

Interception of communication by South African government agencies *vis-a-vis* the right to privacy: The law and the practice in light of the South African Constitution and the International Convention on Civil and Political Rights (ICCPR)

**A mini-thesis submitted to the Law Faculty of the University of the Western Cape in partial fulfilment for the LL.M**

**Supervisor: Prof Benyam Dawit Mezmur**

**Natsinet Tesfaye Fesehaye  
(3101940)**



UNIVERSITY *of the*  
WESTERN CAPE

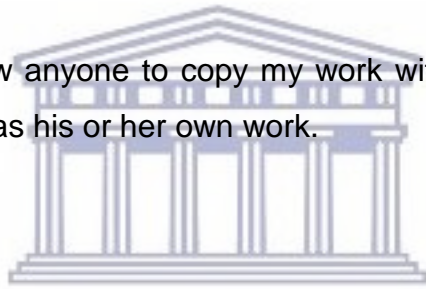
**November 2017**

## DECLARATION

I, **Natsinet Tesfaye Fesehaye** (Student No 3101940) declare as follows:

1. I understand what plagiarism entails and am aware of the University's policy in this regard.
2. This dissertation is my own, original work. Where someone else's work has been used (whether from a printed source, the internet or any other source) due acknowledgment has been given and reference made according to the requirements of the Faculty of Law.
3. I did not make use of another student's work and submit it as my own.
4. I did not allow anyone to copy my work with the aim of presenting it as his or her own work.

Signature:



Date:

UNIVERSITY of the  
WESTERN CAPE  
November 2017

## **Acknowledgments**

I am greatly indebted to my supervisor Prof Benyam Dawit Mezmur. This work would not have come to its successful completion without his meticulous supervision. He was ready to respond to my endless questions, all the time. His friendliness made working under his supervision all the more enjoyable.

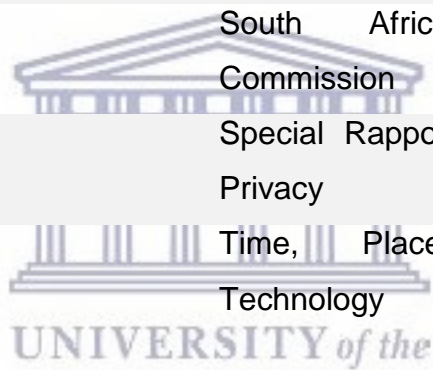
Special thanks go to my eldest brother who made it possible for me to study at the UWC. He helped me throughout the last seven years by constantly following my progress and, despite his busy schedule, always sparing time to explain things that I found difficult to understand.

I would not have been where I am now if it was not for my father Tesfaye Fesehaye and my mother Elsa Tesfaye. They were there for me and my siblings in the best and worst of times. They helped us overcome countless challenges that life threw at us. No word can express how grateful I am to them. All I can say is thank you very much Mom and Dad, and I love you immensely. I would like also to thank my sister Milena Fesehaye, my brothers Abraham Fesehaye and Aklilu Fesehaye for their love, support, and constant encouragement.

## Acronyms

<b>ACHR</b>	American Convention on Human Rights
<b>CRC</b>	The Convention on the Right to the Child
<b>ECA</b>	Electronic Communications Act
<b>ECHR</b>	Electronic Communications and Transactions Act
<b>EUCJ</b>	European Union Court of Justice
<b>FICA</b>	Financial Intelligence Centre Act
<b>IMPA</b>	Interception and Monitoring of Communication
<b>ICASA</b>	Independent Communications Authority of South Africa Act
<b>ICCPR</b>	International Covenant on Civil and Political Rights
<b>ICRMW</b>	International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families
<b>HRC</b>	Human Rights Committee
<b>HRW</b>	Human Right Watch
<b>NCC</b>	National Communication Centre

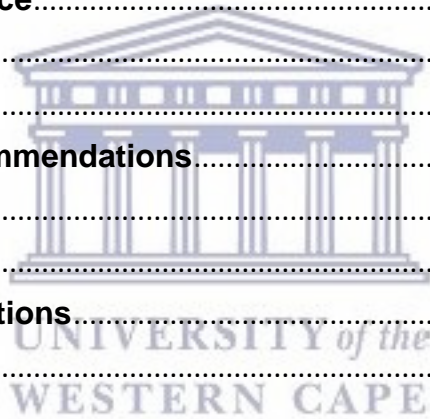
<b>NSA</b>	National Security Agency
<b>MPDP</b>	Media Policy and Democracy Project
<b>PCCAA</b>	Prevention and Combating of Corrupt Activities Act
<b>PCDTRA</b>	Protection of Constitutional Democracy against Terrorism and Related Activities Act.
<b>RICA</b>	Regulation of Interception of Communication Act
<b>SALC</b>	South African Law Reform Commission
<b>SRP</b>	Special Rapporteur on the Right to Privacy
<b>TPET</b>	Time, Place, Economy and Technology
<b>UDHR</b>	Universal Declaration of Human Rights



## Contents

<b>Acknowledgments</b> .....	3
Acronyms .....	4
<b>Chapter 1</b> .....	1
<b>Introduction</b> .....	1
<b>1.1. Background</b> .....	1
<b>1.2. Research question</b> .....	5
<b>1.3. Literature review</b> .....	5
<b>1.4. Methodology</b> .....	6
<b>1.5. Structure of the study</b> .....	7
<b>Chapter 2</b> .....	8
<b>The right to communication privacy under ICCPR and South African Constitutions: Meaning and Scope</b> .....	8
<b>2.1. Introduction</b> .....	8
<b>2.2. The conception of the privacy</b> .....	8
<b>2.3. Why is privacy a right?</b> .....	11
<b>2.4. Privacy and state surveillance in the digital age</b> .....	13
<b>2.5. The right to privacy under South African Constitution</b> .....	17
<b>2.5.1. Limitations on the right to privacy</b> .....	20
<b>2.6. The right to privacy under Article 17 of ICCPR: Meaning and scope</b> .....	22
2.6.1. Legality .....	25
2.6.2. Necessity .....	27
2.6.3. Proportionality .....	29
2.6.4. Procedural safeguards .....	30
<b>2.7. Conclusion</b> .....	31
<b>Chapter 3</b> .....	33
<b>Interception of Communication under RICA</b> .....	33
<b>3.1. Introduction</b> .....	33
<b>3.2. The global and national security context leading to the enactment of RICA</b> .....	33
<b>3.3. History of Interception of communication in South Africa</b> .....	36
<b>3.4. Regulation of Interception of Communication Act (RICA) in brief</b> 40	
3.4.1. Interception defined .....	40

3.4.2.	Principle in the RICA on interception of communication.....	42
3.5.	Interception of communication with 'interception direction' .....	47
3.5.1.	Procedure of securing interception direction .....	49
<b>3.6.</b>	<b>Conclusion</b> .....	50
<b>Chapter 4</b>	.....	52
<b>RICA and its implementation in the light of Legality, Necessity and Proportionality</b>	.....	52
4.1.	<b>Introduction</b> .....	52
4.2.	<b>Restriction of communication privacy under RICA: Legal, necessary and proportional?</b> .....	53
4.2.1.	<b>Legality</b> .....	53
4.2.2.	Necessity .....	58
4.2.3.	Proportionality .....	59
4.2.4.	Procedural safeguards .....	63
4.3.	<b>RICA in practice</b> .....	66
4.4.	<b>Conclusion</b> .....	70
<b>Chapter 5</b>	.....	71
<b>Conclusion and Recommendations</b>	.....	71
5.1.	<b>Introduction</b> .....	71
5.2.	<b>Conclusion</b> .....	71
5.3.	<b>Recommendations</b> .....	75
<b>Bibliography</b>	.....	77

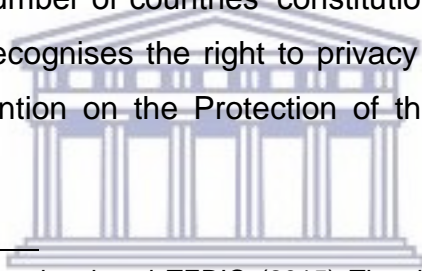


# Chapter 1

## Introduction

### 1.1. Background

The right to privacy is recognised as one of the most important individual rights. It is considered to be central to the protection of one's human dignity. It also forms the basis of any democratic society. Furthermore, it is linked to other basic rights, including the rights to freedom of expression and of association.<sup>1</sup> The right to privacy is contained and recognised in almost every constitutional bill of rights and major international and regional conventions.<sup>2</sup> It is also guaranteed expressly in the Universal Declaration of Human Rights,<sup>3</sup> the European Convention on Human Rights,<sup>4</sup> the American Convention on Human Rights<sup>5</sup> and a number of countries' constitutions.<sup>6</sup> The Convention on the Right to the Child recognises the right to privacy of the child.<sup>7</sup> Moreover the International Convention on the Protection of the Rights of All Migrant



---

<sup>1</sup> Submitted by Privacy International and TEDIC (2015) The right to privacy in Paraguay, Universal Periodic Review Stakeholder Report: 24th Session, Paraguay.

<sup>2</sup> African (Banjul) Charter on Human and Peoples' Rights is conspicuously silent on the right to privacy. The word privacy is not mentioned in the Charter. Lucinda Patrick-Patel argues that the failure to include the right to privacy in the charter emanates from the 'normative flaws' of the Charter which is based on 'strong emphasis on social, economic and cultural rights and the inadequate coverage of civil and political rights'. L Patrick-Patel 'The African Charter on Human and Peoples' Rights: how effective is this legal instrument in shaping a continental human rights culture in Africa?' *Le Petit Juriste* 21 December 2014 <https://www.lepetitjuriste.fr/droit-compare/the-african-charter-on-human-and-peoples-rights-how-effective-is-this-legal-instrument-in-shaping-a-continental-human-rights-culture-in-africa/> last accessed on 10 March 2018.

<sup>3</sup> Art 12 Universal Declaration of Human Rights, 1948.

<sup>4</sup> Art 8 European Convention on Human Rights, 1950.

<sup>5</sup> Art 11 American Convention on Human Rights, 1969.

<sup>6</sup> Most notably the right to privacy is not expressly recognized in the US Constitution. Some of the drafters of the US Constitution, including James Madison, were concerned about the non-inclusion of the right to privacy in the Bill of Rights. Several amendments have been introduced to the Constitution to assuage such fears. The first amendment recognised the privacy of the homes against demands that it be used to house soldiers. The third amendment protects one's person and his or her possession against undue search and seizure. The fourth amendment provides 'the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath fifth amendment'. The ninth amendment provides states that the Bill of right is not exhaustive and the enumeration of those rights in it does not mean other rights are not respected. Some judges have used this clause to interpret the constitution and protect different aspects of the right to privacy.

<sup>7</sup> Art 16 The Convention on the Rights of the Child (CRC).



Workers and Members of their Families provides similar right to migrant workers and their families.<sup>8</sup>

More importantly for purpose of this paper, the ICCPR, under Article 17 provides that everyone should be protected from 'arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation'. It adds that national law should provide everyone a protection from the violation of his or her rights to privacy. Further Article 17(2) requires the provision of legal protection to everyone against interference into his or her privacy whether the threat comes from states authorities, natural person, or legal person. Article 17 imposes an obligation upon the state to adopt legislative and other measure in order to prevent any kind of interference into the right to privacy of, as well as for the protection of the right, under all circumstances.<sup>9</sup> Section 14 of the Constitution which states that everyone has the right to privacy which includes the right not to have, their person, home or property searched, their possession seized or the privacy of their communications infringed.<sup>10</sup>

The right to privacy is not an absolute right. A certain level of limitation can be imposed on this right. This is explicitly stated under section 36(1) the Constitution which provides the right to privacy, like other rights in the Bill of rights, can be limited. The limitation of course has to be done in terms a law of general application and has to be restricted 'to the extent that the limitation is reasonable and justifiable'.<sup>11</sup> The reasonableness and justifiability of the limitation is evaluated in light of 'an open and democratic society based on human dignity, quality and freedom, taking into account the relevant factors including the nature of the right, the importance of the purpose of the

---

<sup>8</sup> Art 14 Convention on the Protection of the Right of All Migrant Workers and Members of Their Families (ICRMW).

<sup>9</sup> Office of the High Commissioner for Human Right *CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation* (Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988).

<sup>10</sup> Section 14 of the Constitution of Republic of South Africa 1996 (hereafter "the Constitution").

<sup>11</sup> Section 36(1) of the Constitution of 1996.

limitation, nature and the extent of the limitation, the relation between the limitation and its purpose and less restrictive means to achieve the purpose'.<sup>12</sup>

The South African surveillance law, formally referred to as the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) of 2002, seeks, among other things, to impose limitation on the right to privacy of individual citizens and residents of the country. It in particular seeks to limit the right to communication privacy of citizens and residents of the Republic since it authorises the South African government to intercept personal communications of citizens and residents of the country under certain circumstances.

This Act is seen by some to be too intrusive and in violation of the right to privacy of individuals, which is protected under the ICCPR and the South African Constitution.<sup>13</sup> Moreover, the relevant South African agencies allegedly abuse the power that they are given under this and other Acts and monitor, record, read personal communication. Hence three right groups - Privacy International, Right2Know, and the Association for Progressive Communications submitted joint report to the Human Right Committee on surveillance and privacy issues in the country.<sup>14</sup>

The organisations brought their concerns to the Human Right Committee.<sup>15</sup> The allegation is that the South African government and intelligence and law enforcement agencies conduct surveillance in a manner contrary to Article 17 of the ICCPR, and in violation of the right to privacy South African citizens and residents.<sup>16</sup> The organisations alleged that the National Communication Centre (NCC) has been collecting information on behalf of the intelligence agencies.<sup>17</sup> Referring to the findings of Ministerial Review Commission on

---

<sup>12</sup> For more on this see Chapter 3. Section 36(1) of the Constitution of 1996.

<sup>13</sup> Right to Know Campaign Submission *in advance of the consideration of the periodic report of South Africa* Human Rights Committee, 116th Session, 2016. (PAC).

<sup>14</sup> *Ibid.*

<sup>15</sup> Privacy International, Association to Progressive Communication (APC) & Right to Know Campaign Submission *in advance of the consideration of the periodic report of South Africa* Human Rights Committee, 116th Session, 2016.

<sup>16</sup> *Ibid.*

<sup>17</sup> *Ibid.*

Intelligence in South Africa (also known as Mathew Commission), the organisations alleged that the NCC has been carrying out mass surveillance and intercepting communication on behalf of the intelligence agencies. According to the Mathew Commission, the NCC is capable of illegally conducting a wide and massive monitoring of telecommunications including conversation, text messages, emails and other data. Such mass surveillance, they allege, is unlawful and unconstitutional as it falls short of the requirements that are set out under RICA.<sup>18</sup> Most importantly for the purpose of this paper, these are forbidden acts under the Article 17 of the ICCPR.<sup>19</sup>

Moreover, not only does the NCC have immense capacity to undertake mass interception of communications, according to White, no law has ever governed the agency's conduct of interceptions.<sup>20</sup> All attempts to regulate the NCC and its activities under the State Security Agency during the general intelligence Laws Amendment Bill had failed. As the result the attempt to regulate NCC by some kind of statutory law was blocked.<sup>21</sup>

Furthermore, the three organisations referred to above allege that the RICA itself is too invasive.<sup>22</sup> The grounds for obtaining direction of interception from the courts are vaguely worded under section 29 of RICA. This, according to the three organisations, has allowed the state agencies to easily obtain interception directions for trivial reasons. Moreover, RICA, under section 30(1) (b), requires communication services providers to store all communication data for about five years. For the right groups, allowing the communication services providers mass communication data retention results in interference with the right to privacy without reasonable ground.

---

<sup>18</sup> Ministerial Review Commission on Intelligence *Final Report to the Minister for Intelligence Services, the Honourable Ronnie Kasrils, MP* (10 September 2008).

<sup>19</sup> *Ibid.*

<sup>20</sup> White V. (undated) *A 21ST century quagmire: Surveillance laws and international laws human rights norms.*

<sup>21</sup> Mail & Guardian, *Say nothing – the spooks are listening*, 18 December 2015 (available at: <http://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening>) Accessed on 18 April 2016.

<sup>22</sup> Privacy International, Association to Progressive Communication (APC) & Right to Know Campagna Submission (2016).

The other fear of the right groups is that there are two Bills that are being processed i.e. The Cybercrimes and Cybersecurity Bills. If these Bills are adopted and enacted as drafted they will further threaten the respect and protection of the right to privacy of South African citizens, as well as the right to freedom of expression and association.<sup>23</sup> The other concern of the organisations is that one cannot defend the disclosure of information based on public interest. Not informing the user after a warrant issuing as disclosure of information is prohibited in terms of the relevant section of RICA.<sup>24</sup>

## 1.2. Research question

Against this backdrop, this study raises the question that; is the RICA and its implementation in line with the Article 17 of the ICCPR and Section 14 of the South African Constitution?

With the view to answering the main question, the study raises several sub-questions including

- What limitation can legitimately be imposed on the right to privacy in general, the right to communication privacy in particular, of individuals?
- What is the extent of the limitations that the RICA seeks to impose on the right to privacy?
- Is the RICA too intrusive viewed in light of the ICCPR and the Constitution?

## 1.3. Literature review

There is hardly any academic work dealing with the RICA or that evaluates the RICA and the practice of interception in light of international human rights conventions. Even worse there is hardly any academic writing linking RICA to the right to privacy as recognised in the ICCPR and the South African Constitution.

---

<sup>23</sup> Right2Know Campaign *Preliminary Position on the draft Cybercrimes and Cybersecurity Bill* (30 November 2015).

<sup>24</sup> *Ibid.*

Russel Luck in his three-page paper titled *RICA: Walking a fine line between crime prevention and protection of rights*, warns that RICA can be used to abuse people's rights, including their right to privacy.<sup>25</sup> However this can hardly be considered as extensive academic work on the matter.

The gap in the existing knowledge on the specific issue that this paper intends to deal makes the undertaking worth the while. There is a report by the Global Information Society Watch 2014. The report which is titled *Communications surveillance in the digital age* discusses on the practice of interception in South Africa based on investigative reports.<sup>26</sup> The discussion is not however framed within the international human right discourse.

A report by the Right to Know titled *The Surveillance State Communications surveillance and privacy in South Africa* deals with the issue of interception. However, there is only a passing discussion on the constitutional and human right implications of the matter. Pierre de Vos in his constitutionally speaking blog discusses the constitutionality of RICA. The discussion is indeed limited to the constitutional aspect of RICA and does not include the international human rights aspect.<sup>27</sup>



#### 1.4. Methodology

The study will be undertaken based on desktop review of relevant laws, court cases, international conventions, and academic writings.

#### 1.5. Scope of the study

As mentioned in the background section, the right to privacy is recognised in almost all international and regional human right conventions and bill of rights of many national constitutions. The meaning that are attached to the concept of privacy and the degree of protection that the right to privacy enjoys varies

---

<sup>25</sup> Luck R. (2014) *Walking a fine line between crime prevention and protection of rights*.

<sup>26</sup> Global information Society Watch (2014), *Communications surveillance in the digital age*

<sup>27</sup> De Vos P. (2011), RICA: Is it unconstitutional?

