provides that human rights, democracy and peace are the essential components of the same historical movement, and must thus develop in relation to each other. [8] He says that if human rights are not recognised and protected there is no democracy and that if there is no democracy, the minimal conditions for a peaceful resolution of conflict do not exist.[9] Among instruments recognising the right is the International Covenant on Civil and Political Rights of 1966, as well as the European Convention on Human Rights and Fundamental Freedoms of 1950.

---

[6] 277 US 438 1928.
[7] *Ibid.*
[8] Norberto, B. 1996. *The Age of Rights.* London: Polity Press, p.viii.
[9] *Ibid.*

It is nonetheless important to note that privacy is seen by many as the most difficult human right to define.[10] The proper definition of privacy has been a subject of much debate. As a right on its own, some authors are of the view that such a right should be defined, or it will bring about uncertainty.[11] Barendt quotes Richard Parker's essay (Chapter 5), that privacy is control over who can sense us. This formulation is advocated in preference to definitions which are in terms of control over information about someone or over personal information. Barendt also cites W.A Parent, who is of the view that privacy is the condition of not having undocumented personal knowledge about oneself possessed by others.[12] Davis sees the right to privacy as representing "that arena into which the state is not entitled to intrude." It is however difficult to establish as a matter of fact, where such a boundary starts.[13]

Under International law, privacy is provided for under Article 12 of the Universal Declaration of Human Rights of 1948, which provides that no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour or reputation.[14] Article 17 of the Covenant on Civil and Political Rights provides for the right to respect of privacy, family, home, correspondence and the protection of honour and reputation. [15] Regarding this provision, it is submitted that the word unlawful means that no interference ought to take place unless such interference is provided for by the law. This means that any interference must comply with the law, which must also comply with the spirit, aims and objectives of the covenant. The expression arbitrary arrest is said to extend to

[10] Michael, J. 1994. *Privacy and Human Rights*. Paris: Unesco Publishing, p.1.
[11] Barendt, E. 2001:xiii.
[12] *Ibid.*
[13] Davies, D. 1997. *Fundamental Rights in the Constitution*. Cape Town: Juta & Co, p, 94.
[14] Human Rights Declaration: 1948
[15] General Comment N0. 16: The Right to Respect of privacy, family, home and correspondence, and protection of honour and reputation (Art 17): 04/08/1988

interferences which may be provided for by the law. The view that arbitrary interferences also apply to instances were it is provided for by the law aims to ensure that laws of a state must also be in accordance with objectives of the covenant. The covenant makes it clear that in a modern society, the protection of privacy is most needed. Nevertheless, it must also be acknowledged that it is only considered as a violation of the right to privacy if it is regarding information about an individual, and such information is essential in the interests of the society.[16] The Committee to the covenant suggests that States must in their reports indicate the laws and regulations governing interferences with privacy. Furthermore, the relevant legislation is expected to specify the circumstances under which interferences are provided for. It is also submitted that compliance with Article 17 of the Covenant requires that the integrity and confidentiality should be guaranteed.[17]

Resolution 428 (1970) of the Consultative Assembly of the Council of Europe, which contains the declaration Concerning the Mass Media and Human Rights[18], defines the right of privacy under Article 8 as, consisting in the right to live one's own life with minimum interference. This includes life at home and family, moral physical integrity, honour, reputation, embarrassing facts, unauthorised publication of private photographs, and the disclosure of other confidential information. In the Canadian case of *R v Pohoretsky*[19]*,* Judge Lamer stated that an unreasonable search had occurred, amounting to a violation of the sanctity of a person's body, which is more serious than that of his home. These remarks were made after a blood sample was taken from an unconscious person for purposes of evidence. There has always been a close link between the right to privacy and the admissibility of evidence in court. In

[16] *Ibid.*
[17] *Ibid.*
[18] *Ibid.*
[19] DLR (4th) 699

some cases, evidence obtained unconstitutionally would also be a violation of the right to privacy. For example, reading ones mails without permission or through unauthorised interceptions constitute invasion of ones privacy and evidence obtained in such a manner is likely to be ruled unconstitutional and therefore inadmissible.

However, section 37 (2)(b) of the Criminal Procedures Act 51 of 1977[20] confers upon a registered medical practitioner attached to any hospital the power to take a blood sample of a person if such person's blood may be relevant at any later criminal proceedings. This provision in the Criminal Procedures Act is an example of the possible limitations that may be placed on enshrined rights, which will be fully discussed in this research paper.