Available at <https://constitutionallyspeaking.co.za/rica-is-it-unconstitutional/>. Accessed on 23 June 2016.

depending on the international or regional human rights instruments or national constitution in question. This study does not intend to investigate all international and regional human rights instruments on the protection they accord to the right to privacy. The discussions in the study, as the title of the study clearly indicates, are limited to the right to privacy as recognised in ICCPR and the South African Constitution. Other international human rights instrument will be mentioned in the study only to illustrate certain points.

### **1.5. Structure of the study**

The study has five chapters including this chapter.

Chapter two discusses the meaning of the right to privacy and both under international law the South African Constitution. It further deals with the arguments regarding why it is imperative that this right is protected and whether and when the right to privacy can justifiably be limited. It deals with interception of communication as an exception to the right to communication privacy. It discusses why interception of communication is necessary and when it is justified. Based on court cases and practices of democratic countries, it discusses how interception of communication is balanced with the right to privacy and the criteria for doing so.

Chapter three discusses RICA, what it is, what kind of interception it allows and the limitations on the interception it allows. Chapter four examines the appropriateness of the interception allowed under the RICA in light of international human rights law and practice and the South African Constitution. Chapter five is the concluding chapter, which summarises the findings of the study and highlights the lessons drawn from the study.

## Chapter 2

### The right to communication privacy under ICCPR and the South African Constitution: Meaning and Scope

#### 2.1. Introduction

As was indicated in chapter 1, this study aims at investigating whether the RICA and the manner of its implementations are in line with the Article 17 of the ICCPR and Section 14 of the South African Constitution. Before dealing with the issue of whether or not the RICA, both the law and the practice, violates the right to privacy, specially communication privacy, of individual citizens and residents of South Africa, it is necessary to identify the meaning and scope of the right to privacy in general and as provided in the two-instrument mentioned above. It is also necessary to discuss the justifications for protecting privacy as a right and at what point limiting one's right to privacy can be justifiable. This chapter is designated for doing so.

The chapter begins by defining the right to privacy. It then explores the scope of the right to privacy, as provided both in the South African Constitution and the ICCPR. The issues here would be whether the right to privacy can be legally limited and under what conditions. The chapter ends with concluding remarks.

#### 2.2. The conception of the privacy

Before dealing with the right to privacy as recognised in the ICCPR and the South African Constitution, it is important to have clarity on what 'privacy' itself is. Every human community, throughout known human history, the level of economic and technological development regardless, is assumed to have a certain concept of privacy. This is not however to mean that the right to privacy was recognised and enforced by the state at all times.<sup>28</sup>

---

<sup>28</sup> Indeed, some notion of privacy was recognised in the Roman Dutch Law within the concept of '*dignitas*'. Even in the Anglo-American legal system unlawful invasion of privacy was entrained as a tort action. Privacy as a constitutional right or human right, especially in the US, India, Canada, is however the result of the judicial interpretation of other well recognised

The claim is that the notion of privacy is as old as the human society itself. However, privacy has no universally agreed upon definition. Moreover, the notion of privacy is highly impacted on by time, place, economy and technology (TPET).<sup>29</sup> Hence legal definitions of privacy and legal principles that were established decades ago for its protection turn out to become useless with passage of time and the advancement of technology. For instance, currently advancement in digital technology has turned previous conceptions of privacy over their head.<sup>30</sup>

The oldest conception of privacy is as one's right to be 'left alone'.<sup>31</sup> Privacy was also defined 'as liberty or freedom to act in personal matters'. In the US jurisprudence, privacy as 'liberty in personal matters' was linked to the debate on reproductive freedom. This aspect of privacy was at the heart of one of the most famous US Supreme Court decision on *Roe v. Wade* in which a woman's right to have an abortion was successfully argued on the grounds of privacy.<sup>32</sup> Privacy is also defined in terms of a person's right to have control over certain information. This is based on the belief that a person should have the power to determine for himself/herself 'when, how, and to what extent information about them is communicated to others'.<sup>33</sup> Privacy is also conceptualized as restricted access to one's information in a sense that one has a restricted access to someone else's information or information about someone else.

Van der Bank puts the different features of privacy into three categories. These are spatial privacy, privacy relating one's choices and information and

---

rights such as the right to life, liberty and security of a person. D McQuid- Mason (1977) Privacy 18-9.

<sup>29</sup> Canattaci J.A. (2016) Report of the Special Rapporteur on the right to privacy, A (HRC/31/64)

<sup>30</sup> See Section 4 of this chapter.

<sup>31</sup> Glancy J. (1979) 'The invention of the right to privacy' 21 (1) *Arizona Law Review* 2; Entrikin. J L (2014) 'The right to be let alone: The Kansas right of privacy' 53 *Washburn Law Journal* 222; Jacoby. N (2007) 'Redefining the right to be let alone: Privacy rights and the constitutionality of technical surveillance measures in Germany and the United States' 35(3) *Georgia Journal of International and Comparative Law* 456.

<sup>32</sup> *Roe v. Wade*, 410 U.S. 113 (1973).

<sup>33</sup> Moor J.H. (1990) 'The ethics of privacy protection' 39(1) *Library Trends* 74.



communication privacy.<sup>34</sup> Spatial privacy is all about protecting a person's personal and territorial space.<sup>35</sup> Also known as territorial privacy, it is concerned with limiting intrusion into one's 'domestic and other environments including workplace or public space'.<sup>36</sup> This also includes body privacy that seeks to protect people's 'physical selves against invasive procedures such as drug testing and cavity searches'.<sup>37</sup> This aspect of privacy seems to be in line with the conception of privacy as the right to be left alone. The privacy relating to choose is about preventing the state or other individuals from interfering in people's choices which seems to in line with the conception of privacy as freedom to act. Information and communication privacy seeks to restrict others access to one's personal information. 'Information privacy' is all about protecting one's personal data such as credit information and medical records.<sup>38</sup> There is also a fourth aspect privacy, privacy of communication, which is also the focus of this paper is, privacy of communications, 'which covers the security and privacy of mail, telephones, email and other forms of communication'.<sup>39</sup>

This study is concerned with two specific elements of privacy; informational and communication privacy. The informational aspect of privacy relates to 'the function and role of privacy in determining the flows of information in society and the resultant impact on the development of the personality of individual citizens as well as almost inextricably related issues such as the distribution of power and wealth within society'.<sup>40</sup> Privacy of communication on the other hand encompasses the right of a person (both nature and legal) to communicate with others, or express opinion, and participate in a community in any manner without any fear that their communications might be

---

<sup>34</sup> Van der Bank C.M. (2012) 'The right to privacy – South African and comparative perspectives' 1(6) *European Journal of Business and Social Sciences*, 78.

<sup>35</sup> 'Privacy is an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined himself to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private'. *Ibid.* See also Ajayakumar J and Ghazinour K 'I am at home: Spatial Privacy Concerns with Social Media Check-ins' The 4<sup>th</sup> International Symposium of Emerging Information, Communications and Networks.

<sup>36</sup> Van der Bank C.M. (2012).

<sup>37</sup> *Ibid.*

<sup>38</sup> *Ibid.*

<sup>39</sup> *Ibid.*

<sup>40</sup> Canattaci (2016).

intercepted.<sup>41</sup> It is also a right that protects individual choices regarding what information to share and with whom to share the information.

### 2.3. Why is privacy a right?

As will be discussed below, privacy is recognised as a right both under the South African Constitution and other human rights instruments including the ICCPR. This raises the issue of why is it given such legal status? Why is privacy a right?

There is two-pronged justification for recognising privacy as right. One justification is based on the intrinsic value of privacy while the other is based on the instrumentality of privacy. Regarding the intrinsic value of privacy, Moor argues that privacy is good for its own sake and as such must be protected. And invading one's privacy even when the invasion has no apparent harm is wrong. Moor maintains one whose privacy is invaded, even if without his knowledge and without his daily life being affect, is 'morally wronged'.<sup>42</sup>

The instrumental justification for protecting one's privacy is based on the benefits that such protection brings about. Protecting one's privacy is a way of showing the respect he deserves. Privacy is critical for friendship, love and other similar social interactions. The protection of privacy is also justified based on the need to ensure that one has personal autonomy.<sup>43</sup>

The legal protection of one's privacy is among the new comers in the evolution of individual rights. For centuries, the focus of legal protection were

---

<sup>41</sup> Geneva Academy International Humanitarian Law and Human Rights (2014) *The right to privacy in the digital age: Meeting Report*, 2.

<sup>42</sup> Moor.J H, (1990) 81. For philosophical and ethincal justification for the protection of privacy see Negley G. (1966) 'Philosophical views on the value of privacy' *Law and Contemporary Problems* 319-325.

<sup>43</sup> *Ibid.* See also Klitou. D (2014) *Privacy-Invasive Technologies and Privacy by Design: Safeguarding Privacy Liberty and Security in the 21<sup>st</sup> Century* Springer, 18-19.

a person's body and property. A person's life and body were legally protected from deprivation and unlawful restraints. A person's lands and cattle were also protected from unlawful seizure or dispossession. When the protection of human right went beyond a person's body and property to include his spiritual and psychological, the law began protecting individuals from fear of injury, nuisance, slander and libel. So, there was no such a thing as right to privacy which was protected on its own other than as part of protecting one's life and body. Among the first who argued in support of the legal protection of one's privacy are Samuel D.<sup>44</sup> Warren and Louis D. Brandeis, in their article that was published in 1890 argued that new technological advancement began to negatively affecting a person preference to be 'left alone'.

'The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.'<sup>45</sup>

What raised the issue of privacy then was the mere invention of camera and the like. As will be shown below, in the information age that we are in, privacy is under increased threat hence its protection needs more attention. This obviously required the recognition of privacy as a right and its increased protection.

'Privacy is regarded as fundamental because of the protection it afford the individuality of the person on one hand and the space it offers for the development of his personality on the other. An individual is entitled to

---

<sup>44</sup> Warren S.W. and Brandeis L.D. (1890) 'The Right to Privacy' 4(5) *Harvard Law Review* 193-220.

<sup>45</sup> *Id*, 196.

function autonomously in his private life and 'privacy' is aimed to shield him in this area from public gaze. What it seeks to recognise is a 'zone of isolation, a legal cloister, for those qualities, wishes, projects and life styles, which each individual man, woman or child, wishes to enjoy or experience'.<sup>46</sup>

Privacy, as a right, is not however on an equal status with other more basic and 'natural' rights, such as the right to life.<sup>47</sup> Even the move towards legal protection of the right to privacy is a relatively recent phenomenon. Moreover, privacy was considered to be a relative value one which is more cherished in one society than others. Furthermore, privacy protected more as a mechanism of protecting other more fundamental rights than for its own value.<sup>48</sup>

#### 2.4. Privacy and state surveillance in the digital age

Privacy is one of those rights that is susceptible for violation with the advancement of technology and many argue that the protection of privacy should take into consideration such advancements. This is especially important because the progress in technology also provides governments with more advanced means of surveillance.<sup>49</sup> Now, the world is in the age of

---

<sup>46</sup> Jayawickrama N. (2002) *The judicial application of human rights law, national, regional and international jurisprudence* 605.

<sup>47</sup> Van der Bank (2012) 79.

<sup>48</sup> *Ibid.*

<sup>49</sup> UN Human Rights Council (2017) Report of the Special Rapporteur on the right to privacy (Human Rights Council Twenty-seventh Session Agenda items 2 and 3 Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development). See also Nyst C and Falchetta T (2017) 'Practice note: The right to privacy in the digital age' 9 *Journal of Human Rights Practice* 104–118; Cole D.D (2013) 'Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism' in Davis F, McGarrity. N & Williams. G (eds) *Surveillance, counter-terrorism and comparative constitutionalism* New York: Routledge 95-116; Dorraji S.E and Barcys. M (2014) 'Privacy in digital age: dead or alive?! Regarding the new EU data protection regulations' 4(2) *Social Technologies* 306–317; R. Wilton 'Identity and privacy in the digital age' x(Y, xxxx) *International Intellectual Property Management* 1-18,

information which came about as a result of advancement in digital technology. This means individuals generate multitudes of volumes of information about themselves and others every second. These are stored in digital forms both online and offline including on mobile devices such as cell phones, computers, and the like.<sup>50</sup>

The advancement in digital technology admittedly creates immense convenience on the lives of many. Digital technologies make businesses increasingly efficient and competitive, are used in health care services and make communications faster and easier. However, they also expose the privacy every individual for interference by state agents and other individuals. This is because digital technologies have also enhanced the states capacity to conduct surveillance and intercept individual's communications. Now a state's effectiveness in terms of 'conducting surveillance is no longer limited by scale or duration'.<sup>51</sup> Moreover, advancement in technology has reduced the cost of surveillance and data storage which in turn has 'eradicated financial or practical disincentives to conducting surveillance'.<sup>52</sup> The advancement in digital technology has also enhanced the capacity of non-state entities, such as companies, to intercept or monitor others. For instance, companies now can electronically monitor the works and actions of their employees.<sup>53</sup>

The immense capacity of the state to intercept individual communications

---

<sup>50</sup> *Ibid.*

<sup>51</sup> *Ibid.*

<sup>52</sup> *Ibid.* Also Milanovic M. 'Human rights treaties and foreign surveillance: Privacy in the digital age' 56(2015) *Harvard International Law Journal* 81-146.

<sup>53</sup> According to N J King employers can now use electronic devices to 'review and measure the work performance of' their workers. As part of evaluating a worker's performance, employer may now 'a computer to retrieve and review an employee's e-mail messages sent to and from customers'. Employers also use "electronic surveillance" "...to observe the actions of an employee'. They do so for purposes unrelated to 'measuring work performance. For instance they monitor their employees emails and use those in case of investigation of misconducts, such as 'investigation of a sexual harassment complaint'. Moreover employers 'use of computer forensics, the electronic recovery and reconstruction of electronic data after deletion, concealment, or attempted destruction of the data... For example, an employer may use specialized software to retrieve e-mail messages related to an investigation of alleged theft of its trade secrets by retrieving and reconstructing e-mail messages sent by an employee (the alleged thief) to someone outside the company'. N J King 'Electronic monitoring to promote national security impacts workplace privacy' 15(3) *Employee Responsibilities and Rights Journal* 128-129.

became clearer after Edward Snowden's revelations of how the American National Security Agency (NSA) intercepts and stores every communication of every individual in the US and beyond. Snowden was a private contractor in the NSA with administrative clearance to the NSA.

'The NSA has built an infrastructure that allows it to intercept almost everything. With this capability, the vast majority of human communications are automatically ingested without targeting. If I wanted to see your emails or your wife's phone, all I have to do is use intercepts. I can get your emails, passwords, phone records, credit cards. I don't want to live in a society that does these sort of things ... I do not want to live in a world where everything I do and say is recorded. That is not something I am willing to support or live under.'<sup>54</sup>

Increasingly African countries are also building their capacity of using technology to spy on their citizens and violate their privacy. For instance, it was reported that Ethiopia received assistance from the NSA to build technological system that helps it conduct surveillance on its citizens.<sup>55</sup> A Human Rights Watch Report also shows that the country has built the capacity to monitor every telephone conversation. An interview of the HRW said;

'They know everything we do...One day they arrested me and they showed me everything. They showed me a list of all my phone calls and they played a conversation I had with my brother. They arrested me because we talked about politics on the phone. It was the first phone I ever owned, and I thought I could finally talk freely.'<sup>56</sup>

---

<sup>54</sup>Macaskill E. (2013) *Edward Snowden, NSA files source: 'If they want to get you, in time they will'* <https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why>. Accessed on 16 March 2017.

<sup>55</sup> Human Rights Watch (2014) "*They know everything we do*" Telecom and Internet Surveillance in Ethiopia. <https://theintercept.com/2017/09/13/nsa-ethiopia-surveillance-human-rights/>. Accessed on 20 May 2017.

<sup>56</sup> *Ibid.*

The advancement in information technology is therefore exposing people's privacy. The United Nations General Assembly was so concerned about the increased capacity of states to conduct mass surveillance that, in a resolution adopted on 18 December 2013, called on member states to respect the right to privacy, in particular in the context of digital communication.<sup>57</sup> It also called on states to 'establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data'.<sup>58</sup> Moreover, it requested the United Nations High Commissioner for Human Rights:

' to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council'.<sup>59</sup>

The SRP reports show a worrying trend in the use of digital technology by state agencies in terms of interception communications, storing data and the like. The SRP, citing a study the Georgetown Center on Privacy and Technology, reported that in the United States "one in two American adults is in a law enforcement face recognition network' which are likely to impact individuals' privacy.<sup>60</sup>

There is an argument that the use of information technology such as email and cell phones exposed one for interception from by another. And when an individual uses such devices he is to some extent taking at a risk of forfeiting his or right to privacy. This is not however accepted by many. Jayawickrama argues that one should not be assumed to have given up his or right to

---

<sup>57</sup> UN General Assembly Resolution ([68/167],2013) *The Right to Privacy in digital age* (Adopted by the General Assembly on 18 December 2013).

<sup>58</sup> *Ibid.*

<sup>59</sup> *Ibid.*

<sup>60</sup> UN Human Rights Council (2017) Report of the Special Rapporteur on the right to privacy.

privacy simply because he or she uses of information technology or other cellular devices. This is specially the case when the interception is conducted by state agencies.<sup>61</sup> Evidences gathered through unlawful interception cannot or should not therefore be used against a suspect.

## 2.5. The right to privacy under South African Constitution

The right to privacy in South Africa was first constitutionally recognised under the Interim Constitution.<sup>62</sup> Before the promulgation of the Interim Constitution, the right to privacy was recognised under the common law within 'broad principles of the *actio injuriarum*'.<sup>63</sup> Under this principle what was prohibited was 'an intentional and wrongful interference with another's right to seclusion in his [or her] private life. Hence the 'delict' involves three elements 'wrongfulness', 'intention' and 'impairment of the plaintiff's personality rights (in this instance, privacy)'.<sup>64</sup> Under the *actio injuriarum* invasion of one's privacy was also considered by South African courts as 'an impairment of *dignitas*'.<sup>65</sup> Invasions of privacy under the common law had two broad elements. The first is intrusions or interferences with one's private life. And the second broad element was 'disclosures and acquisition of information'. Interception of communication, as a violation of rights, fell under the second category.<sup>66</sup>

The right to privacy in South Africa is now recognised both under common law and the 1996 Constitution.<sup>67</sup> Section 13 of the Interim Constitution and

---

<sup>61</sup> Jayawickrama (2002).

<sup>62</sup> S 13, Constitution of the Republic of South Africa, Act 200 of 1993.

<sup>63</sup> Cohen T. 'But for the nicety of knocking and requesting a right of entry': Surveillance law and privacy rights in South Africa' 1(1) (2001) *The Southern African Journal of Information and Communication*.