In Namibia, Article 13 provides for a general right of privacy together with a direct guarantee of a right to privacy regarding life at home, private communications, as well as the prohibition of unlawful entry and search.[21] The general right to privacy has been dealt with in several cases, although it is yet to see much interpretation in the Namibian courts. In the United States case of *Griswold v Connecticut*[22], the Supreme Court struck down a law which prohibited the use of contraceptives and the provision of medical advice about their use. The defendant had given advice to married couples in respect of the prevention of conception and had prescribed certain contraceptive devices. The court held that the legal prohibition against such conduct violated the right to privacy. Later on, the right to privacy was extended beyond the marital context. In *Eisenstadt v Baird*[23], it was stated that the right of privacy is the right of the individual; both married or single, to be free from

[20] Criminal Procedure Act 51 of 1977: Section 37 (2)(b)
[21] Cachalia, A. 1994. *Fundamental Rights in the New Constitution*. Wits: Juta & Co Ltd, p, 2.
[22] 381 US 479
[23] 405 US 438

unwarranted government intrusion into matters so fundamentally affecting a person.[24]

It should be kept in mind that what a particular society regard as privacy may not be regarded as privacy in another society, which may thus add more uncertainty to privacy. The impact of technology on privacy information is another issue that cannot be ignored. In this day and age, computers have increased, and so are cameras and other electronic devices. Back then, the invasion of someone's privacy usually had to do with someone physically entering another individual's zone, but with technology, privacy may now be easily violated without physical presence. This can be done by hacking into someone's accounts, or tapping their phone calls, and other ways. When such acts are done by an individual with no authority, it shall be seen as a clear invasion of another's privacy. The question then comes in, what if such an individual does so, but with authority of the law, is it still a violation of one's privacy?

When Namibia gained independence, a Constitution came into force.[25] The preamble assures us that the Constitution has been adopted as the fundamental law of the country. The Constitution is therefore the supreme law of the country, and any law that is inconsistent with it must be seen as invalid. The Constitution has a Bill of Rights, which is there to protect democracy, protect the citizens from abuse and at the same time guarantee them the fundamental democratic values of human dignity, freedom and equality. Accordingly, the Constitution must serve as the instrument upon which constitutionality of laws are measured.

Looking at the Namibian Constitution, Article 13(1) of the Constitution states that, "No persons shall be subject to interference with the privacy of their homes,

[24] 453
[25] The Namibian Constitution:1990

correspondence or communications save as in accordance with law and as is necessary in a democratic society in the interests of security, public safety or the economic well being of the country…..” It is good to note down that privacy regarding communications is specifically referred to in Article 13. Conversely, the same article provides for exceptions. This means that under such exceptions, one may be subjected to interference with their privacy. The first exception is when the interference is in accordance with the law. This means that, interference in terms of the Communications Act may be permitted, as it is interference provided for by the law. Such law however has to be necessary in a democratic society, like being in the interest of national security and public safety among others. This leads us to asking the question; was enacting the Communications Act necessary in a democratic society? While some may argue that it was not, it shall not go unmentioned that in today’s world, national security has become a main concern due to an increase in crime and wars. Therefore, it may be argued that the Communications Act was well in line with Article 13, although it must then be established, whether the Act remains at the standards of a democratic society. Although a law may be enacted because of national security, it must be made in a manner that does not compromise the rights and freedoms protected in the Bill of Rights of the Constitution. This paper will then have a brief overview of major cases, where the right to privacy was interpreted, looking at how the cases arouse, the law applied and the court’s ruling.

2.2 Case law on privacy

2.2.1 Copland v United Kingdom[26]

In this case, a college employee during her employment, had her telephone, email and internet use subjected to monitoring by the college. At that time, there was no policy in force regarding such monitoring, and the applicant was never given any warning about such monitoring. Moreover, there were no provisions in the domestic law, or in the instruments governing the institution, regarding the regulation of monitoring of employees. The college's argument for the monitoring was to find out if the applicant was abusing college facilities for personal use. The applicant approached the European Court of Human Rights on the basis that such monitoring amounted to a violation of the respect to her private life and correspondence under Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

It was held that telephone calls and communications from the employment premises were *prima facie* covered by the notion of private life and correspondence, for the purposes of Article 8 (1) of the convention. This was correct, because, the applicant was not prohibited from making calls, or sending emails that are not work related. The applicant was not informed about the monitoring, and she had a reasonable expectation that communications she make at work would be subjected to privacy, like calls one would make at home for instance. The applicant's information regarding the duration of calls and the numbers dialled were kept, thereby also violating Article 8 (1), for storing personal data relating to the private life of the applicant. Based on this, the court found it irrelevant whether such information was used against the applicant or not. The monitoring could only be justified if it was in

[26] 2007 25 BHRC

accordance with the law and necessary in a democratic society. The court provided that the term ‘in accordance with the law’ inferred that there must have been measures of legal protection in domestic law against arbitrary interferences by public authorities with the rights protected under Article 8 (1). It does not only require compliance with a domestic law, but it also looks at the quality of the law to avoid a lack of public scrutiny and to ensure compliance with the rule of law. The court further stated that in order to fulfil the requirement of foreseeability, the law had to be sufficiently clear to give individuals an adequate indication to the circumstances and conditions in which authorities would be allowed to apply such measures. It is important to remark upon the fact that the Telecommunications Regulations Act 2000 was not in force at the time in the *Copland* case. As there was no domestic law regulating monitoring, such interference could not be said to have been in accordance with the law, as Article 8 (2) of the Convention provides for. The court therefore held that it can not exclude that the monitoring of an employees use of telephone, fax and other communications at the place of work may be considered necessary in a democratic society in certain circumstances in pursuit of a legitimate aim.