<sup>64</sup> Padayachee C. (2015) *Employee's right to privacy vs the employer's right to monitor electronic communication in the work place* (unpublished master's thesis University of KwaZulu Natal). Cohen (2001)

<sup>65</sup> *Ibid.*

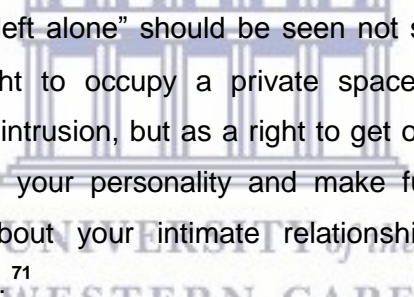
<sup>66</sup> *Ibid.*

<sup>67</sup> The constitutional recognition of the right to privacy does not do away with those rights that are recognised under the common law. It rather creates wider right to privacy which 'may also give rise to new actions for invasion of privacy which will include not only the interests protected by the common law but also a number of important personal interests as against the state. These interests generally involve family arrangements and sexual orientation. In countries such as the United States the result of constitutionalizing these interests is that



Section 14 of the Constitution uses almost the same wording as far the right to privacy is concerned. Section 14 of the Constitution states that everyone has the right to privacy which includes the right not to be have, their person or home searched, their property searched, their possession sized or the privacy of their communications infringed.<sup>68</sup>

David McQuoid-Mason writes that the right to privacy, as recognized in the Constitution can be divided into two categories.<sup>69</sup> In the first category is what he calls substantive privacy. This has to do with ensuring that one's 'personal autonomy' is not violated. 'Personal autonomy' is all about protecting one's personal life including one's home 'marriage, procreation, contraception, family relationships, child-rearing, and education'.<sup>70</sup> In this respect the Court in the *National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others* states:



"right to be left alone" should be seen not simply as a negative right to occupy a private space free from government intrusion, but as a right to get on with your life, express your personality and make fundamental decisions about your intimate relationships without penalisation'.<sup>71</sup>

One's personal autonomy cannot, as a rule, be violated by the state. A state can only limit an individual's personal autonomy when the conditions that are listed in the 'limitation clause' are fulfilled.<sup>72</sup>

In the second category is informational privacy which is also the focus of this study.<sup>73</sup> This is concerned with protecting one's private information. It seeks to prohibit the state and others from gaining or accessing, publicizing or

---

'what once were victimless crimes are now lawful pursuits, the invasion of which creates a constitutional tort'. Van der Bank (2012).

<sup>68</sup> Section 14 of the Constitution of Republic of South Africa 1996.

<sup>69</sup> McQuoid-Mason (1998) 18-9.

<sup>70</sup> *Ibid.*

<sup>71</sup> (CCT11/98) [1998] ZACC 15; 1999 (1) SA 6; 1998 (12) BCLR 1517 (9 October 1998).

<sup>72</sup> For discussion on this see Ssection 5.1. of this chapter.

<sup>73</sup> McQuoid-Mason (1998) 18-9.

otherwise using one's information without the consent of the person concerned. As will be discussed in the next chapter, the constitutional recognition of this aspect of a person's right to privacy was necessary for this was particularly a target of violation under the apartheid system.<sup>74</sup> In this respect, the Constitution explicitly prohibits infringing one's communications. The infringement may take different forms. Based on Section 13 of the Interim Constitution the Supreme Court, in *Klein v Attorney-General, WLD, & another*, decided that restoring information that was deleted by the owner of the information and accessing the information was a violation of the right to privacy.<sup>75</sup> In *S v Kidson*,<sup>76</sup> the Supreme Court decided that an information that is obtained by one using concealed recording device was not in violation of the right to information privacy of the other party since one of the two parties to the conversation had agreed to carry out the recording. The court stated that what the Prohibition of the Interception of Communication Act prohibited was third party eavesdropping.

Section 14 of the South African Constitution is not an absolute right and, therefore, under the right circumstances can be limited. The right to privacy can be limited in terms of section 36(1) of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, quality and freedom, taking into account the relevant factors including the nature of the right, the importance of the purpose of the limitation, nature and the extent of the limitation, the relation between the limitation and its purpose and less restrictive means to achieve the purpose.<sup>77</sup> Furthermore under subsection (2) it states that except as provide under subsection (1) or any other provision in the Constitution no law

---

<sup>74</sup> See Chapter 3, Section 3.

<sup>75</sup> Klein was working in certain company before he was dismissed because he was accused of fraud and forgery. The company managers accessed the computer that he was working on and restored some of the data that Klein deleted. They transferred the data to the General Attorney so that the latter can use the data for prosecuting Klein. The Supreme Court found the action of the managers of the company in terms of restoring and deleted data and obtaining the data, without the consent of Klein, was a violation the right to privacy of the latter. *Klein v Attorney-General, WLD, & another* 1995 (3) SA 848 (W) at 865.

<sup>76</sup> 1999 (1) SACR 338 (W).

<sup>77</sup> Section 36(1) of the Constitution 1996.

may limit any right entrenched in the Bill of Rights.<sup>78</sup> Infringements of private communications through eavesdropping and surveillance would be regarded as reasonable if authorised by a judge where a serious offence is concerned, or where the security of the country is at risk.<sup>79</sup> In the case of *Bernstein v Bester NO* the court stated that the nature of privacy implicated by the right to privacy related only to the most personal aspects of a person's existence, and not every aspect within his or her personal knowledge and experience.<sup>80</sup>

### 2.5.1. Limitations on the right to privacy

The South African Constitution provides that all rights that it recognises, including the right to privacy, can be limited when certain specific conditions are fulfilled. Section 36(1) of the Constitution provides that:

'The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including:

- (a) the nature of the right;
- (b) the importance of the purpose of the limitation
- (c) the nature and extent of the limitation
- (d) the relation between the limitation and its purpose;
- (e) and less restrictive means to achieve the purpose.'

#### 2.5.1.1. Law of general application

The first condition is 'legality'. This is to mean that the right to privacy, like all rights in the Bill of rights, can be limited in accordance with 'law of general application'.<sup>81</sup> The term 'law' may include parliamentary acts and common law rules. There is no agreement on among scholars on whether 'directives

<sup>78</sup> Section 36(2) of the Constitution 1996.

<sup>79</sup> Interception and Monitoring Prohibition Act 127 of 1992.

<sup>80</sup> *Bernstein and Others v Bester NO and Others* (CCT23/95) [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (27 March 1996).

<sup>81</sup> There are a number of Acts that put some limitation of the right to privacy. The reasonableness of the limitation these Acts put was challenged in courts and some were found to be reasonable.

or guidelines issued by government agencies or statutory bodies should qualify as laws of general application'.<sup>82</sup> According to Woolman and Botha, there are four tests for determining whether a law limiting one's right in the Bill of Rights is a 'law of general application'. These are 'generality, non-arbitrariness, publicity and precision'.<sup>83</sup> The requirement of 'generality' is that the law restricting one's right to privacy should be 'supreme and general' that is applicable both on ordinary citizens and government officials.<sup>84</sup> The most important consideration in this respect is that the law should not be what are known as 'bills of attainder'.<sup>85</sup> These are 'laws which are designed to pick out specific named individuals or easily ascertainable members of a group for punishment without judicial trial'.<sup>86</sup> The idea is therefore to prevent the law maker from adopting laws that can allow the violation of the rights of 'easily ascertainable individuals' there by ensuring that the law maker does not adopt laws that are arbitrary and discriminatory.<sup>87</sup>

Precision has to do with avoiding vagueness and providing clear criteria, using precise wordings, regarding when, where and how one's right to privacy can be restricted.<sup>88</sup> The requirement of 'publicity' is all about having a law that seeks to restrict one's right to privacy available for the public in form of codification or publication. As the Court in *De Lille & another v Speaker of the National Assembly* stated such law should be 'codified or capable of ascertainment'.<sup>89</sup> The requirement of 'non-arbitrariness' has to do with ensuring that a law does not provide unrestrained power of infringing one's right to a state agent thereby inviting for arbitrary actions from state agents. A law authorising the police to intercept the communication of one having 'questionable moral character', without clearly defining what constitutes

---

<sup>82</sup> Woolman S. and Botha H. (2008) 'Limitations' in Woolman S, Roux T and Bishop M (eds) *Constitutional law of South Africa* Kenwyn: Juta, loose leaf, 12-1-12-19.

<sup>83</sup> *Id*, 28.

<sup>84</sup> *Ibid*.

<sup>85</sup> *Ibid*.

<sup>86</sup> *Ibid*.

<sup>87</sup> *Ibid*.

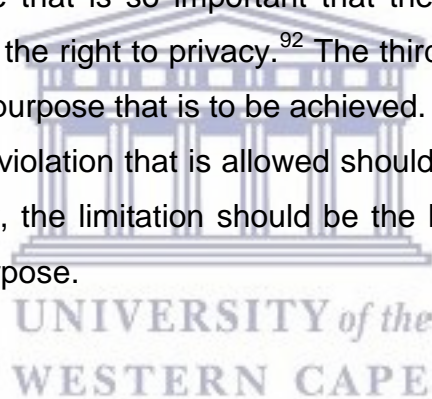
<sup>88</sup> *Ibid*.

<sup>89</sup> 1998 (3) SA 430 (C), 1998 (7) BCLR 916 (C).

'questionable moral character', can be considered as 'vague' which lacks precision and also arbitrary.<sup>90</sup>

#### 2.5.1.2. Proportionality

Law which restricts one's right to privacy might be challenged if it imposes a restriction which is not proportional. Proportionality is about ensuring that the limitation that is imposed on the right to privacy is 'reasonable and justifiable in an open and democratic society' based on human dignity, equality and freedom'.<sup>91</sup> The proportionality of the limitation is assessed, among others, by taking into consideration five factors under section 36(1) of the Constitution. The first factor in this regard is the 'the nature of the right' that is to be limited, the right to privacy in this case. The other factor is 'the importance and purpose of the limitation'. The question in this respect is whether there is a purpose or an objective that is so important that the achievement of which justifies the limitation of the right to privacy.<sup>92</sup> The third factor is that limitation should be linked to the purpose that is to be achieved. The fourth factor is that the extent or degree of violation that is allowed should be only to the extent it was necessary. Finally, the limitation should be the least intrusive limitation that can achieve the purpose.



## 2.6. The right to privacy under Article 17 of ICCPR: Meaning and scope

The right to privacy is one of the individual rights that are recognised almost by every international treaty dealing with human rights.<sup>93</sup> It is considered to be

---

<sup>90</sup> Woolman and Botha (2008) 12-30.

<sup>91</sup> Section 36(1) of the Constitution 1996.

<sup>92</sup> Rautenbach I. M. (2014) 'Proportionality and the limitation clauses of the South African bill of rights' 17(6) PER 2229-2267.

<sup>93</sup> This right is recognized almost in every international and regional human rights instrument. Article 12 of the Universal Declaration of Human Rights provides that 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.' The American Declaration of the Rights and Duties of Man also provides 'Every person has the right to the protection of the law against abusive

central to the protection of one's human dignity. It also forms the basis of any democratic society. It is also linked to other rights, in particular with freedom of expression and of association.<sup>94</sup>

More importantly for purpose of this paper, the ICCPR, under Article 17 provides that everyone should be protected from 'arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation'. It adds a national law should provide everyone a protection from the violation of his or her rights to privacy. Further, Article 17(2) requires the provision of legal protection to everyone against interference into his or her privacy whether the threat comes from states authorities, natural person, or legal person. Moreover, Article 17 imposes an obligation upon the state to adopt legislative and other measure in order to prevent any kind of interference into the right to privacy of, as well as for the protection of the right, under all circumstances.<sup>95</sup>

In addition, the right to privacy, as enshrined under Article 17 of ICCPR, prevents others from gaining or attempting to gain access to one's information, publishing it, or disclosing or using information. According to the HRC one's correspondences 'should be delivered to the addressee without interception and without being opened or otherwise read'.<sup>96</sup> Some argue that what is protected is the content of a correspondence. However, government may intercept and collect data about communications, or so-called metadata,

---

attacks upon his honor, his reputation, and his private and family life'. It also protects one's 'Right to the inviolability and transmission of correspondence'. The European Convention on Human Rights recognizes one's right to have one's 'private and family life, his home and his correspondence' respected. The right to privacy is also contained and recognised in almost every constitutional bill of rights and major international and regional conventions. The Convention on the Right to the Child recognises the right to privacy of the Child. Moreover, International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families provides similar right to migrant workers and their families.

<sup>94</sup> Privacy International and TEDIC (2015) *The right to privacy in Paraguay*, Universal Periodic Review Stakeholder Report: 24th Session, Paraguay.

<sup>95</sup> Office of the United Nations High Commissioner for Human Rights *ICCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation (Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988)*.

<sup>96</sup> Office of the United Nations High Commissioner for Human Rights *The right to privacy in the digital age; Report of the Office of the United Nations High Commissioner for Human Rights*, 6.

without actually intercepting the content of the communication. This, they argue, in line with Article 17 of ICCPR. However, HRC views such arguments as unacceptable.<sup>97</sup> The HRC accepts the reasoning of the European Union Court of Justice (EUCJ) that, ‘communications metadata “taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained’.<sup>98</sup> At the same time under international law individuals have the right to know who holds the information about them and how that information is used.

The Human Rights Committee (HRC) states that a state can be considered to have complied with Section 17 of the ICCPR when it guarantees in law and practice the integrity and confidentiality of one’s correspondence including written and oral, whether transmitted electronically or mechanically. This aspect of privacy requires that one’s correspondence should reach to the address that it is sent to without interception. This in turn forbids surveillance of any form including the interception of electronic, telephonic or telegraphic correspondence. Taping one’s telephone or otherwise intercepting one’s telephonic conversation is considered as serious interference into one’s correspondence. As Taylor argues, ‘[i]t is essential to have clear, detailed rule of the subject, especially as the technology available for use is continually becoming more sophisticated’.<sup>99</sup>

Nevertheless, the right to privacy, like any other right, is not an absolute right that has no limitations.

‘Privacy, like other rights, is not absolute. While the ‘inner sanctum’ of a person (e g family life, sexual preference and home environment) may be shielded from erosion by conflicting rights of the community as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly.’<sup>100</sup>

---

<sup>97</sup> *Ibid.*

<sup>98</sup> *Ibid.*

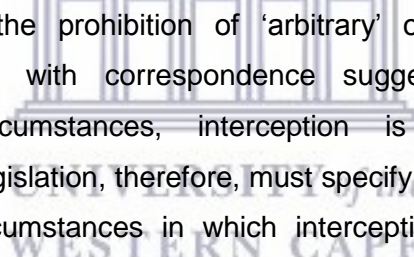
<sup>99</sup> Taylor K. (2002) ‘State surveillance and the right to privacy’ 1(1) *Surveillance & Society* 68.

<sup>100</sup> Mason 18-1.

Article 17 of the ICCPR itself implies that this right is not an absolute right by stating that what is prohibited is illegal and arbitrary invasion of one's right to privacy.<sup>101</sup> According to the HRC, the right to privacy, like any other right recognised under ICCPR, can be limited if the requirements of legality, necessity and proportionality are met.<sup>102</sup> In the *Tristan Donoso*, the Court stated that such restrictions on privacy must be statutorily enacted, serve a legitimate purpose, and meet the requirements of suitability, necessity, and proportionality, which render it necessary in a democratic society.<sup>103</sup>

### 2.6.1. Legality

Paragraph 2 of Article 17 of the ICCPR states that one is protected from 'unlawful' interference into his/her privacy. The term 'unlawful' implies that there is a possibility that one's privacy can be legally restricted.



'However, the prohibition of 'arbitrary' or 'unlawful' interference with correspondence suggest that in certain circumstances, interception is permitted. Relevant legislation, therefore, must specify in detail the precise circumstances in which interception may be permitted. A decision to make use of such authorized interferences must be made by the authority designated under the law, on a case by case basis.'<sup>104</sup>

This of course requires the adoption of a piece of legislation that clearly defines when and how one's privacy can be restricted. This is because 'regardless of the end to be achieved, no right guaranteed by the Convention

---

<sup>101</sup> Art 17 of ICCPR. Other international and regional human rights also contain limitations on the right to privacy. The European Convention on Human Rights such implies that this right may be restricted 'in accordance with the law' and if it is 'necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

<sup>102</sup>West End Strategy Team "Amnesty International Withdraws Support for the USA Freedom Act, Urges Stronger Reforms", 2014.

<sup>103</sup> *Tristán Donoso v. Panamá*, H.R. (ser. C) No. 193, 56 (2009).

<sup>104</sup> Jayawickrama (2002) 629.



should be interfered with unless a citizen knows the basis for the interference through an ascertainable national law'.<sup>105</sup> As the European Court of Human Rights in *Malone v United Kingdom* stated, 'the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous measures'.<sup>106</sup>

As far as the interception of one's communications is concerned, the above implies that a state, an individual or a company can intercept one's communications, telephonic, electronic or otherwise, based on an existing law allowing the action. The law authorising interference into one's privacy, or intercepting one's correspondence, should not undermine the objective and purpose of the ICCPR. Hence 'secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law"'.<sup>107</sup> The law restricting one's privacy cannot however be too intrusive that violates the ICCPR or another relevant international human rights law.

#### *Accessibility of the law*

The law limiting the right to privacy must not only exist but also be accessible to everyone. According to the HRC, "accessibility" implies a piece of legislation that is published and written in precise manner.<sup>108</sup> With regard to precision of the law it should 'detail the precise circumstances in which any such interference may be permitted, the procedures for authorizing, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of the data collected'.<sup>109</sup> In other word the law should not provide too much discretion to state agents in terms of where and when they can intercept one's communication. The idea is to inform 'to enable the affected person to regulate his or her conduct, with foresight of the consequences that a given

---

<sup>105</sup> Taylor (2002) 68.

<sup>106</sup> [1984] ECHR 10.

<sup>107</sup> Human Rights Council *The right to privacy in the digital age* (Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37), 10.

<sup>108</sup> *Ibid.*

<sup>109</sup> *Ibid.*

action may entail'.<sup>110</sup> The restriction of one's privacy, in particular the interception of one's communications, can be done for specific legitimate purpose. Moreover, the law must provide procedural safeguards against undue interference into one's privacy.

In the case of *Klass and Others v. Germany* court found that the mere existence of legislation that allowed a system to secretly monitor communications gave rise to a menace of surveillance that amounted to an interference with the privacy of all those to whom the legislation may have been applied.<sup>111</sup> However Article 17 does not provide us with clear guidelines regarding when, how, and under what circumstance the right to privacy can be legally limited. It however implies that the limitation cannot be done without legal basis or legitimate ground. Moreover, the law limiting one's privacy must 'comply with the provisions, aims and objectives of the Covenant'.<sup>112</sup> If the national law permitting interference in one's privacy is contrary to the ICCPR, then the interference, though legal under the national law, is considered to be unlawful under international law. From the above provision, it is clear that the right to privacy, under all conventions, is not absolute right. What is prohibited is 'arbitrary' and 'unlawful' interference in one's right to privacy. This implies if lawful, interference in one's privacy or family or correspondence is not viewed as violation of one's right to privacy, unless the invasion is unnecessary or disproportional. As stated in the case *Rojas Garcia v. Colombia* even if interference is within the scope a domestic law, the State needs a clear justification for it.<sup>113</sup>

## 2.6.2. Necessity

While lawful, in a sense that there is a national law permitting intervention in one's privacy, if the interference is unnecessary, random or subjective, such

---

<sup>110</sup> *Ibid.*

<sup>111</sup> *Klass and Others v. Germany*, no. 5029/71, 6 September 1978.