In the *Copland case*, the court had to look into the law of privacy. At the time the issue arouse, there was no general right to privacy in English law. The applicable Act that provided for interception of communications was not yet in force. This Act had a provision allowing employers to monitor employees’ communications, but they had a duty to inform the employees that there is a possibility that their communications might be intercepted. Having given the importance of the phrase ‘in accordance with the law’, it is also of importance that, although communications may be intercepted, such persons must be informed about such interceptions. Coming back to the

Namibian position, we are now left to ask ourselves, whether the Communications Act ought to have a provision, allowing persons to be informed in case their communications are being intercepted, or might be intercepted. On one hand, it would seem like the whole purpose of interception will fall away if persons are to be informed. For example, a person whose communications are being intercepted because s/he is being suspected of drug dealing may not be informed, as that would then hinder the investigations, and render the interception process useless. In some instances, it would be impossible to inform the people, depending on the nature of the reason behind the need for interception. If information is obtained about certain people conspiring to overthrow the government, a warrant would be quickly granted, information then quickly obtained and arrests are likely to ensue. In such a scenario, it becomes impractical to inform the people to be intercepted. On the other hand, a different view on informing persons whose communications are to be intercepted is that, such persons ought not to be informed because the Act is of general application, and everyone must know that it applies to them and not be told specifically.

In the same case, the court referred to the case of *Malik v Bank of Credit and Commerce International SA (in liquidation)*[27]*,* in which it was held that as a matter of law, it is implied that an employer will not without reasonable and proper cause, conduct itself in a manner likely to destroy or seriously damage the relationship of confidence and trust between the employer and the employee. This principle, can not be ignored as far as national legislation is concerned. In the case of the Namibian Communications Act, the position of the employer and the employee can be implied to the position between the state and the society. The society has

[27] 1997 3 All ER 1

confidence and trust in the government, and such a relationship must not be destroyed. It is upon this argument that it would be advised for governments to promote laws that ensure that the society feels safe and free.

In *Copland,* the government argued that, the interception did not amount to a violation of the applicant's right to privacy, and if it does, it was justified. The argument was that the interception was aimed at protecting the rights and freedoms of others by ensuring that the facilities belonging to the public are not abused. Another argument was that, the interception was necessary in a democratic society as it was only done to establish whether the facilities were being used for personal use or not. It is also of great significance that the court in *Copland* ruled in favour of the applicant, based on the fact that there was no law in place at the time, allowing for lawful interception. This shows us that domestic laws serve an immense duty in ensuring that the people's right to privacy is not infringed upon, and in instances were it might be, justification on such domestic laws must be provided for.

2.2.2 Szuluk v United Kingdom[28]

The case came before the European Human rights court, after the applicant complained that his medical correspondence sent to and by him was being intercepted by the prison authorities. The applicant claimed that his right to privacy was being violated as provided for by Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The court in assessing whether an interference with the exercise of the right of a convicted prisoner was necessary in a democratic society, had to look at the ordinary and reasonable requirements of imprisonment. This is because; some measure of control must always be taken over

[28] 27 BHRC 406

prisoners. It was argued that, despite the nature of the prison's environment, individuals detained also have the right to privacy. This judgment is a clear indication to us that privacy ought to be respected as far as all human beings are concerned.

In the case of *Malone v United Kingdom*, the European Court of human Rights held that the UK was in breach of Article 8, regarding the interception of communications. This was a breach because it was not provided for in any law. To comply with this judgment, the Interception of Communications Act 1985 was enacted. S 7 of this Act allowed any person who suspects that their communications are being monitored to a tribunal which may order that interceptions should be stopped, and damages be paid if necessary. The Act further provided for issuing of warrants in the interest of national security, which is also among the reasons why the Communications Act was enacted in Namibia.

CHAPTER THREE

3. Privacy as a fundamental right and its limitations

3.1 Limitation provisions

In terms of the Bill of Rights, any limitation on a constitutional right must be reasonable and justifiable, in a democratic society. Article 22 (a) of the Namibian Constitution provides that the limitation on any fundamental right or freedom shall be of general application, shall not negate the content thereof, and it shall not be aimed at a particular individual. Subsection (b) states that such limitation must further specify the ascertainable extend of such limitation and identify the articles on which authority to enact such limitation is claimed to rest.

Under the European Convention for the protection of…on Human Rights and Fundamental Freedoms, limitations on the right to privacy are provided for in Article 8 (2). Article 8(2) provides that limitations on the right may only be permitted where they are necessary in a democratic society, in the interest of national security, public safety or the democratic well being of the country, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Article 17 (9) went on to say that state parties are under a duty to not to engage in interferences inconsistent with Article 17. State parties are also expected to make laws prohibiting such interferences.

3.2 The Oakes test

This test was formulated in the case of *R v Oakes,* and it may be used as a primary test in determining if the purpose of a limitation on a right is justifiable in a free and democratic society.[29] In *R v Big M Drug mart Ltd*[30]*,* it was asserted that limitations on rights must be motivated by an objective of sufficient importance. Furthermore, the limitation must minimal as possible.[31] It was asserted that limitations on rights must be motivated by an objective of sufficient importance. Moreover, the limit must be as small as possible. In the *Oakes* case, the court elaborated on the standard and found that David Oakes' rights had been violated as he had been presumed guilty. Such a violation was said not to be justifiable.