<sup>112</sup> Amnesty International Withdraws Support for the USA Freedom Act, Urges Stronger Reforms, 2014.

<sup>113</sup> *Rojas Garcia v. Colombia*, Communication No.687/1996, U.N. Doc. CCPR/C/71/D/687/1996 (2001).

interferences may be viewed as violation of one's right to privacy.<sup>114</sup> This means the interception of one's communication by a state agent is a violation the person's privacy unless the interception is critical for some purpose. The level or degree intrusion into one's privacy is also assessed in light whether that degree of interference is necessary for achieving a certain legitimate purpose. The HRC emphasized that non-arbitrariness requires that interference is reasonable in the particular circumstances.<sup>115</sup>

'Where there is a legitimate aim and appropriate safeguards are in place, a State might be allowed to engage in quite intrusive surveillance; however, the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime.'<sup>116</sup>

The Committee stated that 'it is not sufficient that the restrictions serve the permissible purposes; they must also be necessary to protect them'.<sup>117</sup> According to the HRC any interference authorised by a government has to be conducted in terms of the law and must comply with the aim and objectives of the ICCPR.<sup>118</sup> Moreover interferences into one's privacy have to be reasonable under particular circumstances.<sup>119</sup> This means what is reasonable interferences under one particular situation might not necessarily be the same

---

<sup>114</sup> Vincent S. (2014) *International law and secret surveillance: Binding restrictions upon state monitoring of telephone and internet activity* Centre for Democracy and Technology. United Nations High Commissioner for Human Rights, 8.

<sup>115</sup> *Rojas Garcia v. Colombia*.

<sup>116</sup> United Nations High Commissioner for Human Rights *The right to privacy in the digital age; Report of the Office of the United Nations High Commissioner for Human Rights*, 9.

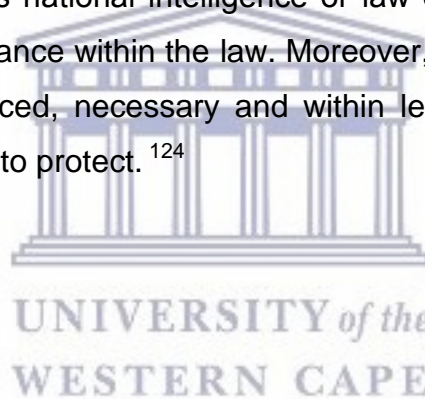
<sup>117</sup> *Ibid*.

<sup>118</sup> Le Rue F. The present report, submitted in accordance with Human Rights Council resolution 16/4, analyses the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression 7.

<sup>119</sup> Office of the High Commissioner for Human Rights CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988.

in another situation.<sup>120</sup> Therefore what is reasonable interference may differ depending on the circumstances of each situation.<sup>121</sup> What is important is that the interference into one's privacy, the interception of one's communication this case, should not affect the 'essence of' the person's privacy.

Among the instances where interference into the right to privacy is allowed is related to national security or public interest and prevention of terrorist attacks.<sup>122</sup> Where there is an immediate and serious threat to national security then interference in one's privacy, including the interception of his/her communications, may be tolerated regardless of whether the threat is coming within or from without the country.<sup>123</sup> National security or public interest and terrorism are viewed as legitimate reason for state to intercept communication. Therefore, under such circumstance the interference can be necessary. Yet a state's national intelligence or law enforcement institutions have to conduct surveillance within the law. Moreover, the surveillance should be objective and balanced, necessary and within legitimate public interest, which the state is trying to protect.<sup>124</sup>



### 2.6.3. Proportionality

Even though national security is often viewed as legitimate reason that justifies interfering in one's privacy, it by no means mean that it will always be justifiable and good enough reason to interfere with the right to privacy.<sup>125</sup> In *Van Hulst v Netherlands* the HRC stated that reasonableness and proportionality are the same. Proportionality has four elements. There must be a legitimate aim to be pursued by limiting the right. There should be a rational connection between the measure limiting the right and the aim. There must be minimal impairment of the right to privacy, and that a fair balance must be

---

<sup>120</sup> Le Rue, 9.

<sup>121</sup> *Ibid.*

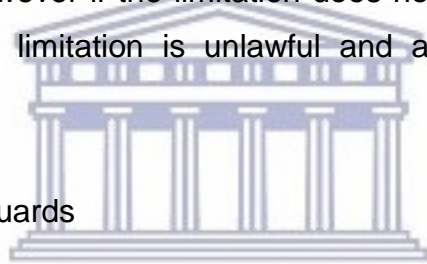
<sup>122</sup> White (undated).

<sup>123</sup> *Ibid.*

<sup>124</sup> *Ibid.*

<sup>125</sup> United Nations High Commissioner for Human Rights, 7.

struck between the aim and the right.<sup>126</sup> States are required under international law to provide evidence to justify the interference to the right to privacy.<sup>127</sup> Furthermore, the greater the interference the more the evidences presented by the state have to be more compelling.<sup>128</sup> In other words the interference into the right to privacy of a person has to be proportional with the aim and objective of that the limitation that is meant to be achieved through such interference.<sup>129</sup> Also in terms of international law the limitation has to be authorised by warrant from independent party and subject to judicial and political control. The limitation has to be done without any discrimination. In terms of Article 17(2) ICCPR everyone has the right to the protection of the law against such interference or attacks. Moreover, the government has the duty to ensure that the limitation is connected to legitimate and lawful aim and consistent with law and that the limitation should not render the right to privacy pointless.<sup>130</sup> However if the limitation does not meet a legitimate and lawful reason then the limitation is unlawful and arbitrary to the right to privacy.



#### 2.6.4. Procedural safeguards

Ensuring that interference into one's privacy is indeed conducted based on a law, for legitimate purpose and that it is proportionate requires some kind of procedural safeguard. These procedural and institutional safeguards are to avoid arbitrariness and arbitrary or unlawful intrusions. This is especially important in the digital age, as the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism stated, in order to ensure that there is no 'secret surveillance system that is not under review of an independent oversight body and all

---

<sup>126</sup> *Van Hulst v The Netherlands*, HUMAN RIGHTS COMM., Communication No. 903/1999, 7, U.N. Doc. CCPR/C/82/D/903/1999 (2004).

<sup>127</sup> Emmerson B. Promotion and protection of human rights and fundamental freedoms while countering terrorism, Report submitted to the United Nations General Assembly available at <https://assets.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf>. Accessed on 10 April 2016.

<sup>128</sup> *Ibid.*

<sup>129</sup> United Nations High Commissioner for Human Rights, 7.

<sup>130</sup> Geneva Academy International Humanitarian Law and Human Rights (2014) *The Right to Privacy in the Digital Age: Meeting Report*.

interferences must be authorized through an independent body'.<sup>131</sup> What is considered to be the most important safeguard in this regard is judicial oversight. Authorization by a judge should be a requirement for legal interception. And an executive organ should not be in charge of providing such authorization. In the UK the Home Secretary was in charge of authorizing interception. The interception of a telephonic conversation one who was accused of selling stolen goods based on the authorization of the Home Secretary was hence considered violation his privacy.<sup>132</sup> Parliamentary oversight is also critical even though it cannot help in terms of ensuring each and every interception is conducted in legal and proportional manner.<sup>133</sup> For instance, in Germany surveillance can be authorized by designated federal or Lander authority when the latter is convinced that there is imminent danger to the nation. However, the surveillance is supervised by an independent official. Moreover, the federal or lander authority which has the power to authorize surveillance is required to report to a parliamentary commission in which all political parties are represented.<sup>134</sup> This is viewed by the European Court as a good safeguard against excessive intrusion into one's privacy. Civil society organizations and the media also plays important role in terms of exposing illegal and undue interception of communication. The Snowden case is a good example of how the media can play important role in this regard.

## 2.7. Conclusion

The concept of 'privacy' has evolved from recognising that one has the right to be left alone to include privacy on one's person, information, property and the like. The right to information privacy has been exposed for violation with the advent of the age of information technology. The increasing the ability of state agencies and other interested individuals and groups, to conduct surveillance and retain data about the communication of almost everyone, the digital age has exposed people to for increased interference with their privacy.

---

<sup>131</sup> A /HRC/27/37, 13.

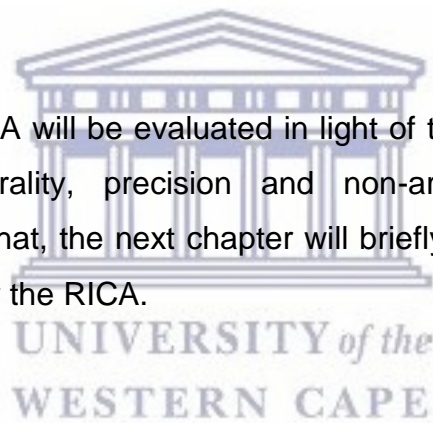
<sup>132</sup> Jayawickrama (2002)630.

<sup>133</sup> *Ibid.*

<sup>134</sup> *Id.*, 631.

Yet the right to privacy is a right that is recognised in national constitutions and international human rights instruments. Both the South African Constitution and the ICCPR recognise all elements of the right to privacy including personal, communication and information privacy. Under the South African Constitution and the ICCPR, the right to privacy, correspondence and information could be legally restricted only under certain conditions. The conditions that both the South African Constitution and the ICCPR provide in this respect are legality, necessity, proportionality. These elements are used for assessing the legality of interference in one's privacy. The two instruments also provide procedural safeguards that need to be put in place were for ensuring the conditions that legitimise interference into a person's privacy. The most important procedural safeguard in this regard is judicial oversight.

In chapter four, the RICA will be evaluated in light of the principles of legality (which includes generality, precision and non-arbitrariness), necessity proportionality. Before that, the next chapter will briefly introduce interception of communication under the RICA.



## **Chapter 3**

### **Interception of communication under RICA**

#### **2.7. Introduction**

The main question that this study aims to answer is whether the interception of individuals' communication that RICA allows is consistent with the right to privacy of citizens and residents of South Africa. This entails an in-depth discussion of why RICA was adopted and what it provides in terms of allowing interception of communication and evaluating the Act in light of the right to privacy of individuals. It is also necessary to discuss the national and global context that required the adoption this and other similar pieces of legislation. This chapter therefore aims to provide an account of the domestic and international political and security situations that gave rise to RICA. It also aims to discuss what the RICA provides in terms of substantive requirements for interception of communications and procedural safeguards against undue intrusion into the privacy individual citizens.

The chapter begins with a brief account of the global and national security context that prompted the South African government to enact RICA. It then provides a brief description of RICA. Then it discusses what RICA provides in terms of interception of communication.

#### **2.8. The global and national security context leading to the enactment of RICA**

On the 11 September 2001, a terrorist attack that target the World Trade Centre, in New York City of the United States of America, resulted in the tragic death of over 3000 innocent individuals.<sup>135</sup> This terrorist attack, which is commonly referred to as 9/11, was preceded and followed by numerous others terrorist attacks in different European countries and cities including

---

<sup>135</sup> Deutsche Welle (2017) *Madrid to Manchester to Barcelona: A chronology of terror in Europe*. Available at <http://www.dw.com/en/madrid-to-manchester-to-barcelona-a-chronology-of-terror-in-europe/a-38949481>. Accessed on 20 September 2017.



London, Madrid, Barcelona, Brussels, Paris and the like.<sup>136</sup> The countries and cities in our continent, Africa, were not also spared from similar terrorist attacks. Kenya, Ethiopia, Tanzania, Egypt and Somalia also suffered from terrorist attack that was coordinated by international terrorist organisations such as Al Qaida and regional terrorists such as Al Shebaab.<sup>137</sup>

The 9/11 terrorist attack had unprecedented legislative, military and political impacts with national and international consequences. It led to a global war dubbed as 'war on terror', which was led by the US under the auspices of the North Atlantic Treaty Organisation (NATO), in a number of countries, most importantly in Afghanistan and Iraq.<sup>138</sup>

It also led many countries in the world to adopt what are in general referred to as 'antiterrorism laws'.<sup>139</sup> A 2012 Human Rights Watch report indicates that, following 9/11, as many as 140 countries, including those that were not directly impacted on by terrorist attacks, adopted antiterrorism laws.<sup>140</sup> For instance, a month after the attacks of 9/11, the USA Congress adopted what is known as 'the Patriot Act'.<sup>141</sup> The British Parliament adopted several pieces of anti-terrorist legislation, namely, the Terrorism Act of 2000, the Anti-Terrorism, Crime and Security Act 2001 and the Terrorism Act of 2006. India adopted what is called the Information Technology Amendment Act of 2008.

---

<sup>136</sup> *Ibid.*

<sup>137</sup> Matthew B. Ridgway Center (2005) Anatomy of a Terrorist Attack: An in-Depth Investigation Into the 1998 Bombings of the U.S. Embassies in Kenya and Tanzania <[https://www.files.ethz.ch/isn/26356/05\\_anatomy\\_terr\\_attack.pdf](https://www.files.ethz.ch/isn/26356/05_anatomy_terr_attack.pdf)>; Jonathan Figiel (2011) Al-Qaeda –Mombassa Attacks 28 November 2002 (The Meir Amit Intelligence and Terrorism Information Center) <[http://www.terrorism-info.org.il/Data/pdf/PDF\\_19300\\_2.pdf](http://www.terrorism-info.org.il/Data/pdf/PDF_19300_2.pdf)> ; Patrick Kimunguyi *Terrorism and Counter terrorism in East Africa*<http://artsonline.monash.edu.au/radicalisation/files/2013/03/conference-2010-terrorism-counter-terrorism-eafrica-pk.pdf>. Accessed 25 of July 2017

<sup>138</sup> Daniel B. P. (2009) War About Terror: Civil Liberties and National Security After 9/11 (New York; Council on Foreign Relations).

<sup>139</sup> Stephen P M. 'International Law and the 'War on Terrorism': Post 9/11 Responses by the United States and Asia Pacific Countries' (2006) 14 (1) *Asia Pacific Law Review* 48. M Pearson and N Busst (2006) 'Anti-terror laws and the media after 9/11: Three models in Australia, NZ and the Pacific' 12(2) *Pacific Journalism Review* 9-27.

<sup>140</sup> Human Rights Watch (2012) In the Name of Security Counterterrorism Laws Worldwide since September 11(Human Rights Watch).

<sup>141</sup> Betsey S.C. (2011) 'The Right to Privacy in Light of the Patriot Act and Social Contract Theory' (Unpublished thesis; University of Nevada, Las Vegas) <[http://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=2087&context=thesesdissertation\\_s](http://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=2087&context=thesesdissertation_s)>. See USA Patriot Act (H.R 3162) <<https://epic.org/privacy/terrorism/hr3162.html>> Accessed on 10 of August 2017.

The antiterrorism laws in general define the term 'terrorism' very broadly. In some cases they incorporating what could be considered as peaceful dissents within the definition of 'terrorism'. They designate what the countries consider as terrorist organisations. In many cases, what was designated as terrorist organization is political organization with differing political programmes. The laws also tend to restrict free expression and silence the media, and restrict freedom of peaceful assembly.

Most importantly for the purpose this research, the anti-terrorism of laws, and other laws that fall in this category, provided the countries' security agencies with almost unfettered power of surveillance, with or without warrant, and arrest. According to Tuval, the Patriot Act allowed 'the US security agencies to take invasive measures, including invasive powers of search and surveillance, detention, and seizure of property and its confiscation, which previously had not been allowed because they compromised human rights and basic freedom'.<sup>142</sup> The Human Rights Watch report states that:

'More than 120 counterterrorism laws vastly expand police powers to surveil, search persons and property, make arrests, and seize objects and contraband in cases the police deem related to terrorism, in many cases without judicial warrant. By enhancing the ability of police forces to act without judicial approval, and lowering—or removing altogether—the grounds of reasonable suspicion or probable cause ordinarily required to justify police interference, these laws may violate the right to privacy and encourage racial profiling and the targeting of minorities.'<sup>143</sup>

The above was the global political, military and security context that underpinned the adoption of RICA. Interception of communication in South

---

<sup>142</sup> Tuval Y. 'Anti-Terrorism Legislation in Britain and the U.S. after 9/11' (The Israel Democracy Institute) <https://en.idi.org.il/articles/6936>. Accessed on 12 of August 2017.

<sup>143</sup> Human Rights Watch (2012), 51.

Africa however has much longer history which goes back to the time of the apartheid system. This directly or indirectly informs the debate on RICA.

## 2.9. History of interception of communication in South Africa

The very idea of interception of communications by state agents creates a rather strong revulsion among South African citizens since it brings about a painful memory of the apartheid system. Interception of communications during the apartheid system took the form of intercepting postal articles and telephonic conversation since the internet was not yet in a wide use at the time.<sup>144</sup> Maintaining national security was the apartheid regime's central justification for intercepting individuals' communications. These were enforced through various pieces of so called 'security legislation'. The most important piece of legislation in this regard was the Post Office Act of 1958.<sup>145</sup> Initially, even this piece of legislation was not too intrusive in terms of intercepting individuals' communications. The Act in fact allowed interception of postal communications only if and when there was a reasonable suspicion that a crime was being, or about to be, committed. Most importantly it did not allow the tapping of telephonic conversation.<sup>146</sup> The Potgieter Commission and the Rabie Commission, which were convened in 1972 and 1981, respectively, however recommended that the state security agencies be statutorily allowed to intercept postal communication for the purpose maintaining security.<sup>147</sup> To this end the Postal Office Act of 1958 was amended in 1972 and in 1981.

The Act was amended to authorise the apartheid regime to intercept, among others 'any particular article or particular communication which has been or is being or is intended to be transmitted by telephone or in any other manner

---

<sup>144</sup> Cohen (2001).

<sup>145</sup> Mathew A.S. (1986) *Freedom, State Security and the Rule of Law: Dilemmas of the apartheid society Johannesburg: Juta and Co Limited*, 173. See also Truth and Reconciliation Commission of South Africa Report Vol 3 <<http://www.justice.gov.za/trc/report/finalreport/Volume%203.pdf>> Accessed on 20 of March 2017.

<sup>146</sup> *Ibid.*

<sup>147</sup> 'The 1972 Potgieter Commission, set up to investigate matters relating to the security of the state, recommended the insertion of s 118A into the Post Office Act. This amendment was seen to accord with similar legislation and powers in Australia, West Germany and Britain. In 1981, the Rabie Commission of Inquiry into security legislation reviewed the provisions of s 118A and proposed certain further administrative, procedural and technical amendments'. Cohen (2001) 11.

over a telecommunication line;<sup>148</sup> The Act anticipated the invention of new means of communications and authorised the state to intercept those too. There is a rich account of how the letters that political prisoners that were imprisoned in Robben Island received and sent were intercepted and how words, sentences, paragraphs that were viewed as politically sensitive were cut out of their correspondences.<sup>149</sup> The government became more intrusive in terms of intercepting communications as new methods of communications and of interception were invented.