As one of the first requirements, there must be a pressing and substantial objective, permitting for such a limitation. Secondly, the means must be proportional, and such means must be rationally connected to the objective. Furthermore, it is required that there must be minimal impairments on the rights, and that there must be proportionality between the infringement and the intended objective. [32] This test is mainly based on analyzing facts and strict adherence should not always be done. A degree of overlap is to be expected as there are some factors, such as vagueness, which are to be considered in multiple sections. If the legislation fails these requirements, it is said to be unconstitutional.[33]

[29] 1986 1 S.C.R. 103
[30] 1985
[31] Available at www.law.ualberta.ca/centres/ccs/rulings/theoakestest.php; last accessed on [20, September 2011].
[32] *Ibid.*
[33] *Ibid.*

In the case of *S and Marper v United Kingdom*[34], the European court of human rights ruled that the storing of data relating to the private life of an individual amounted to an interference with the right to privacy as provided for in the European Convention. Despite this principle, the court went on to state that the right to privacy is subject to the limitation that it may be interfered with by a public authority in accordance with the law and is necessary y in a democratic society for the prevention of disorder or crime.[35] In the learned judge's own words:"the interference was necessary and proportionate for the legitimate purpose of the prevention of disorder or crime and/or the protection of the rights and freedoms of others. It was of vital importance that law enforcement agencies took full advantage of available techniques of modern technology and forensic science in the prevention, investigation and detection of crime for the interests of society generally. They submitted that the retained material was of inestimable value in the fight against crime and terrorism and the detection of the guilty and provided statistics in support of this view. They emphasised that the benefits to the criminal-justice system were enormous, not only permitting the detection of the guilty but also eliminating the innocent from inquiries and correcting and preventing miscarriages of justice."

These arguments did not really convince the European Court however, but it did have more success in the United Kingdom courts, in which the courts went on to rule that interference is justifiable.[36]

---

[34] (Applications no. 30562/04 and 30566/04) (ECtHR 2008-12-04).
[35] *Ibid.*
[36] Curie, I. 2010. *Balancing and the limitation of rights in the South African Constitution*. Johannesburg: University of the Witwatersrand, p, 2.

An example of what may be seen as a violation of privacy is, under the South African Constitution, were it can be argued that retention of DNA data and cellular samples in a forensic database is constitutionally permissible, although it infringes upon ones right to privacy.[37] When one is faced with such a position, one can not help but ask what the Constitution means by the expression 'everyone has the right to privacy'? Author Curie enquires as to what exactly is it that this expression achieves if the right can simply be balanced against the interests of crime detection and prevention and, as the decisions of the UK courts demonstrate, may be outweighed by these policy goals? He further contents that if rights can be weighed against competing public interests justifying their restriction, and if they are sometimes outweighed by those interests, then it is not clear what is gained by having a right.

In *Brümmer v Minister for Social Development*[38] the court gave the following summary in a nutshell of the limitation enquiry: "In assessing whether the limitation . . . is reasonable and justifiable under section 36(1), regard must be had to, among other factors, the nature of the right limited; the purpose of the limitation, including its importance; the nature and extent of the limitation; the efficacy of the limitation, that is, the relationship between the limitation and its purpose; and whether the purpose of the limitation could reasonably be achieved through other means that are less restrictive of the right in question." In conclusion, all these factors ought to be weighed up but eventually the exercise is one of proportionality and involves the assessment of competing interests.

[37] *Ibid.*
[38] 2009 6 SA 323 CC.

3.3 Kauesa v Minister of Home Affairs and Others[39]

The case of *Kauesa* dealt with the limitations of rights as provided for by the Namibian Constitution, in most of its part. The appellant, a warrant officer in the Namibian Police Force, had been a member of a discussion panel of the Namibian Broadcasting Corporation in which the subject of discussion was affirmative action and the restructuring of the police force. As a result of comments that had been made by the appellant during the panel discussion he had been charged with contravening regulation 58(32). Regulation 58(32) provided that (a) member shall be guilty of an offence if he comments unfavourably in public regarding the administration of the force or any other Government department. The appellant had filed an application in the High Court challenging the constitutionality of the regulation through article 21 of the Constitution of the Republic of Namibia. Article 21(1)(a) of the Constitution provides that all persons have the right to freedom of speech and expression, while sub article (2) provides that the fundamental freedoms referred to in sub article (1) hereof shall be exercised subject to the law of Namibia, insofar as such law imposes reasonable restrictions on the exercise of the rights and freedoms conferred by the said sub article, which are necessary in a democratic society and are required in the interests of the sovereignty and integrity of Namibia, national security, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.