Things began to change when the Interception and Monitoring Prohibition Bill of 1992 was adopted, a year before the demise of the apartheid system and the adoption of the Interim Constitution. At this stage, the apartheid government was under pressure and the intrusion of the government into the privacy of individual citizens was being condemned by all sections of the society. Hence this Act aimed at protecting the right to privacy of individuals as recognised in the common law and protecting 'confidential information from illicit eavesdropping'.<sup>150</sup>

The Act aimed at repealing the Postal Office Act and prohibit the interception and monitoring of certain communications, except in accordance with the law and to provide for authorisation to do so in certain circumstances'. This is clearly indicated in the objective of the Act which provides:

'To prohibit the interception of certain communications and the monitoring of certain conversations; to provide for the interception of postal articles and communications and for the monitoring of conversations in the case of a serious offence or if the security of the Republic is threatened; and to provide for matters connected therewith.'<sup>151</sup>

To this effect the Interception and Monitoring and Prohibition Act (IMPA) allowed interception of communication not as a method of protecting 'state

---

<sup>148</sup> S 118A(I) Postal Office Act of 1958 as amended in 1972 and in 1981.

<sup>149</sup> Moseneke D. (2016) *My Own liberator: A memoire* Johannesburg: Picador Africa.

<sup>150</sup> South Africa interception and monitoring prohibition Act No. 127 of 1992.

<sup>151</sup> *Ibid*, Preamble.

security' but as a way of thwarting the commission of serious crimes.<sup>152</sup> "Serious offence' was qualified in so far as it must have been committed over a lengthy period of time, on an organised and regular basis; or it must be one that may harm the economy of the Republic, or is an offence contemplated in the Drugs and Drug Trafficking Act 1992'.<sup>153</sup> This 'change necessitated a shift in focus from state security to the combating of serious crime'.<sup>154</sup> Moreover, the Act stripped the Minister of the Interior to authorise interception of communication or wiretapping. Instead of the Minister, the Act provided that a retired judge could authorize interception of communication when there is a suspicion that a serious crime is being or about to be committed. According to Cohen, 'this change was vital in order to divest the 'security establishment of the state' of the vast powers of authorisation in this regard'.<sup>155</sup>

The Act further provides two conditions regarding when a direction to monitor and intercept one's communications could be undertaken. Before such direction is issued, first a convincing evidence should be presented to the judge that a serious offence was committed or about to be committed.<sup>156</sup> Not only that, it must be shown that the crime cannot be prevented (when it is in the process of being committed) or properly investigated in any other manner. The other ground for securing direction of interception was that the security of the Republic is threatened.<sup>157</sup>

However, soon it became clear that criminals were taking advantage of the increased sophistication of means of communications, including the inventions of cellphones, emails, and the like, to commit serious crimes, 'especially organised crime, heists, and other serious violent crimes'.<sup>158</sup> On the other hand, the IMPA was principally directed at preventing monitoring and interception of communication by state agencies and hence tied up the

---

<sup>152</sup> Cohen (2001), 2.

<sup>153</sup> *Ibid.*

<sup>154</sup> *Ibid.*

<sup>155</sup> *Ibid.*

<sup>156</sup> *Ibid.*

<sup>157</sup> *Ibid.*

<sup>158</sup> Bawa N. (2006) 'The regulation of the interception of communications and provision of communication related information act' in L Thornton, Y Carrim, P Mtshaulana and P Reyburn (eds) *Telecommunications law in South Africa* Johannesburg: STE Publishers, 297.

government's hand form preventing serious crimes or apprehending criminals once the crimes have been committed. Hence in 1995 a White paper on telecommunication policy was adopted.<sup>159</sup> The White paper stated that the government's authority to intercept and monitor telephonic communication should be controlled and that to this effect the Interception and Monitoring Prohibition Act should be reviewed 'in order to ensure sufficient safeguards are in place and that such a review should of necessity involve public debate and the participation of other Ministries, such as that of Safety and Security'.<sup>160</sup> The South African Law Reform Commission (SALC) thus began working towards reforming South Africa's pieces of security legislation with a view rationalising them 'to international norms, the interim Constitution and the country's changed circumstances and requirements'.<sup>161</sup>

In 1999, the SALC submitted its report to the Ministry of Justice and Constitutional Development for consideration. The report compared South Africa's security legislation with other similar pieces of legislation including that of France, the Netherlands, Belgium, Germany, Britain, the United States, Hong Kong and Canada and concluded that IMPA does not adequately deal with new technology and recommended that it be substantially repealed and replaced with new legislation. SALC also came up with a draft bill which was later adopted as RICA.

'RICA was drafted in response to the increasing diversity and developments in communication technologies, globalisation of the telecommunications industry, and the convergence of the telecommunications, broadcasting and information technology industries, which inter alia include satellites, optical fibres, computers, cellular technology, e-mail, surveillance equipment, and the electronic transfer of information and data. RICA sets out the circumstances under which government entities and other persons

---

<sup>159</sup> Cohen (2001) 3.

<sup>160</sup> *Ibid.*

<sup>161</sup> Bawa (2006)

may or must intercept or monitor conversations, cellular text messages, e-mails, faxes, data transmissions and postal articles, and establishes that in all other circumstances, such interception or monitoring is prohibited.<sup>162</sup>

It is important to note that RICA was adopted a year after 9/11. Other security minded Acts were also adopted around the same time including the Financial Intelligence Centre Act 38 of 2001 (“FICA”), the Electronic Communications and Transactions Act 25 of 2002 (“ECT”) and the Protection of Constitutional Democracy against Terrorism and Related Activities Act 33 of 2004 (“PCDTRA”). As will be discussed below, the ‘RICA permits greater latitude for the interception and monitoring of communication than was permitted by the IMPA’.<sup>163</sup>

## **2.10. Regulation of Interception of Communication Act (RICA) in brief**

The RICA was initially adopted as Act 70(2002). It was amended by the prevention and combating of corrupt activities Act 12(2004), Protection of constitutional democracy against terrorist and related activities Act 33(2004), Electronic communications Act 36(2005) and Regulation of Interception of Communications and Provision of Communications 48(2008).

### **2.10.1. Interception defined**

The RICA defines interception as:

The aural or other acquisition of the contents any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the-

- a. monitoring of any such communication by means of a

---

<sup>162</sup> Bawa (2006) 298.

<sup>163</sup> *Id.*, 299.

monitoring device;

- *b.* viewing, examination or inspection of the contents of any indirect communication: and
- *c.* diversion of any indirect communication from its intended destination to any other destination.<sup>164</sup>

From the above definition it is clear simply monitoring or inspecting or a person's communication can be considered as intercepted even when it is simply monitored so long as the intention is making the content of the communication available for a third party .i.e. anyone other than the sender, the receiver, or intended receiver. Monitoring is in turn defined as listening to or recording communications by means of a monitoring device.

What is intercepted might be direct or indirect communication. Direct communication is

(a) oral communication...between two or more persons which occurs in the immediate presence of all the persons participating in that communication; or

(b) utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication.<sup>165</sup>

The definition of interception of communication is not however exhaustive in a sense that anything, other monitoring, viewing and inspecting or redirecting one's communication, done with the purpose of making the content of the communication available for a third party constitutes interception. All one needs to prove is that the act was undertaken with above intention in mind.

Interception or monitoring devices are defined as 'electronic, mechanical or other instrument, device, equipment or apparatus' which on its own or in

---

<sup>164</sup> Section 1 of Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2000.

<sup>165</sup> Section 1 of RICA.



combination with others is used or can be used to intercept any communication.<sup>166</sup> This definition however excludes those devices that a telecom company provides its customers or that one purchases in order to be able to communicate with others. These might include cellular phones. Moreover, hearing aids that are used by those who have hearing impairment cannot be used as interception devices even if they are capable of being as such.<sup>167</sup>

Indirect communication on other hand is 'the transfer of information' through postal or telecommunication service. This might include a message or any part of a message which might take the form of speech, music or other sounds, data, text, visual images, whether animated or not, signals, or radio frequency spectrum.<sup>168</sup>

Obtaining or providing information relating to one's real-time or archived communication is also considered as a form interception. This is not about the content of the communication itself. It is rather information about real-time or archived communication of a customer which may be obtained or provided on an ongoing basis, as it becomes available. Included within the definition of interception of communication is also encrypting or having encrypted one's decrypted information.

#### 2.10.2. Principle in the RICA on interception of communication

The Act, as a matter of principle, prohibits interception of communication of any kind.<sup>169</sup> RICA also prohibits a telecommunication service provider or its employees from intentionally providing information relating to real time of archives communication to anyone except the person.

---

<sup>166</sup> *Ibid.*

<sup>167</sup> *Ibid.*

<sup>168</sup> *Ibid.*

<sup>169</sup> Section 2 of RICA.

### 2.10.3. When is interception of communications allowed?

RICA envisages that one's communication might be intercepted, therefore, monitored, viewed, inspected, examined or in case of indirect communication, redirected, or his/her real-time or archived communication related information provided to another, with or without interception direction or real-time or achieved communication related depending on the circumstances of the interception and the party who is conducting the interception. To this effect it enjoins telecommunication service providers, at their own expense, to provide telecommunication services that can be intercepted. Put differently, it is prohibited for a telecom company to make its services interception-immune. Telecom companies are also required to install a system that stores all relevant information about the communication of their customers.<sup>170</sup>

Moreover, to make interception of communication possible RICA requires telecom companies to obtain all relevant information about their customers and keep such records. The information includes the person full name, address, ID card number, and a copy of the customer's ID card in which his pictures are clearly visible. In case juridical person, the details of the person representing it should be kept.<sup>171</sup>

It provides a long list of substantive requirements and procedural guidelines for doing so. In general interception of communication can be undertaken with or without interception directions.

### 2.10.4. Interception of communication without 'interception direction'

RICA provides some 11 grounds based on which interception of communication can be legally conducted without the need to secure an

---

<sup>170</sup> Section 30(1) of RICA.

<sup>171</sup> Section 39 of RICA.

interception direction.<sup>172</sup> The Act allows one to intercept a communication that he/she is a party to so long as the interception is not intended for the purpose of committing offence. This does not however work for law enforcement agents, including a member of the police force, defence force, or one having prosecuting authority. As a rule, these cannot intercept a communication even if they are parties the communications. A law enforcement agent may intercept communication that he/she is a party to without interception direction if he/she believes that:

- a serious offence has, is being or will be committed,
- to gather information regarding actual or potential threats to public health, national security or national economic interest
- when so asked to assist by a competent authority of the republic or based on international agreements, by competent authorities of another country, to intercept communications or gathering of information relating to organised crimes or terrorism
- To gather information concerning a certain property that is believed to be instrument to proceed of serious crimes<sup>173</sup>

RICA allows one, who is not however a law enforcement agent, to intercept a communication to which he/she is not a party after securing a written consent of one of the parties.<sup>174</sup> Again as a rule one's written consent is not sufficient for a law enforcement agent to intercept communication without interception direction. Over and above the written consent, the law enforcement agent needs to be satisfied that a serious crime is being or about to be committed and that the interception is necessary for thwarting the crime or for subsequent investigation.<sup>175</sup>

The other ground of interception of communication without interception direction related to indirect communication which relates to conducting the

---

<sup>172</sup> Interception direction is a document issued by a designated judge to authorise 'the interception, at any place in the Republic, of any communication in the course of its occurrence or transmission. A designated judge may issue interception direction in writing or orally.

<sup>173</sup> Section 4(2) and section 16(5) of the RICA.

<sup>174</sup> Section 5(1) of RICA.

<sup>175</sup> Section 16(5) of RICA.

business. According to Padayachee this provision is particularly relevant for employer-employee relationship in that as far as it is related to 'the monitoring and/or accessing of employee's emails, monitoring of internet usage and recordings of telephone calls'.<sup>176</sup> This means employers are allowed to intercept indirect communication; provided that such communication relates to a transaction entered into in the course of business, conducted with explicit or implied knowledge of the employees that their communication might be intercepted and that the communication system is provided for the use 'wholly or partly in connection with that business'.<sup>177</sup>

A law enforcement officer may intercept, or request a telecommunication provider to intercept a certain communication, without interception direction, if he/she believes that one of the parties to the communication seeks or threatens to cause bodily harm on another or seeks or threatens to take his/her own life.<sup>178</sup> The law enforcement officer must be of the opinion that given the urgency of the matter, there is not time to make an application for direction of interception communications and that he/she needs to take swift measure.<sup>179</sup> In such cases the law enforcement agent is authorised to intercept the communication himself or 'may orally request a telecommunication service provider to route duplicate signals of indirect communications specified in that request to the interception center designated therein'.<sup>180</sup> The telecommunication provider is under legal obligation to carry out what the law enforcement agents' requests in this respect. In such cases the officer is required to provide the telecommunication service provider with a written note confirming the requests for interception.<sup>181</sup> And the latter is expected to submit an affidavit to a judge explaining what it did in terms of intercepting the said communication.<sup>182</sup> Interception can take place for the purpose locating individuals involved in an accident. One who has the

---

<sup>176</sup>Padayachee C. (2015) Employees right to privacy verses the Employer's Right to Monitor Electronic Communication in the Workplace (Unpublished Masters thesis), 57.

<sup>177</sup>Section 6(1) of RICA.

<sup>178</sup> Section 7(1) (a) of RICA.

<sup>179</sup> Section 7(1) (b) of RICA.

<sup>180</sup> Section 7(1) (c) of RICA.

<sup>181</sup> Section 7(3) of RICA.

<sup>182</sup> Section 7(4) of RICA.

responsibility of installing or maintaining telecommunication equipment, as part of discharging his/her duties, monitor signals if doing so is necessary for discharging installing or maintain the telecommunication equipment.<sup>183</sup> Also, one who is charged with controlling radio frequency may intercept if and when doing so is necessary for discharging his/her duty.<sup>184</sup>

The other ground of interception of communication without prior authorisation is when one of the parties to the communication or another person is believed to be involved in an emergency situation and there is a need to determine his/her location. The emergency that the law contemplates include one being seriously injured or his/her life being or likely to be endangered.<sup>185</sup> A law enforcement agent may orally request the telecommunications service provider to intercept the communication and locate the person when and if he/she believes that locating the party of the communication would be of assistance for rescuing the person whose life is endangered.<sup>186</sup> The telecommunication service provider has a legal obligation to comply with the agent's request. Once the rescue operation is over and as soon as practicable, the agent is required to provide the telecommunication service provider that with a written confirmation that he/she has made the above request.<sup>187</sup> And the telecommunication service provider is required to submit a written affidavit to a designated judge about the request the law enforcement agent made regarding intercepting communications and what it did to comply with the request.<sup>188</sup>

RICA also allows a telecommunication service provide to intercept of communications without the need to secure interception direction for the purpose of installing or maintaining devices that are necessary for telecommunication services.<sup>189</sup> A person who is appointed as inspector as per the Independent Communications Authority of South Africa Act, or is given the

---

<sup>183</sup> Section 10 of RICA.

<sup>184</sup> Section 11 of RICA.

<sup>185</sup> Section 8(1) (b) of RICA.

<sup>186</sup> Section 8(1) (b) (i) of RICA.

<sup>187</sup> Section 8(4) of RICA.

<sup>188</sup> Section 8(5) of RICA.

<sup>189</sup> Section 10 of RICA.

responsibility of managing radio frequency spectrum the Electronic Communications Act, is also authorised to intercept communications the course of performing its duty. It can specially 'monitor a signal or radio frequency spectrum relating to an indirect communication which is transmitted over radio, where it is reasonably necessary for that employee to monitor that signal or radio frequency spectrum for purposes of identifying, isolating or preventing an unauthorised or interfering use of such a signal or frequency or of a transmission'.<sup>190</sup>

#### 2.10.5. Providing real-time and achieved communications related information

As was mentioned above, the RICA as rule prohibits telecommunication service providers from intentionally allowing another to access one's information regarding his/her real time or achieved information.<sup>191</sup> The exception to this rule is that a telecommunication service provider may allow the customer to whom the real-time or archived communication-related information relates, to have access to the information.<sup>192</sup> It can also provide such information when authorized to do so, in writing, 'on each occasion, and subject to the conditions determined by the customer concerned'.<sup>193</sup> Otherwise, as will be seen below, the telecommunication provider can allow others to have access to the information relating to one of its customer's real time or achieved communication, when it is so required by direction

#### 2.11. Interception of communication with 'interception direction'

Section 3 provides that one's communication may be intercepted by an 'authorised person' or, in case of postal communications, by postal service provider. The authorised person or postal service provider can intercept one's communication only after securing 'an interception direction'.<sup>194</sup> An

---

<sup>190</sup> Section 11 of RICA.

<sup>191</sup> Section 12 of RICA.

<sup>192</sup> Section 13 of RICA.

<sup>193</sup> Section 14 of RICA.

<sup>194</sup> Section 3(b) of RICA.

interception direction is a direction that is issued by a designated judge – who is a retired High Court judge or any retired judge who is designated by the Minister of Justice to perform the functions of a designated judge - authorising the interception, at any place in the Republic, of any communication in the course of its occurrence or transmission.<sup>195</sup> The direction may authorize a member of the South African Service, a member of the defence force, a member of the intelligence service to authorise such interception.<sup>196</sup> When the interception direction may also include a decryption direction when application for interception direction also includes for such direction.<sup>197</sup> The direction in principle needs to be issued in a written form.<sup>198</sup> However in some cases it may take an oral form.<sup>199</sup>

In some cases, intercepting one's postal communications may require entering into a certain premise. Intercepting one's telephonic communication may also require installing interception devices in a certain premise, for instance, the house or office of the person whose communication is to be intercepted. In such cases the state agent who seeks to undertake the interception needs to secure entry warrant.<sup>200</sup> The agent may submit application for entry warrant to the designated judge while applying for the direction of interception of communication. He/she may also apply for entry warrant after the interception direction is issued. In the latter case, the state agent has to attach with his/her application proof that shows that an interception direction has been issued. The designated judge may thus issue an entry warrant if he/she is satisfied that the state agent is making the application for entry warrant only to undertake what he/she has mentioned in his/her application.<sup>201</sup> The judge is required to refuse the application for If the judge has a reason to believe that the entry warrant will be used for a purpose other than installing interception device. Moreover, the designated judge should be satisfied that installing interception devices in the premise that is

---

<sup>195</sup> Section 1 of RICA.

<sup>196</sup> Section 26 of RICA.

<sup>197</sup> Section 21(3) of RICA.

<sup>198</sup> Section 23(1) of RICA.

<sup>199</sup> Section 23(7) of RICA.

<sup>200</sup> Section 22 of RICA.

<sup>201</sup> Section 22(3) of RICA.

indicated in the entry warrant is critical in order to intercept the communications that is authorised under the interception direction.<sup>202</sup> If the interception of communication that is authorized by the interception direction can be undertaken without the need to entering a given premise, then the judge has to refuse the application for entry warrant.

#### 2.11.1. Procedure of securing interception direction

In order to secure interception direction, one has to make a written application to a designated judge. The application for interception direction may also include a request for a decryption direction.<sup>203</sup> RICA requires that the application for interception direction to contain detailed information about the identity of the state agent applying for the direction, the person whose communication is intercepted, the postal or telecommunication provider to whom the direction is addressed, the grounds for the application and other relevant facts.<sup>204</sup> When the application for interception direction is accompanied by an application for decryption direction,

Before issuing an interception direction the designated judge must be satisfied that there is a reasonable ground to believe that: a serious offence has been, is being or will probably be committed. It must be showed that 'the gathering of information concerning an actual or potential threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary'.<sup>205</sup> The judge may issue the interception direction if the application for the direction is due to 'the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, as per international treaties or considering the country's

---

<sup>202</sup> Section 22(4) of RICA.