The question before the Court was whether the limitations on article 21(1)(a) as set out in article 21(2) were reasonable; freedoms had to be exercised in accordance with the law of Namibia only if that law imposed reasonable restrictions on the

[39] 1996 (4) SA 965 (NMS)

exercise of the rights and freedoms entrenched in article 21(1)(a); they had to be necessary in a democratic society; not only did they have to be necessary in a democratic society but they also had to be required in the interests of the sovereignty and integrity of Namibia, national security, public order, decency or morality, or in relation to contempt of court, defamation or incitement to commit an offence.[40] Limitations were imposed so that the rights enshrined in the Constitution should not interfere with the rights and freedoms of others. The court additionally held that in assessing the extent of the limitations to rights and freedoms the Court had to be guided by the values and principles that were essential to a free and democratic society which respected the inherent dignity of the human person, equality, non-discrimination, social justice and other such values.[41]

The dictum in *R v Oakes*[42] was accordingly approved and applied. The Namibian Constitution in Article 22 recognised the importance and the need to protect the essential content of rights and that the legislation providing for limitations should therefore not be aimed at a particular individual, and it should specify the ascertainable extent of such limitation and identify the article or articles hereof on which authority to enact such limitation is claimed to rest. Additionally, it was held that the onus of proving a limit or restriction on a right or freedom guaranteed by the Bill of Rights was on the party that alleged that there was a limit or restriction to the right or freedom.

Another issue was whether it could be said that regulation 58(32) constituted a permissible restriction on the right to freedom of speech of a serving member of the Namibian Police such as the appellant against performance of his duties and

[40] *Ibid.*
[41] *Ibid.*
[42] 1986 26 DLR (4th) 200 at 225

functions and the composition of the Namibian Police force as a disciplined force. What was important was the fact that limitations to the right of free speech had to be both reasonable and necessary and therefore a stricter interpretation of the restrictions was required. The court pointed out that it was essential that Courts should be strict in interpreting limitations to rights so that individuals were not unnecessarily deprived of the enjoyment of their rights.[43] In this case, the limitation was not rationally connected with its objective, therefore the regulation 58(32) was arbitrary and unfair and its objective was obscured by it's over breadth and could not easily be identified. Because of that, it seemed that there was no rational connection between the restriction and the objective. The limitation was not proportional to the objective so it did not attain the particular effect which was justified by a sufficiently important objective.[44] The importance of this matter was that, in order to live in and maintain a democratic State the citizens had to be free to speak, criticise and praise where praise was due. Silence was not a good ingredient of democracy because the exchange of ideas was essential to the development of democracy.[45]

What we can learn from the *Kauesa* case is that, human rights are of great importance in a democratic society, and they should therefore be protected at all times. Despite that, we are reminded that the same Constitution that protects the rights provides for limitations on the same rights. Such limitations are put up so that rights of other individuals, as well as the entire society are protected. In determining whether such limitations are in line with Article 22, it has to be established that such limitations are of general application and the articles on which authority to enact such legislation is claimed. Interception of communications can be justified on the basis

[43] At 980
[44] *Ibid.*
[45] At 982 G, read with 982-983

that, rights, including privacy can be limited for important reasons such as national security. Such actions may only be permissible if the limitation is reasonable in a democratic society. Determining whether an action is reasonable or not is a matter of looking at what extend the right is restricted. Although it is stated in the Communications Act that no interception may occur without a warrant from a judge, uncertainty exists as to whether monitoring would be occurring through out, while warrants may just be brought in after something suspicious has been discovered during the ongoing monitoring.

Chapter Four

4. The Act in detail

4.1 Provisions of Part 6

Section 70 (1) provides that the President must establish such interception centres as are necessary for the combating of crime and national security.[46] This provision clearly explains the main reason behind the establishment of the interception centres, that the aim is combating crime and for national security. In attempting to ensure that interception centres are not abused, the legislator in Section 70 (3) provided that any staff member, before performing any function relating to interceptions must take an oath before the Judge-president in chambers.[47] Under the oath, the staff member makes a promise to perform his duties in accordance with the law of Namibia. The oath stands to ensure that no one carries out an unlawful interception, which is otherwise contrary to the laws of the country.

Section 75 lays down the penalty for contravention of the regulations regarding interceptions according to the Act. Anyone who is convicted may be liable to a fine of N$ 100 000 or ten years imprisonment, or both.[48] This section must be seen as one of the attempts by the legislator to ensure that interceptions of communications is not abused, and only made with the aim or reason of which such information was intended. Staffs members who are to be penalised are those who reveal information that may not provide the information sought, use the information for other purposes other than for which it was intended, or provide information that is not part of the

[46] Section 70(1)
[47] Section 70 (3)
[48] Section 75

lawful interception or monitoring. The provisions are broad enough that they also include employees of service providers who may assist in intercepting communications.[49]

Section 76 provides for a penalty of N$ 20 000 or five years imprisonment or both, to any person who is in possession, or deals in equipment as prescribed in the Act.[50] The equipment is those to be used for interception and monitoring, or those that may be used in preventing lawful interception. This provision is to ensure that no one will be able to carry out interceptions, or prevent them, apart from the authorised authorities. In this way, the Act protects the society from unlawful interceptions, that may be carried out by individuals or entities not authorised to do so.