<sup>203</sup> Section 21 of RICA.

<sup>204</sup> Section 16(2) of RICA.

<sup>205</sup> Section 16(5) of RICA.



interest.<sup>206</sup> The judge must also be satisfied that the interception communication is useful for obtaining the relevant information and that other investigative procedures have been applied and have failed to produce the required evidence or reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence and that the offence therefore cannot adequately be investigated, or the information therefore cannot adequately be obtained, in another appropriate manner.

It needs to be in writing. It can be given for a period not exceeding three months at a time and the direction should specify other restrictions.

The interception direction may be a real-time communication-related direction or/and archived communication-related direction or a combination of two or more of these. Real time communication-related information is information that a telecommunication service provider retains before, during and after a transmission of indirect communication.<sup>207</sup> Hence real-time communication-related direction involves a direction to obtain such information.

### **3.6. Conclusion**

Various global and national security related matters have led the government of South Africa to the adopt RICA. The national context that led to the adoption of RICA was the ever-increasing crime rate in the country which was in part related to the increasing sophistications of the means that criminal use for committing crimes. Important in this regard is digital communications including mobile devices such as cell phones. The global context was related to international terrorism. Even if South Africa has not been thus far the target of international terrorism, it was found necessary to adopt the required legislative framework for combating it. RICA was thus adopted for this purpose.

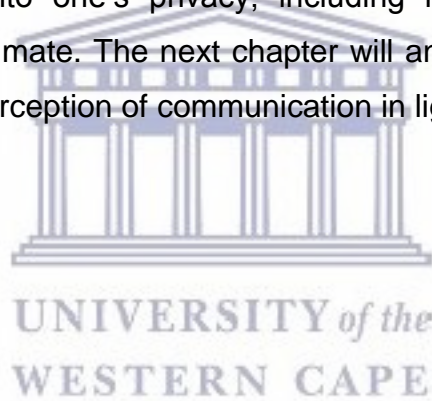
---

<sup>206</sup>Section 16(5) (a) (iv) of RICA.

<sup>207</sup> Section 18 of RICA.

RICA as rule prohibits the interception of anyone's communication. As an exception to this rule, it also provides that one's communication can be intercepted with or without interception direction. Interception of direction can be undertaken without the need to secure interception direction from a judge by one who is a party for the communication, by a state agent for the purpose of preventing crimes or locating one who is in distress and the like. In other cases, interception of communication can take place only when so authorised by designated judge. RICA details the substantive and procedural requirement that need to be fulfilled before the designated judge authorise the interception of communication of an individual.

In chapter two the principles of legality (generality, publicity and precision), necessity, and proportionality have been identified as the basis for assessing whether interference into one's privacy, including intercepting his or her communications is legitimate. The next chapter will analyse the provisions of RICA that authorise interception of communication in light of those principles.



## **Chapter 4**

### **RICA and its implementation in the light of legality, necessity and proportionality**

#### **4.1. Introduction**

Whether the RICA is in line with the right to privacy, especially information and communication privacy of citizens and residents of South Africa is the main question in this paper. As part of answering this question, chapter 2 dealt with the concept of 'privacy' and 'communications privacy'. The right to privacy as recognised and protected under the South African Constitution and the ICCPR was also discussed. The various conditions that need to be fulfilled before one's right to privacy, including one's right to communication and information privacy, can be legitimately limited, restricted, , were highlighted. The conditions are legality, necessity, and proportionality. It was also shown that there must be a procedural safeguard to ensure that the conditions of legality, necessity and proportionality have been met before and after one's right to communication and information privacy is restricted. The most common procedural safeguard in this respect is the requirement of judicial approval before someone's right to communication privacy is restricted and judicial oversight while the restriction of one's privacy is taking place. Moreover, in chapter 3, provisions of the RICA that are putting limitation on individual's right to communication privacy were discussed.

This chapter is designated to analyse the RICA in light to the conditions that provided in the ICCPR and the South African Constitution i.e. legality, necessity, and proportionality. The procedural safeguards will also be analysed in light of the standards set in the Constitution and ICCPR. The chapter will also discuss the practice in terms how South Africa's security agencies and agents exercise the power they are given under the RICA.

The chapter begins with analysis of RICA in light of legality, necessity, and proportionality. It then discusses procedural safeguards and finally, some issues associated with the practice of implementing the RICA are discussed.

## **4.2. Restriction of communication privacy under RICA: Legal, necessary and proportional?**

### **4.2.1. Legality**

In chapter 2, it was stated that one's right can be restricted only by law.<sup>208</sup> As was implied in the ICCPR, the right to privacy can be limited only in accordance with law. The South African Constitution provides a stringer clause as far as the requirement of legality is concerned. It provides that a piece of legislation that seeks to restrict one's right to privacy has to be a law of general application. This raises the question that; is RICA a law of general application?

#### **4.2.1.1. *Is RICA a law of general application?***

As was stated in chapter two,<sup>209</sup> a law that aims to restrict one's right in the Bill of Rights needs to be a 'law of general application'. The term 'law of general application' was defined to mean that the law should be general (that is applicable to everyone), public, precise, and non-arbitrary.

#### **4.2.1.2. Generality**

RICA is an Act of Parliament of South Africa. Parliament is authorised under the Constitution to adopt laws on matters that are within the mandates of the national government. RICA principally deals with interception of communications. Matters relating to communications are not listed in Schedule 4 or Schedule 5 of the Constitution. This means such matters are neither exclusive provincial mandates nor concurrent national and provincial matters. These matters are therefore by definition national matters within the exclusive legislative competence of Parliament. RICA is thus a piece of legislation that is properly adopted by the National Assembly of South Africa.

---

<sup>208</sup> Chapter 2, section 6.1.

<sup>209</sup> Chapter 2, section 6.1.

Moreover, Section 44(2)(a) provides that Parliament may legislate on matters that are within the exclusive competences of provinces or concurrent national and provincial matters if doing so is necessary for the purpose of maintaining national security. In short RICA is a piece of legislation that is appropriately adopted by Parliament.

As was stated in chapter 2,<sup>210</sup> it is unclear whether or not directives or guidelines issued by government agencies or statutory bodies qualifies 'as laws of general application'. There is however a consensus that an Act of Parliament, if it fulfills the others requirements, can be considered as law of general application. RICA is not an executive decree, directive or guidelines that are adopted by a ministry or some other state agency. It is a Parliamentary Act. This gives RICA a character of generality.

Moreover, RICA is a law of general application in a sense that it is applicable on or against every natural and juridical person within South Africa. The provisions in the RICA are formulated in such a manner that they are applicable on everyone. For instance, Section 2 of the RICA, which is the main principle of the Act, provides that 'no person may intentionally intercept or attempt to intercept or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission'.<sup>211</sup> And section 3 which is one of the exceptions to the above principle provides that 'any authorised person who executes an interception direction or assists with the execution thereof may intercept any communication'. A postal service provider to whom an interception direction is addressed, may intercept any indirect communication, to which that interception direction relates'. The other provisions allowing or authorizing interception of communication start with 'any person'. This shows that the RICA does not target any individual or any certain or ascertainable group of people. In other words, RICA is not a 'bills of attainder' in that it is not directed towards 'specific named individuals or easily ascertainable members

---

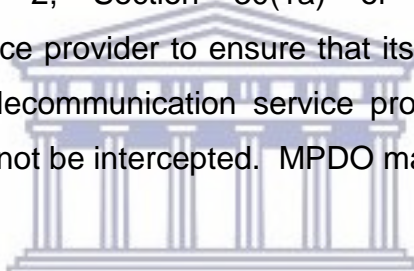
<sup>210</sup> Chapter 2, section 6.1.

<sup>211</sup> Section 2 of RICA.

of a group for punishment'. This give the RICA the character of being 'general'.

#### 4.2.1.3. Precision

A law providing for restriction of one's privacy, in this case intercepting one's communication, should be clear and precise and not lend itself for too much interpretation. Most of the operative terms of the RICA are clearly defined in section 1 of the RICA.<sup>212</sup> However, some of the provisions in the RICA are criticised for being too vague. Media Policy and Democracy Project (MPDP), in its 2015 report, maintains the grounds under RICA for issuing interception direction are vague which open the gate for abuse.<sup>213</sup> The MPDP further argues that Section 30(1)(a) of the RICA is extremely vague. As was discussed in chapter 2, Section 30(1a) of RICA requires every telecommunication service provider to ensure that its services are capable of being intercepted. A telecommunication service provider cannot, therefore, install a system that cannot be intercepted. MPDO maintains:



'Section 30(1a) is very vague in the sense that it simply says 'capability of being intercepted'. It does not specify what it is required by telecommunication service providers. This violates the Necessary and Proportionate Principle on integrity of communications and systems which suggests that 'states should not compel service providers or hardware or software vendors to build surveillance or monitoring capabilities into their systems, or to collect or retain particular information purely for state communications surveillance purposes"<sup>214</sup>

---

<sup>212</sup> *Ibid.*

<sup>213</sup> Admire M. and Jane D. (2015) An Analysis of the communications surveillance legislative framework in South Africa Media Policy and Democracy Project (2015) 20.

<sup>214</sup> *Ibid.*

#### 4.2.1.4. Accessibility of the law

One of the four requirements of generality is accessibility of the law for the general public. RICA fulfils this requirement. RICA was published on 23 January 2003 in the Government Gazette of South of Africa after it was assented by the President.<sup>215</sup> As indicated in the Gazette, the RICA was published for 'general information'.<sup>216</sup> The Act is available in hard copies. It can also be downloaded from the internet for free. The requirement of 'accessibility' is thus fulfilled.

#### 4.2.1.5. Non-arbitrariness

As was stated in chapter 2, the requirement of 'non-arbitrariness' has to do with ensuring that a law does not provide unrestrained power of infringing one's right to a state agent thereby inviting for arbitrary actions from state agents.<sup>217</sup> There are some provisions in the RICA that open a room for some arbitrariness. Section 7 authorises any law enforcement agent to intercept on any communication or may orally request a telecommunication service provider to do so without the need to apply for interception direction. He/she can do so if he/she 'is satisfied that there are reasonable grounds to' one has sustained or has been threatened with serious bodily harm and that he/she is 'of the opinion' the matter is so urgent that 'it is not reasonably practicable' to make an application for interception direction'. Likewise, section 8(1) (c) authorises a law enforcement agent to intercept or request a telecommunication service provider to intercept one's communication, without the need to apply for interception direction, for the purpose of locating the person who is in an emergency situation if the former is 'of the opinion that determining the location of the sender is likely to be of assistance in dealing with the emergency'.

---

<sup>215</sup> Government Gazette of the Republic of South Africa Vol. 451 Cape Town 22 January 2003 No. 24286.

<sup>216</sup> The Presidency No. 122 22 January 2003 It is hereby notified that the President has assented to the following Act, which is hereby published for general information.

<sup>217</sup> Chapter 2, Section 6.1.

Clearly the terms ‘if he/she is of the opinion’ and ‘if he/she is satisfied that there are reasonable grounds to’ seem to allow a wide discretion to the law enforcement agent to determine whether or not he/she can intercept one’s communications without the need to secure interception direction.

Certainly, providing such discretion to state agents in certain circumstances is necessary. However, there is also a chance that state agents may be arbitrary in terms of exercising the power to intercept communication without securing interception direction from a judge. As will be discussed later,<sup>218</sup> the RICA provides a procedural safeguard to prevent the temptation for state agents to abuse their power of intercepting one’s communication without interception direction which is a *post facto* judicial oversight. The oversight mechanism is however considered as too weak. As the HRC states:

‘The Committee is concerned about the relatively low threshold for conducting surveillance in the State party and the relatively weak safeguards, oversight and remedies against unlawful interference with the right to privacy contained in the 2002 Regulation of Interception of Communications and Provisions and Provision of Communications Related Information Act (RICA).’<sup>219</sup>

The other related problem relates to the fact that RICA not only allows but also requires telecommunication companies, which are often privately owned, to retain and store data about the communication of their clients. As will be discussed below,<sup>220</sup> this raises a question of proportionality as what they are required to store bulk data relating to the communication of their clients. Over and above the issue of proportionality, the fact that telecommunications are allowed and required to store every communication data is feared that it could lead to arbitrariness.

---

<sup>218</sup> Section 4.1.4.

<sup>219</sup> UN Human Rights Committee Concluding observations on the initial report of South Africa CCPR/C/ZAF/CO/1 27 April 2016.

<sup>220</sup> Section 4.1.3.



Moreover, whether individuals who are by law allowed to have access to privileged information about others can be targets of interception. The issue here is whether professionals such as lawyers, doctors, priests who are often entrusted with other people's confidential information can be targets of interception. This is not clearly outlined in the RICA and the fact that these are not explicitly excluded from being targets of interception leads to arbitrariness and raises constitutional issues.

#### 4.2.2. Necessity

As indicated in chapter 2, one's privacy can be limited only if and when it is necessary for achieving some legitimate purpose.<sup>221</sup> Nowhere in the RICA is indicated why it was necessary to adopt this piece of legislation. The preamble of the Act simply states what the purpose of the Act was, not why it was necessary to adopt this specific piece of legislation.<sup>222</sup>

As was discussed in chapter 3, the South African government forwards a two-pronged argument as far the need to adopt the RICA is concerned. The first argument is linked to the ever-increasing domestic crime in the country.<sup>223</sup> South Africa is among countries with very high crime rate in Africa.<sup>224</sup> The criminals are using increasingly sophisticated ways and devices for committing crimes. Preventing and investigating crimes in the country has

---

<sup>221</sup> Chapter 2, section 6.2.

<sup>222</sup> 'To regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information; to regulate the making of applications for, and the issuing of, directions authorising the interception of communications and the provision of communication-related information under certain circumstances; to regulate the execution of directions and entry warrants by law enforcement officers and the assistance to be given by postal service providers, telecommunication service providers and decryption key holders in the execution of such directions and entry warrants; to prohibit the provision of telecommunication services which do not have the capability to be intercepted; to provide for certain costs to be borne by certain telecommunication service providers; to provide for the establishment of interception centres, the Office for Interception Centres and the Internet Service Providers Assistance Fund; to prohibit the manufacturing, assembling, possessing, selling, purchasing or advertising of certain equipment; to create offences and to prescribe penalties for such offences; and to provide for matters connected therewith'.

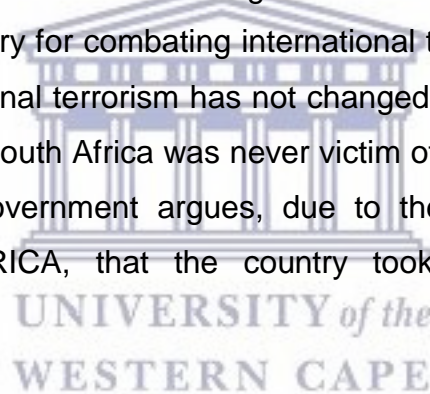
<sup>223</sup> Chapter 3, section 3. Cohen (2001) 4.

<sup>224</sup> Africa Check *Factsheet: South Africa's crime statistics for 2016/17* <<https://africacheck.org/factsheets/south-africas-crime-statistics-201617/>>. Accessed on 17 November 2017.

necessitated the interception of communication without which the crime rate is likely to worsen.<sup>225</sup>

It is also important that the RICA was adopted in the early 2000. Around that time there was a high spike in crime rate in the country. Hence given the high crime rate in the country and the increasing sophistication of the criminals, interception of communication appeared to be necessary as a crime preventing and investigating tool.<sup>226</sup>

The other argument regarding the necessity of RICA is based on the global security context. As was stated in chapter 3, RICA was adopted a year after the 9/11. The terrorist attack on the World Trade Centre, in New York, had shocked many and prompted almost every country to adopt several pieces of security minded and antiterrorism legislation. South Africa also found adopting RICA necessary for combating international terrorism. The situation with regard to international terrorism has not changed since 9/11, if it has not gotten worse. Indeed, South Africa was never victim of international terrorism. This is in part, the government argues, due to the legislative and other measures, including RICA, that the country took in order to prevent terrorism.<sup>227</sup>



#### 4.2.3. Proportionality

As was discussed in chapter 2, proportionality is about ensuring that the limitation that is imposed on the right to privacy is 'reasonable and justifiable in an open and democratic society' based on human dignity, equality and freedom' which is assessed, among others, by taking into account 'the importance and purpose of the limitation', whether the limitation is linked to the purpose that is to be achieved, and the extent or degree of limitation that

---

<sup>225</sup> Cohen (2001) 4.

<sup>226</sup> *Ibid.*

<sup>227</sup> Ducan J. (2016) Reports of the death of communications privacy are greatly exaggerated: reflections on recent UN Human Rights Committee's findings on South Africa. Available at, <https://www.privacyinternational.org/node/850>. Accessed on 15 Oct 2017.

is allowed. The limitation should be the least intrusive limitation that can achieve the purpose.

As it is clear from the discussion in the previous section there is little disagreement on the need to have some kind of legislative measure that allows law enforcement agencies to be able to combat domestic crimes and international terrorism. Even some privacy minded right groups understand that combating crime and terrorism might involve intercepting individuals' communications. Everyone's fear seems that RICA puts excessive limitations on individual's right to communication privacy.

Indeed, whether or not the interception of one's communication is proportional is something that can and needs to be determined on case by case basis by taking into consideration what the interception is meant to achieve, how intrusive it is and the like.<sup>228</sup> However, there are certain problems in RICA that raise issues pertaining to lack of proportionality. The fact that telecommunication service providers can and are required to store every data relating to the communication of each of their clients raises issue of proportionality.<sup>229</sup> Hence the UN Human Right Committee expressed its concerns 'about the wide scope of the data retention regime under' the Act RICA.<sup>230</sup> Some argue that such indiscriminate retention of data is unnecessary for preventing or investigating crimes and disproportionate to

---

<sup>228</sup> Chapter 2, section 6.3.

<sup>229</sup> '[T]elecommunications interception was taken to include the interception of data communications (communicated via mobile communications and fixed-line networks), voice communications (communicated via landline or mobile networks) and metadata (also known as callrelated data, which includes the time of call, duration of call, caller identity, receiver identity and location of the caller and receiver). Interception can be categorised according to the number of persons targeted simultaneously. To this end, a distinction is made between targeted interception, on the one hand, and bulk interception (also known as mass interception, blanket interception, or massive, passive interception) on the other. Targeted interception refers to the monitoring of specific individuals or groups of individuals, usually for a set period. Bulk interception is ongoing monitoring, recording and storing of the communications of large sections of the population. With bulk interceptions, millions of people's communications can be recorded simultaneously. The South African government is known to possess equipment to carry out both types of interception'. Swart *H Communications surveillance by the South African intelligence services* (A report commissioned Media Policy and Democracy Project, a joint project of the Department of Journalism, Film and Television at the University of Johannesburg and the Department of Communication Science at Unisa).

<sup>230</sup> Human Rights Committee (20016) Concluding observations on the initial report of South Africa.

when seen in light of the right of privacy of the person the history of whose communication is stored. As United Nations High Commissioner for Human Rights in its states, telecom service providers, which are often under private ownership, are authorized to retain data.<sup>231</sup> The access and use of such data is not 'tailored to specific legitimate aims' which is 'neither necessary nor proportionate'.<sup>232</sup>

Regarding the bulk retention of information about subscriber's communication, the European Court of Human Right, acknowledges that the use of modern investigative techniques to fight serious crimes is important, '[such an objective of general interest ... cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data ...]'.<sup>233</sup> The Office of the High Commissioner for Human Rights, has echoed similar sentiments that, while states may be allowed to undertake intrusive surveillance that has a legitimate aim and appropriate safeguards, "[m]ass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime".<sup>234</sup>

Moreover, in the *Digital Rights Ireland v Minister for Communications* in which the Court of Justice of European Union (CJEU) found that the retention of customers' data by service providers for up to two years breached the rights to privacy and data protection under international law. The court was the view that the directive that authorised such mass surveillance amounted to wide range and particularly serious interference with the rights to privacy and data protection "without such interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary".<sup>235</sup> It

---

<sup>231</sup> United Nations High Commissioner for Human Rights *The right to privacy in the digital age; Report of the Office of the United Nations High Commissioner for Human Rights*

<sup>232</sup> *Ibid.*

<sup>233</sup> LawBizTech (2017) *Privilege: bolstered by the EU Court of Justice*. Available at <http://www.lawbiztech.co.uk/2017/01/23/privilege-bolstered-by-the-eu-court-of-justice/>. Accessed on 25 Oct 2017.

<sup>234</sup> Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age: Report of the OHCHR*, U.N. Doc. A/HRC/27/37.

<sup>235</sup> *Digital Rights Ireland v Minister for Communications* C-293/12 and C-594/12.

should be noted that RICA is even worse in this regard since it requires the retention of bulk information about communication for five years.

In short even it can be said that RICA is a law of general application, and necessary, the provisions that allow the bulk retention of everyone's communication data seems to put its proportionality into question.

The other challenge with RICA relates to the authorisation of decryption of encrypted information. As was discussed in chapter 3,<sup>236</sup> having decrypted one's encrypted information falls within the definition of interception and allowed under RICA. RICA authorizes the decryption of encrypted information following the procedure that is used for interception of communication.<sup>237</sup> A decryption key holder is also required to provide assistance in this regard. However, allowing a backdoor into one's encrypted information has been controversial in other jurisdictions and said to be too intrusive. For instance, there was huge uproar when President Obama disclosed his intention to require information technology companies to disclose their decryption key for encrypted information when so asked by authorities.<sup>238</sup> Finally, he abandoned his intentions to have a piece of legislation passed 'requiring companies to decode messages for law enforcement'.<sup>239</sup> Moreover, the Special Rapporteur complemented the US and Netherland's governments for 'the restraint demonstrated in their unwillingness to permit the law to be used to engineer back-doors in communication'.<sup>240</sup>

---

<sup>236</sup> Section 3.4.1.

<sup>237</sup> Chapter 3, section 4.3.1.

<sup>238</sup> Nakashima E. and Peterson A. (2015) The Obama administration opts not to force firms to decrypt data. Available at [https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699\\_story.html?utm\\_term=.5ee87d753ace](https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html?utm_term=.5ee87d753ace). Accessed on 22 October 2017.

<sup>239</sup> *Ibid.*

<sup>240</sup> 'On the 4<sup>th</sup> January 2016, it was announced that the Dutch government has formally opposed the introduction of backdoors in encryption products. A government position paper, published by the Ministry of Security and Justice and signed by the security and business ministers, concludes that "the government believes that it is currently not appropriate to adopt restrictive legal measures against the development, availability and use of encryption within the Netherlands." The conclusion comes at the end of a five-page run-through of the arguments for greater encryption and the counter-arguments for allowing the authorities access to the information. "By introducing a technical input into an encryption product that would give the authorities access would also make encrypted files vulnerable to criminals, terrorists and foreign intelligence services," the paper noted. "This could have undesirable

#### 4.2.4. Procedural safeguards

As was stated in chapter two,<sup>241</sup> the limitation of one's right to privacy can be conducted under certain procedural safeguards that are designed to prevent arbitrariness and abuse of power by state agents. The procedural safeguards operate both prior to and after one's communication is intercepted. The pre-interception procedural safeguards are meant to ensure that there is a legitimate cause that justify the interception. The post-interception procedural safeguards are intended to ensure that the interception was conducted for the intended purpose only and there is no overreach by state agents while conducting the interception.

The pre-interception procedural safeguard is securing interception direction from a judge who is appointed to deal with such matter. RICA as a principle prohibits interception of communication. If it has to be done, RICA provides that as rule interception of communication can be conducted only after interception direction has been secured. As has been discussed in chapter 3, RICA provides a long list of conditions that have to be fulfilled before a judge can provide interception direction. Without such procedural safeguards RICA would have been open for abuse by state agents.<sup>242</sup> Hence the pre-interception of communication procedural safeguard has been clearly provided in RICA.

RICA also has post-interception procedural safeguards. As have been discussed in chapter 2, a state agent might be forced to conduct interception

---

consequences for the security of information communicated and stored, and the integrity of ICT systems, which are increasingly of importance for the functioning of the society.'

<sup>241</sup> Chapter 2, 6.4.

<sup>242</sup> 'The Court considers that the manner in which the system of secret surveillance operates in Russia gives the security services and the police technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorisation. Although the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system, the Court considers that a system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great.'

of communication without securing interception direction due to emergency situation or other reason. In such cases the fact that interception of communication has taken place and the reason for doing so has to be communicated to the designated judge. This a post-interception procedural safeguard.

A number of criticism are however levelled with respect to the post-interception procedural safeguards. The first criticism against RICA in this respect relates to the fact that it does not require that state agents inform the person whose communications are intercepted the fact that his/her communications were indeed intercepted. Obviously, the state agents are not expected to inform the person that his/her communication is being intercepted while the interception is on-going specially if the interception is intended for the purpose of investigating crimes. Doing so might defeat the purpose of the interception. The problem is that state agents are not required to inform the person whose communication they intercepted even after the interception has been ceased and the investigation has been concluded. This is a serious constitutional flaw since it would not allow the person whose communication was intercepted to challenge the legality of interception.<sup>243</sup> In addition, under the HRC's *International Principles on the Application of Human Rights to Communications Surveillance*, state agents are required to notify the target person that they have applied for interception his/her communications.<sup>244</sup> Delay of notification would for instance only be justified if it would "seriously jeopardise" the purpose of the surveillance. This suggests that RICA, in this regard, falls short of international best practice.

Moreover, as Court of Justice of the European Union, in European Court of Human Rights, *Zakharov vs. Russia* stated, intercepting or retaining a subscriber's data, without his/her being informed 'is likely to cause the

---

<sup>243</sup> This was launched 'after global consultation with various stakeholders - requires notification of the application'.Botha C. (2017) *Cybercrimes and cybersecurity Bill*, Part 2 - Failing to address legislative shortcomings on the State's surveillance powers <<http://www.cfc.org.za/index.php/latest/751-article-the-cybercrimes-and-cybersecurity-bill>> accessed on 23 October 2017.

<sup>244</sup> *Ibid.*

persons concerned to feel that their private lives'.<sup>245</sup> It therefore negatively impacts on the right to freedom of expression of the subscriber.

The other flaw in the procedural safeguards under RICA relates to its silence of 'about the procedure state officials should follow when examining, copying, sharing, storing, etc., the intercepted data'.<sup>246</sup> In some cases, the data that is collected through interception might be of no value for the investigation. However, it is unclear whether the state agents are required to destroy or store such data. Nor does RICA provide a 'certifiable procedure for the data to be destroyed'.<sup>247</sup>

Moreover, as stated in the previous chapter, RICA provides a long list of requirements that have to be fulfilled before the designated judge provides a state agent an interception direction. However, it does not provide a procedure in which the designated judge may follow up whether the interception was used only for the purpose for the achievement of which it was authorised. Having authorised the interception, the judge goes out of the picture.<sup>248</sup> Indeed, the judge is authorised to require progress report with respect to the execution of entry warrant when interception requires entry into certain premise and that the judge has authorised such entry. The judge is not however authorised to require progress report on the interception that is conducted based on his/her interception direction. This is feared to allow state agents to use the interception direction for a purpose other than the one that it was intended for.

---

<sup>245</sup> *Zakharov vs. Russia*, No. 47143/06, available at, <http://hudoc.echr.coe.int/eng?i=001-159324>. Accessed on 23 October 2017.

<sup>246</sup> Botha C. (2017).

<sup>247</sup> *Ibid.*

<sup>248</sup> The Mathew Commission however states in its report that 'RICA reflects Parliament's views on appropriate safeguards to protect the right to privacy and prevent unjustified infringements of this right'. Matthews Commission Report, 194.



### 4.3. RICA in practice

The implementation of RICA has been a cause of for much uproar from individuals, journalists, and civil society organisations.<sup>249</sup> There are many who claim that the RICA has opened the gate for interference of individuals' privacy by state agents. Many also claim that state agents often disregard the requirements in the RICA and intercept individuals' communications illegally.<sup>250</sup>

Among those who argue that RICA itself is the problem are civil society organisations such as Right2Know, amaBhungane Investigative Journalism and the like. Their criticism of RICA is linked to what has been discussed above including RICA's shortcoming in terms of ensuring transparency by requiring a person whose communication is intercepted that the interception has taken place. This has been a cause for litigation and brought about constitutional challenge on RICA. The party that brought the constitutional challenge in the High Court against the RICA is amaBhungane Investigative Journalism. Its application was supported by a journalist in the name of Mr Sam Sol an investigative journalist. The constitutional challenge in this regard is that 'certain provisions of RICA unduly infringe on an individual's rights to privacy and access to courts'.<sup>251</sup> Mr Sol alleged that he suspected that communication between himself and the senior prosecutor investigating charges against President Zuma in relation to the Arms deal in 2009 were intercepted'. He was not however informed the fact that his communication was intercepted. He realized that his communication was indeed intercepted only when 'extracts of the intercepted communication later became public in Court papers'. He alleged that was never 'provided with the initial interception

---

<sup>249</sup> Saba A. (2017) Cop illegally bugged Sunday Times calls <<https://www.timeslive.co.za/sunday-times/news/2017-07-29-cop-illegally-bugged-sunday-times-calls/>> accessed on 26 October 2016; Botha C. (2017) Cybercrimes and Cybersecurity Bill: Better but still bad. Available at <http://www.politicsweb.co.za/news-and-analysis/cybercrimes-and-cybersecurity-bill-better-but-still>. Accessed on 23 October 2017

<sup>250</sup> *Ibid.*

<sup>251</sup> *Ibid.*

order or the information that the RICA judge considered to grant the interception order'.<sup>252</sup>

Moreover, there are reports that members of the South Africa Policy Service have used the 'the emergency-location services to spy on their rivals and love interests, and bypass the Rica process entirely'.<sup>253</sup> Having interviewed a former member of the SAPS the Mail & Guardian reported the following regarding how the members of the Police arbitrarily intercept people's communication.

'After leaving the police, he said, he maintained close ties with former colleagues at crime intelligence headquarters in Prieska Street, Erasmuskloof, in Pretoria. The links were useful for his work as a private investigator. Loots claimed that he could approach a contact at this office at any time and request information about, or the communication of, whoever he was investigating. Such information was usually obtained illegally through state facilities, he said. But things went sour. Loots claimed that, after a personal dispute, his contact had used the crime intelligence division's facilities to intercept his cellphone communication and access his bank accounts to sabotage his business and financial endeavours. He said he knew this because his former contact knew intimate details of his financial and legal affairs that he had not shared with her and which she could only have learned through state facilities. But there is another reason why Loots was certain that his communication was being intercepted. As a former member of the intelligence community, he said, he was

---

<sup>252</sup> *Ibid.*

<sup>253</sup> *RICA in South Africa: How big is Big Brother?* < [https://www.groundup.org.za/article/rica-south-africa-how-big-big-brother\\_1882/](https://www.groundup.org.za/article/rica-south-africa-how-big-big-brother_1882/)>. Accessed on 27 October 2017. *Secret state: How the government spies on you* < <https://mg.co.za/article/2011-10-14-secret-state/>>. Accessed on 27 October 2017

well aware that illegal interception was an everyday occurrence.<sup>254</sup>

Right2know reports several instances where the RICA was either abused or violated by state agents including in Mr Sol's case. The second case relates to the interception of the communication of Mr Mzilikazi wa Afrika and Mr Stephan Hofstatter. These two are journalist working for the Sunday Times. These journalists were investigating corruption in SAPS Crime Intelligence Division. Members of the SAPS requested from a judge interception direction by misleading the judge that the phones to be intercepted belonged to criminals. Using the interception direction, the policemen obtained the communication information of the two journalists. Bongani Cele, a crime intelligence officer in the SAPS, was found guilty of illegally intercepting the communications of the two journalists mentioned above. Right2know argues what led to this illegal act are the shortcomings in the RICA itself. It maintains.<sup>255</sup> first, RICA contains low threshold for issuing interception directions. This allows 'rogue' state agents to deceive designated judges. Even worse members of the intelligence community intercept communications without securing interception direction.<sup>256</sup> Second, victims of illegal interception cannot find out when their communications are intercepted since RICA does not require that they be informed of the interceptions. For instance, Afrika and Hofstatter were informed of the interception of their communication by sources other than the state agents.<sup>257</sup> Third, citizens can no longer communicate anonymously since, as per the requirement of RICA, their identity is registered to the SIM card. And journalist can no longer speak to 'to speak to confidential sources without compromising their identity'.<sup>258</sup>

The third case relates to one Paul Scheepers, formerly crime intelligence official. This person, while a member of the police force, was on the side

---

<sup>254</sup> *Ibid.*

<sup>255</sup> Saba. A. (2017) *Cop illegally bugged Sunday Times calls* <<https://www.timeslive.co.za/sunday-times/news/2017-07-29-cop-illegally-bugged-sunday-times-calls/>> accessed on 26 October 2016.

<sup>256</sup> *Ibid.*

<sup>257</sup> *Ibid.*

<sup>258</sup> *Ibid.*

working as private detective. This person allegedly supplied ‘falsified affidavits to a magistrate’ and obtained interception direction. And using the interception direction obtained ‘meta-data records of lawyers, senior cops, an individual from the financial services regulator, and other individuals’.<sup>259</sup>

The fourth case relates to the possible use by the police and individuals of a device called IMSI Catcher also locally known as ‘grabber’. This device is said to be ‘capable of sucking up data from thousands of mobile phones in a radius of up to several kilometres, and identify each user by their SIM card’. It is discovered that not only the intelligence community but also some individuals are in possession of such devices in South Africa. These devices can be and are being used illegally. The problem as far as RICA is concerned, the devices intercept the communication of everyone within a certain radius, indiscriminately, even when they are used for intercepting communications based on interception direction. ‘Therefore, even if a judge has authorised the surveillance of one particular person, when the device is used this way, it may violate thousands of other people’s privacy too.’<sup>260</sup> This is in clear violation of the RICA, which aims to limit interceptions, when needed, to specific individuals. The fact that the devices indiscriminately intercept everyone’s communication means that the right to privacy of those who happen to be within certain radius of the device, but who have nothing to do with the crime being investigated, would be automatically violated. As the Right2Know Campaign states:

‘South Africans need to be very worried about the possible existence of these devices in our society, and the extreme secrecy that surrounds them. Especially given the clear interest that our security agencies have in identifying and targeting people involved in protests, and the clear risk of abuse that these devices are capable of, they represent a huge risk to constitutional

---

<sup>259</sup> Right2Know Campaign (2017) *Case studies how communication has been abused in SA* <<http://www.r2k.org.za/2017/04/20/case-studies-communications-surveillance-abuse/>> accessed on 15 October 2017.

<sup>260</sup> *Ibid.*

rights to privacy. In any case, even if governments acquire this technology with ‘the best intentions’, the “Grabber” saga shows that such devices may end up in the hands of criminals, raising the question – should this technology exist at all?<sup>261</sup>

#### 4.4. Conclusion

The main takeaway from the discussion in this chapter is that RICA is adopted appropriately by Parliament. It is a law of general application in that it has generality. It is published in print and online and therefore it is accessible. Some of its provisions however lack precisions and therefore open the door for arbitrariness. Despite this, RICA, in general, can be considered to have fulfilled the requirement of legality. There is also a general agreement on the necessity of adopting RICA given the crime rate in the country and the global security situation that pose danger on the national security of the country. However, RICA’s requirement that all information regarding everyone’s communications be recorded and kept is clearly disproportionate measure. Moreover, RICA does not provide sufficient procedural safeguard against arbitrary interception. It does not require state agents to inform one whose communication they have intercepted about the interception. Thus, the person cannot challenge the legality of the interception his or her communication. Moreover, RICA does not authorise designated judge to follow up whether the interception of one’s communication that he or she authorised is carried out in accordance with RICA, the Constitution and the ICCPR.

Reports regarding the practical implementation of RICA show that state agents abuse their powers under RICA in disregard of the requirements in the piece of legislation.

---

<sup>261</sup> Right2Know Campaign (2015) *Does the government have ‘grabber technology’ ? We demand to know* < <http://www.r2k.org.za/2015/09/03/surveillance-device/> > accessed on 28 October 2017.

## Chapter 5

### Conclusion and recommendations

#### 5.1. Introduction

RICA, a piece of legislation that was adopted by Parliament in 2002, authorises state agents to intercept the communication of individual residents and citizens of the Republic of South Africa. The interception that is allowed under RICA also includes collecting metadata about the communication of everyone in the country. The main question this research paper sought out to answer was whether RICA was in line with the right to privacy as recognised under Article 17 of the ICCPR and Section of the South African Constitution. With a view to answering the above question, the paper raised several other sub-questions including what privacy is, why it is protected, whether and when it can be justifiably restricted, and the like. This chapter summarises the discussion in each chapter and brings out the conclusion and provides few recommendations.

#### 5.2. Conclusion

##### 5.2.1. Summary of chapters

In order to answer the above questions, the paper in chapter two discussed why privacy is. The discussion showed that at different time privacy was conceptualised differently. Initially it considered to be left alone. Later it was considered to be as one's liberty in personal matter. Latter the concept of privacy was extended to other matters including communication and information privacy. Privacy was protected since its protections affords one to develop his/her individuality, the innovation of modern means of communication impacts on lives of individual requiring putting limits on their intrusion in people's lives. Protection of privacy in the digital age is in particular important because, even though the advancement in digital technology creates immense convenience on the lives of people, by enhancing the surveillance capacity of the state, it has also exposed their privacy for interference by state agents and other individuals. The chapter also dealt with the right to privacy, in particular the right to communication and information privacy, as recognised in the ICCPR and the South African

Constitution. Both documents recognise the right to communication privacy of everyone. Yet, as any right, they both, impliedly or otherwise, provide that the right to privacy, including communication privacy, can be restricted so long as certain conditions are fulfilled. The conditions are legality, necessity, and proportionality and the existence some procedural safeguards that ensures that the conditions of legality, necessity and proportionality have been met before and after one's right to communication privacy is restricted or violated.