The interception of communications, on the face of it, presents a threat to privacy. This argument is nonetheless countered by the argument that the state on the other hand, has a duty to preserve national security, and at the same time help in detecting and preventing crime.[51] As such, state action would be an attempt to maintain and protect democracy and peace, and it is important that the same concept being protected is not encroached upon. This is to say, if the state's attempt is to protect peace and democracy, it would not be of any use, if in that same process, an individual's right to privacy is violated. This perhaps also draws us to the question of who is seen as most important, between individuals and the state. If one compares the two, it is evident that the state includes the well being of everyone, as opposed to an individual, who only comprises of himself. However, it should not be forgotten that, it's those same individual's, who make up the state as a whole. Therefore, even if the state may seem more important than individual's, it would not

[49] Section 75 (d)
[50] Section 76
[51] *Ibid*.

be advisable to undermine their rights as in the end, it does not make sense trying to protect a right at the hands of constantly violating another equally important right. As far as the 20th century, telephonic interceptions could be made, but facilities have since then improved significantly.[52] Although interception methods have been improving, and thus helping in combating crime, the protection of privacy has not been given much attention. Author Fenwick provides that before 1985, there were no requirements pertaining to procedures to be done when taping a phone call. [53] In 1985, The Interception of Communications Act 1985 was introduced, due to the ruling of the European Court of Human Rights in *Malone v UK*[54], that the procedure that was in place violated the right to privacy. The decision was induced by the fact that domestic law that existed did not among others, provide for any remedies against abuse of such communications tapping. This meant that, such tapping did not therefore fall under the phrase 'in accordance with the law', as provided for in Article 8 (2). As technology improved, the Act became inadequate, and a new Regulation of Investigatory Powers Act 2000 was introduced.

Authors Britz and Ackerman formulate that even in a constitutional democracy the right to privacy can never be absolute.[55] In South Africa, legislation is in place allowing for searches of property, as well as interceptions of communications like emails and telephone calls, thereby overriding the right to privacy of the individual. Although interception of communications allow for an infringement on the right to privacy, it must be noted that, such is only permitted in accordance with the laws put in place, both in Namibia and South Africa. For that reason, the purpose of such interceptions must be clearly stated. An important aspect that needs to be made

[52] Fenwick, H. 2002:670
[53] *Ibid*.
[54] 1979 Ch 344.
[55] Britz, H, Ackerman, M. 2006. *Information, Ethics & the Law*. Pretoria: Van Schaik Publishers, p. 18.

clear is the difference between interception and monitoring, and which one will be applied. Interception is described as the process were the interceptor takes cognisance of the content of one's communication, while monitoring is when the monitor observes who is contacting who.[56] In short, interception refers to instances where the interceptor only views a certain communication, for example, trying to find out something, as opposed to monitoring, were there is someone who is viewing whatever is going on around someone. Due to the reason that interception involves ones right to privacy, it is important to make it clear on which interceptions are lawful.

4.2 The Namibian Act compared to South Africa's Act

As Namibia's legal system is closely related to the South African one, it would be good to compare the positions in both countries. In South Africa, the Regulation of Interception of Communications and Provision of Communication-related Information Amendment Act (48 of 2008 (the Amendment Act)) came into force on July 1 2009, as an amendment to the Regulation of Interception of Communications and Provision of Communication-related Information Act (70 of 2002.[57] According to the Department of Justice and Constitutional Development, the purpose of the Amendment Act is to help in assisting the law enforcement agencies to carry out their duties efficiently.[58] These duties include investigating crime and locating criminals using cellular phones. The Act was to operate in a manner that information of cellular phone users was to be obtained by the service providers. The service providers thus have a duty to capture such information of its users, and that the SIM cards of which information could not be captured must be terminated thereof. As the

[56] *Ibid*, p.95
[57] Machabaphala, T, Sikhakhane, M. 2009. *Legal eavesdropping and the consequences*. Available at www.withoutprejudice.co.za; last accessed on [14, October 2011].
[58] *Ibid*, p, 20.

Act provides for penalties in case of non compliance, it is important that individuals, as well as service providers know their obligations. Service providers are expected to provide correct and accurate information, while consumers are expected to avail such information. The Namibian Act is expected to operate in this same manner, capturing information of cellular phone users.

The South African Act briefly outlaws the unauthorised; interception of communications, provision of communications related information, disclosure of information for purposes other than that for which it was obtained and manufacturing of certain equipment.[59]The above mentioned Act provides that a judge of the High Court may authorise for interception, and order that service provides give certain information. Again, these provisions in the South African Act are similar to the one in the Namibian Act. As the two Acts are similar, elements to be considered in determining whether there was unlawful interception or not, ought to be the same. The four elements to be given attention are as follows:

Authorisation: both positions are that, unless the Act provides otherwise, interceptions allowed are only those authorised by a designated judge on the grounds given by the Act. This means that a private investigator who intercepts a communication without such authorisation commits an offence. In Namibia, this would not only apply to a private investigator, but it would also include an employee of the interception centres, who carries out an interception with no order from the judge.

Intention: It should be known that an act of interception must be intentional, and someone who comes across a communication by accident commits no offence. [60]

[59] as noted by Britz & Ackerman.
[60] Britz, H, Ackerman, M. 2006:97

However, such accident is not an offence only if such person stops the act, as soon as he realises that s/he is intercepting a communication. If such persons nevertheless continue with the interception, then the intention comes in and they may be liable of an offence.[61]

Communication: The South African Act sees the term communication as referring to direct and indirect communications. Direct communications is described as an oral communication between two or more people who are at the same place, while indirect communications refer to the transfer of information in any form by means of telecommunications.[62]

Interception: The South African Act provides that an interception is the aural or other acquisition of the contents of any communication through the use of any means, with the purpose making such content available to someone other than the person sending or receiving such contents.[63] Such interception however includes monitoring, for example listening, viewing or inspecting of indirect communications.

Due to considerations of privacy, it is reassuring, that a judicial officer is present to avoid abuse among others. Permitting a judge to decide when a warrant of interception must be issued means that the judge will exercise his discretion, and make a reasonable and just conclusion. A reasonable judge would not allow for an interception if in his opinion, it cannot be justified that such a warrant be issued. One of the main concerns is however that, it is possible that an interceptor may be monitoring communications without authority, and because of such interceptions, obtains further evidence that he then may approach the judge with. If this was to

---

[61] *Ibid.*
[62] *Ibid*.
[63] *Ibid.*

happen, how would one know that an unlawful interception took place before the lawful interception? Although that may help in combating crime for instance, it is on the other hand violating ones privacy. If this was to happen, it would mean that whatever one does, is being monitored by interceptors, who are waiting to see any suspicious information, before going to obtain an order. One of the main arguments that the Namibian Communications Act would not be a threat to privacy is that, only lawful interceptions are allowed. We are however faced with a problem, if an unlawful interception is to occur. The question is how would anyone ever find out that an unlawful interception was done? The only time one would know that an interception actually occurred is when arrests, for example, are made, and it then appears in court that evidence was obtained through interceptions. At such a stage, the accused would not be able to challenge the unlawfulness of the interception, as the one being used in court was the lawful one, but which might have been obtained as a result of information obtained through an unlawful interception.

Given the nature of telecommunications and the advanced technology, it would be difficult if impossible to ever detect any unlawful interceptions. One way in which the process would be made transparent is if an independent telecommunications company was to serve as an auditor so to say, of the communications centres, and any other firms authorised to intercept. Their duty would be to monitor what communications have been intercepted on which dates, and whether such interceptions can be matched with any interception orders granted on that same date.

Another issue might also be on the basis of interceptions. As stated earlier, interceptions may help in combating crime and protecting the state and its interests. Given the fact that only lawful interceptions are permitted, that would mean, it is

likely that any lawful interceptions to be carried out are regarding persons who are already arrested, or who have raised alarm in another manner, not being through telecommunications. If interception was to be the first source of information that a certain illegal act is going on, it would mean that interceptors were monitoring people at random, or certain individuals, in search of information linked to certain activities. If that was to be the case, it would also mean that such interceptors may in the process come across information such as people's marital affairs, which ought to be private matters. Although the right to privacy cannot be absolute, citizens must be guaranteed that their communications will not be intercepted all the time and at random. Let's have a look at a scenario, were a thief calls someone abroad and organises on how to bring illegal equipment in the country. Given the provisions of Part 6 of the Communications Act, would the interception centres help in capturing this thief? The answer is no. This is because; there was nothing more done, apart from the single call made. If such a thief is then to be arrested, one would wonder how it would have happened. The possibility would be that, if such a thief was to be caught, most, if not all communications were being monitored at random and in the process coming across such information. The possibility would then be that, further evidence would be obtained from the thief's premises for example, warranting the need for the authorised order, which would then validate the initial communication which was actually obtained unlawfully. Given this argument, one may thus question whether the provision of lawful interceptions really makes any difference.

If interception centres abide by the Act and only do interceptions when authorised to do so, it would be good, as people would be free to communicate willingly, knowing that no one is viewing or listening to their discussions. Interceptions may also be abused, for instance, whereby one would intercept his partner's communications.

What then happens if he finds out that his partner is cheating? As a human being, one would be tempted to confront her, which might even end up in divorce. In this case however, the Act is clear on someone who uses information for purposes which were not intended for, and provides fines and/imprisonment under Section 75. It would however be hard to prove that the interceptor found out about the extra affair though unlawful interception, and he is likely to deny it himself knowing that it was an illegal activity. The South African Act provides a maximum sentence of R 2 Million or ten years imprisonment, which is very high as compared to the Namibian penalty.

CHAPTER FIVE

5. Conclusion and Recommendations

Privacy is seen as a basic human need which is needed in developing, as well a maintaining a free, mature and stable personality of a human being.[64] The right to privacy is an internationally acclaimed right, which is respected and protected in any given society. Despite its importance, the right to privacy is said to have no definition, which some fear might bring about uncertainty regarding its interpretation and enforcement. In Namibia, the right to privacy is provided for by Article 13 of the Constitution, which outlaws interference with personal communications. However, even in a democratic society, such a right cannot always be absolute. Fundamental Rights and Freedoms, although entrenched, are subject to limitation by virtue of Article 13 itself, provided that such interference falls within the given justifications. Any interference that is seen as necessary in a democratic society or in the interest of national security should fall within the bounds of Article 13. Moreover, such interference will also have to comply with Article 22, that it is of general application and not aimed at an individual. As author Jeffery contents, no right is absolute, and the right to privacy is limited to rights accruing to other citizens.[65] As to the question of wether Part 6 of the Communications Act is an infringement to the right to privacy, the answer lies in wether Part 6 meets the requirements of Article 13 (1) and Article 22. Determining the requirements laid down in Article 13 is a complicated process, as subjectivity plays a big role. For example, what is necessary and reasonable in a democratic society is a broad phrase, and different people may see it differently. Also, if one says, in the interest of national security; does it mean taking

[64] Devenish, GE. 1999. *A commentary on the South African Bill of Rights.* Durban: Butterworths, p, 135.
[65] Jeffery, A.1997. *Bill of Rights report*. Johannesburg: SA Institute of Race Relations: p, 50.

precautionary measures even when there is no threat, or is national security better protected when there is chaos? Such broad contexts in which these elements fall makes it a bit hard for us to specifically point out wether Part 6 infringes upon the right to privacy. Regarding Article 22 (1), it is perhaps fairly clear that Part 6 or the Act itself was not aimed at a particular individual. As to Article (2), authority upon which legislation was enacted would be Article 13 (1), although it is hard to ascertain to what extend the right was limited.

Privacy is enshrined in the Constitution, but can be limited as long as the limitations are not discriminatory, aimed at an individual, or unreasonable in a democratic society. Part 6 was enacted to fight crime and enhance national security, and not to necessarily view people's private information. In addition to the already existing safeguards, the government should look into reviewing the Act, and clarify issues like, the monitoring of the staff who will be responsible for monitoring and interceptions. Another unclear issue is the differentiation between monitoring and interception, and which one would be employed at what times. It would be advisable not to have any full time monitoring going on, or it will pose a big risk to the right to privacy. It must also be ensured that after the warrant time has lapsed, interceptions must also stop.

It is recommended that an independent body is created, or given the task to monitor or audit the activities of the interception centres. This would ensure that only lawful interceptions are done, and at the time the orders are given, and not have a situation where communication are intercepted or monitored before a warrant is given by the judge. The fine may as well be considered, as it is at the moment low. Having the fine increased would ensure that staff members at the interception centres only carry out their functions, and not indulge in acts not provided for in their duties.

It would also be good, if an effort is made to explain the main aim of the Act to the public, in simple terms they can understand, that it is aimed at preserving national interest and help fight crime. Explaining the Act to the public, as well as the measures put in place to avoid abuse would ensure that the public understands why such legislation was enacted, and know that it was aims to protect their overall interests. One fact however remains, the Act should be seen as enacted within the bounds of the Namibian Constitution, unless it can be proved unreasonable by a court of law.

Bibliography

Books

Barendt, E. 2001. *The International Library of Essays in Law & Legal Theory: Privacy*. Aldershot: Dartmount Publishing Company

Britz, H, Ackerman, M. 2006. *Information, Ethics & the Law*. Pretoria: Van Schaik Publishers

Cachalia, A. 1994. *Fundamental Rights in the New Constitution*. Wits: Juta & Co Ltd

Curie, I. 2010. *Balancing and the limitation of rights in the South African Constitution*. Johannesburg: University of the Witwatersrand

Davies, D. 1997. *Fundamental Rights in the Constitution*. Cape Town: Juta & Co

Devenish, GE. 1999. *A commentary on the South African Bill of Rights.* Durban: Butterworths

Fenwick, H. 2002. *Civil Liberties and Human Rights*. Cavendinish Publishing: London

Jeffery, A.1997. *Bill of Rights report*. Johannesburg: SA Institute of Race Relations

Lloyde, I. 2000. *Legal Aspects of the Information Society*. London: Butterworths

Michael, J. 1994. *Privacy and Human Rights*. Paris: UNESCO Publishing

Norberto, B. 1996. *The Age of Rights.* London: Polity Press

Statutes

The Constitution of the Republic of Namibia Act 1 of 1990

Communications Act No.8 of 2009

Telecommunications Regulations Act 2000

The Interception of Communications Act 1985

Regulation of Investigatory Powers Act 2000

Regulation of Interception of Communications and Provision of Communications-related Information Act No.70 of 2002.

Treaties

European Convention on Human Rights and Fundamental Freedoms of 1950

General Comment N0. 16: The Right to Respect of privacy, family, home and correspondence, and protection of honour and reputation (Art 17): 04/08/1988

International Covenant on Civil and Political Rights of 1966

Resolution 428 (1970) of the Consultative Assembly of the Council of Europe

Universal Declaration of Human Rights of 1948

Websites

www.law.ualberta.ca/centres/ccs/rulings/theoakestest.php

www.withoutprejudice.co.za

Cases

Brümmer v Minister for Social Development 2009 6 SA 323 CC

Kauesa v Minister of Home Affairs and Others 1996 (4) SA 965 (NMS)

Malik v Bank of Credit and Commerce International SA (in liquidation) 1997 3 All ER

Malone v UK 1979 Ch 344

Olmstead v United 277 US 438 1928

R v Oakes (1986) 26 DLR (4th) 200

R v Pohoretsky DLR (4^{th}) 699

S and Marper v United Kingdom ECTHR 2008

Szuluk v United Kingdom 27 BHRC 406