Chapter three dealt with the global and national context that led to the adoption of RICA. In this regard, the chapter discussed how the 9/11 attack on the World Trade Centre in New York influenced the adoption of several national security minded pieces of legislation in different countries in South Africa. Among such laws are those that allow state agents to intercept individuals' communication with or without judicial warrant. It then discussed interception of communication by state agents in the political history of South Africa. The apartheid system adopted various pieces of legislation that allowed to intercept the communications of those who were suspected of being involved in anti-apartheid struggle. Finally, the chapter briefly introduced RICA. RICA defines what interceptions is. It in principle prohibits interception of communications of individual citizens and residents of South Africa. It then defines when one's communication can legitimately be intercepted. It provides for two types of interceptions, interception with and without interception direction. In the first category are interception by a party to a communication, interception by a state agent in case of emergency or for identifying one's location. Interception of communication with interception direction is often for investigating crimes. RICA provides detailed procedure for intercepting communication with interception direction.

### 5.2.2. Key findings

In chapter two it was argued that the right to privacy, including the right to communication privacy, can be restricted when certain conditions are fulfilled. These are legality, necessity, and proportionality. The right to communication privacy can be restricted only in accordance with law of general application. Whether or not a given law is if 'law of general application' is assessed in light

of its generality, precision, publicity and whether or not it allows a room for arbitrariness.

The restriction on the right to communication privacy in RICA was evaluated in light of the requirement of legality. The restrictions are put in RICA which is an act of parliament not some kind of executive decree or regulations. The fact that RICA is adopted by Parliament gives it an element of legality. RICA has generality in a sense it is applicable on everyone. RICA is not, therefore, a 'bills of attainder' which is directed towards 'specific named individuals or easily ascertainable members of a group for punishment'.

When it comes to precision, even though most of the operative terms of RICA are clearly defined, there are certain provisions, including those that define the criteria for authorising interception by a judge, are said to be which open the gate for arbitrariness. RICA is well publicised and available online and in print. Hence the requirement of publicity is fulfilled. In short in light of the four criteria above, RICA can be considered as law of general application despite the vagueness in some of the provisions in it. Hence the requirement of legality in terms of restricting one's right to communication privacy has been met.

One's communication privacy can be limited only if and when it is necessary for achieving some legitimate purpose. As per the South African government there are two reasons why it was necessary to adopt RICA. First, it was necessary to adopt RICA because South Africa has one of the highest crime rates in Africa, the prevention and investigation of which necessitated the interception of communication without which the crime rate is likely to worsen. Hence given the high crime rate in the country and the increasing sophistication of the criminals, interception of communication necessary crime preventing and investigating tool. The other reason was related to the global security context. RICA was adopted a year after the 9/11. South Africa also found adopting RICA necessary for combating international terrorism. The requirement of necessity is also fulfilled.



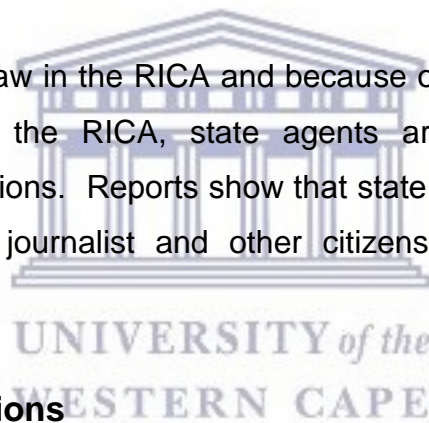
Proportionality is about ensuring that the limitation that is imposed on the right to privacy is 'reasonable and justifiable in an open and democratic society' based on human dignity, equality and freedom' which is assessed, among others, by taking into account 'the importance and purpose of the limitation', whether the limitation is linked to the purpose that is to be achieved, and the extent or degree of limitation that is allowed. The limitation should be the least intrusive limitation that can achieve the purpose. The proportionality of interception of communication is something that can only and need to be determined on case by case basis by taking into consideration what the interception is meant to achieve, how intrusive the interception is and the like. However, the indiscriminate retention of data is considered as unnecessary for preventing or investigating crimes and disproportionate to when seen in light to the right of privacy of the person the history of whose communication is stored. Moreover, the possibility of authorising the decryption of encrypted information is also viewed as disproportional.

Procedural safeguards are also critical for the enjoyment of the right to privacy in the context of the application of RICA. The limitation of one's right to privacy can be conducted under certain procedural safeguards that are meant to ensure that there is a legitimate cause that justify the interception and post-interception procedural safeguards that are intended to ensure that the interception was conducted for the intended purpose only and there is no overreach by state agents while conducting the interception. RICA provides that as rule interception of communication can be conducted only after interception direction has been secured. It also has post-interception procedural safeguards. When interception of communication is conducted without interception direction, the interception and the reason for it has be communicated to the designated judge.

RICA does not however require that a state agent inform the person whose communications are intercepted the fact that his/her communications were indeed intercepted. This is viewed by some as serious constitutional flaw

since it would not allow the person whose communication was intercepted to challenge the legality of interception. RICA is also silent 'about the procedure state officials should follow when examining, copying, sharing, storing, etc., the intercepted data'. In some cases, the data that is collected through interception might be of no value for the investigation. However, it is unclear whether the state agents are required to destroy or store such data. It does not also provide a 'certifiable procedure for the data to be destroyed'. Moreover, RICA does not provide a procedure in which the designated judge may follow up whether the interception was used only for the purpose for the achievement of which it was authorised. This is feared to allow state agents to use the interception direction for a purpose other than the one that it was intended for.

Partly because of the flaw in the RICA and because of complete disregard to what are provided in the RICA, state agents are illegally intercepting individual's communications. Reports show that state agents are intercepting the communication of journalist and other citizens and residents of the country.

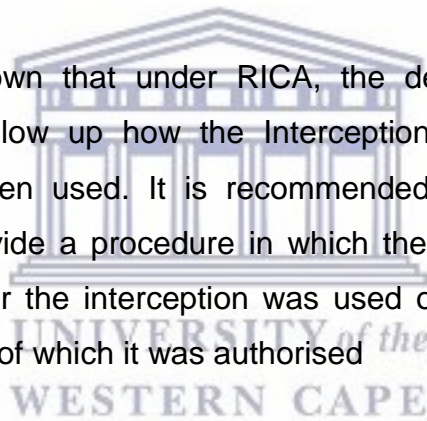


### **5.3. Recommendations**

Based on the above observations, it is possible to offer a number of recommendations, including on the need for training, awareness raising, capacity building, strengthening of the relevant institutional frameworks for oversight, as well as the role of civil society in contributing towards the upholding of the right to privacy in the application of RICA.

However, below, this paper provides brief recommendations that are considered to be a priority with a view to ensure the right to privacy in the application of RICA in South Africa. These recommendations are both specific, and urgent, with a view to ensure both the conceptualisation and application of RICA in order for it to comply with the South African Constitution and the relevant provisions of the ICCPR.

- It has been shown that the indiscriminate retention of data for five years, as provided under RICA, is considered as unnecessary for preventing or investigating crimes. It is also considered disproportionate when seen in light to the right of privacy of the person the history of whose communication is stored. It is therefore recommended that RICA should be amended to prohibit the bulk retention of information about the communication of everyone.
- There is no a requirement under RICA for state agents to destroy information they collected once the investigation is completed. It is recommended that RICA should require state agents to destroy such data and provide clear and 'certifiable procedure' for so doing.
- It has been shown that under RICA, the designated judge is not authorised to follow up how the Interception Direction that he/she provides has been used. It is recommended that RICA should be amended to provide a procedure in which the designated judge may follow up whether the interception was used only for the purpose for the achievement of which it was authorised
- It has been shown that state agents wilfully violate RICA and illegally intercept individuals' communications. Such violations should be investigated by the Independent Police Investigative Directorate and the perpetrators be brought to justice.



## Bibliography

### Books

Bawa N 'The regulation of the interception of communications and provision of communication related information act' in L Thornton, Y Carrim, P Mtshaulana and P Reyburn (eds) *Telecommunications law in South Africa* Johannesburg: STE Publishers 296-332

Cole D.D (2013) 'Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism' in Davis. D, McGarrity. N & Williams.G (eds) *Surveillance, counter-terrorism and comparative constitutionalism* New York: Routledge 95-116

Eric H (1995) *Sexual orientation a human right law* Leiden Leiden: *Martinus Nijhoff*

Jayawickrama N (2002) *The judicial application of human rights law, national, regional and international jurisprudence* Cambridge: Cambridge University Press

Klitou. D (2014) *Privacy-Invading Technologies and Privacy by Design: Safeguarding Privacy Liberty and Security in the 21<sup>st</sup> Century* Springer

McQuoid-Mason D. (1998) 'Privacy' in M Chaskalson (eds) *Constitutional law of South Africa* 2<sup>nd</sup> ed Kenwyn: Juta, loose leaf, 18-1-18-16

Woolman S and Botha H (2008) 'Limitations' in Woolman S, Roux T and Bishop M (eds) *Constitutional law of South Africa* Kenwyn: Juta, loose leaf, 12-1-12-64

### Articles

Amnesty International (2014) *Amnesty international withdraws support for the USA Freedom Act, urges stronger reforms* <

<https://www.amnestyusa.org/files/aiusafreedomactmay2014.pdf>> accessed on 20 May of 2016

Africa Check *Factsheet: South Africa's crime statistics for 2016/17* <<https://africacheck.org/factsheets/south-africas-crime-statistics-201617/>> accessed on 17 November 2017.

Botha C. (2017) *Cybercrimes and Cybersecurity Bill: Better but still bad* <<http://www.politicsweb.co.za/news-and-analysis/cybercrimes-and-cybersecurity-bill-better-but-stil>> accessed on 23 October 2017

Botha C (2017) *Cybercrimes and Cybersecurity Bill, Part 2 - Failing to address legislative shortcomings on the State's surveillance powers*. Available at <<http://www.cfcr.org.za/index.php/latest/751-article-the-cybercrimes-and-cybersecurity-bill>> accessed on 23 on October 2017

Canattaci JA. (2016) Report of the special Rapporteur on the right to privacy, A (HRC/31/64/)

Casman B S (2011) 'The Right to Privacy in Light of the Patriot Act and Social Contract Theory' (Unpublished thesis; University of Nevada, Las Vegas) <<http://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=2087&context=thesesdissertations>> accessed on 10 August 2017

Cohen (2001) 'But for the nicety of knocking and requesting a right of entry': Surveillance law and privacy rights in South Africa' 1(1) (2001) *The Southern African Journal of Information and Communication*

De Vos P (2011), RICA? <<https://constitutionallyspeaking.co.za/rica-is-it-unconstitutional/>> accessed on 23 June 2016

Duncan J (2016) *Reports of the death of communications privacy are greatly exaggerated: reflections on recent UN Human Rights Committee's findings on*

South Africa <<https://www.privacyinternational.org/node/850>> accessed on 15 October 2017

Deutsche Welle (2017) *Madrid to Manchester to Barcelona: A chronology of terror in Europe*. Available at <http://www.dw.com/en/madrid-to-manchester-to-barcelona-a-chronology-of-terror-in-europe/a-38949481> accessed on 20 September 2017

Dorraj, S.E. and Barcys M. (2014) 'Privacy in digital age: dead or alive?! Regarding the new EU data protection regulations' 4(2) *Social Technologies* 306–317; R. Wilton 'Identity and privacy in the digital age' x(Y, xxxx) *International Intellectual Property Management* 1-18,

Emerson E *Promotion and protection of human rights and fundamental freedoms while countering terrorism* (Report submitted to the United Nations General Assembly)  
<<https://assets.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf>> accessed on 10 April 2016

Entrikin, J. L. (2014) 'The right to be let alone: The Kansas right of privacy' 53 *Washburn Law Journal* 222

Geneva Academy International Humanitarian Law and Human Rights *The right to privacy in the digital age*

Glancy J (1979) 'The invention of the right to privacy' 21 (1) *Arizona Law Review* 1-39

Global Information Society Watch (2014) *Communications surveillance in the digital age* APC and Hivos

Hunter M *RICA in South Africa: How big is Big Brother?* <[https://www.groundup.org.za/article/rica-south-africa-how-big-big-brother\\_1882/](https://www.groundup.org.za/article/rica-south-africa-how-big-big-brother_1882/)> accessed on 27 October 2017

Human Rights Council Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/23/40) <[http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40\\_EN.pdf](http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf)> accessed on 23 April 2016

Human Right Watch (2014) 'They know everything we do' telecom and internet surveillance in Ethiopia. <<https://theintercept.com/2017/09/13/nsa-ethiopia-surveillance-human-rights>> accessed on 20 May 2017

Human Rights Watch (2012) *In the name of security counterterrorism laws worldwide since September 11* Human Rights Watch

Jacoby N (2007) 'Redefining the right to be let alone: Privacy rights and the constitutionality of technical surveillance measures in Germany and the United States' 35(3) *Georgia Journal of International and Comparative Law* 456

King N J 'Electronic monitoring to promote national security impacts workplace privacy' 15(3) *Employee Responsibilities and Rights Journal* 128-129.

Le Rue F The present report, submitted in accordance with Human Rights Council resolution 16/4, analyses the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression

Luck R (2014) *Walking a fine line between crime prevention and protection of rights*

Macaskill E (2013) *Edward Snowden, NSA files source: 'If they want to get you, in time they will'* <<https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why>> accessed on 16 March 2017

Mare A and Duncan J (2015) *An Analysis of the communications surveillance legislative framework in South Africa* Media Policy and Democracy Project

<[http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework\\_mare2.pdf](http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-framework_mare2.pdf) > accessed on 20 May 2016

Marks S P 'International law and the 'war on terrorism': Post 9/11 responses by the United States and Asia Pacific Countries' (2006) 14 (1) *Asia Pacific Law Review* 43-74

Mathew A S (1986) *freedom, state security and the rule of law: Dilemmas of the apartheid society* Johannesburg: Juta and Co Limited

Milanovic M 'Human rights treaties and foreign surveillance: Privacy in the digital age' 56(2015) *Harvard International Law Journal* 81-146.

Ministerial Review Commission on Intelligence *Final Report to the Minister for Intelligence Services, the Honourable Ronnie Kasrils, MP* (10 September 2008)

Nakashima E and Peterson A (2015) *The Obama administration opts not to force firms to decrypt data* <[https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699\\_story.html?utm\\_term=.0d4f17d4514e](https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html?utm_term=.0d4f17d4514e)> accessed on 22 October 2017

Nyst C and Falchetta T (2017) 'Practice note: The right to privacy in the digital age' 9 *Journal of Human Rights Practice* 104–118

Moor J H (1991) 'The ethics of privacy protection' 39(1) *Library Trends* 69-82

Office of the High Commissioner for Human Right *CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family,*



*Home and Correspondence, and Protection of Honor and Reputation* (Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988).

Padayachee C (2015) Employees right to privacy verses the employer's right to monitor electronic communication in the workplace (Unpublished Master's thesis, University of the KwaZulu Natal)

Patrick-Patel. L, (2014) 'The African Charter on Human and Peoples' Rights: how effective is this legal instrument in shaping a continental human rights culture in Africa?' *Le Petit Juriste* 21 December 2014 <https://www.lepetitjuriste.fr/droit-compare/the-african-charter-on-human-and-peoples-rights-how-effective-is-this-legal-instrument-in-shaping-a-continental-human-rights-culture-in-africa/> last accessed on 10 March 2018.

Pearson M and Busst N (2006) 'Anti-terror laws and the media after 9/11: Three models in Australia, NZ and the Pacific' 12(2) *Pacific Journalism Review* 9-27

Pierre de Vos (2011), RICA: Is it unconstitutional? Available at <https://constitutionallyspeaking.co.za/rica-is-it-unconstitutional/> accessed on 23 Jun 2016

Prieto D B (2009) *War about terror: Civil liberties and national security after 9/11* (New York; Council on Foreign Relations)

Privacy International, Association to Progressive Communication (APC) & Right to Know Campagna Submission (2016) *In advance of the consideration of the periodic report of South Africa Human Rights Committee, 116th Session.*

Rautenbach I M (2014) 'Proportionality and the limitation clauses of the South African bill of rights' 17(6) *Potchefstroom Electronic Law Journal* 2229-2267

Right to Know Campaign (2016) *Submission in advance of the consideration of the periodic report of South Africa Human Rights Committee 116th Session*

Right2Know Campaign *Preliminary Position on the draft Cybercrimes and Cybersecurity Bill* (30 November 2015)

Right2Know Campaign (2017) *Case studies how communication has been abused in SA* < <http://www.r2k.org.za/2017/04/20/case-studies-communications-surveillance-abuse/>> accessed on 15 October 2017

Right2Know Campaign (2015) *Does the government have 'grabber technology'? We demand to know* < <http://www.r2k.org.za/2015/09/03/surveillance-device/>> accessed on 28 October 2017

Saba A(2017) *Cop illegally bugged Sunday Times calls* <<https://www.timeslive.co.za/sunday-times/news/2017-07-29-cop-illegally-bugged-sunday-times-calls/>> accessed on 26 October 2017

Submitted by Privacy International and TEDIC (2015) *The right to privacy in Paraguay* Universal Periodic Review Stakeholder Report: 24th Session, Paraguay.

Swart H 'Say nothing – the spooks are listening' Mail & Guardian, 18 December 2015 < <http://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening>> accessed on 18 October 2016

Swart H. (2016) *Communication surveillance by the South African intelligence service* (A report commissioned Media Policy and Democracy Project, a joint project of the Department of Journalism, Film and Television at the University of Johannesburg and the Department of Communication Science at UNISA) < [http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart\\_feb2016.pdf](http://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/comms-surveillance-nia-swart_feb2016.pdf)> accessed on 15 of November 2016

Swart H *Secret state: How the government spies on you Mail & Guardian* < <https://mg.co.za/article/2011-10-14-secret-state/>> accessed on 10 October 2017

Steiner H, Alston P, and Goodman R, (2008) *International human rights in context: law, politics, morals* Oxford: Oxford University Press

Taylor K (2002) 'State surveillance and the right to privacy' 1(1) *Surveillance & Society* 68

Truth and Reconciliation Commission of South Africa Report Vol 3. < <http://www.justice.gov.za/trc/report/finalreport/Volume%203.pdf>> 20 Mar 2017

Tuval Y 'Anti-terrorism legislation in Britain and the U.S. after 9/11' (The Israel Democracy Institute) < <https://en.idi.org.il/articles/6936>> 20 Aug 2017

United Nations High Commissioner for Human Rights (2014) *The right to privacy in the digital age; Report of the Office of the United Nations High Commissioner for Human Rights*

United Nations High Commissioner for Human Rights *The right to privacy in the digital age; Report of the Office of the United Nations High Commissioner for Human Rights*

United Nation (2016) Human Rights Committee concluding observations on the initial report of South Africa

United Nation Human Rights Council (2017) Report of the Special Rapporteur on the right to privacy

United Nation General Assembly Res ([68/167],2013) The Right to Privacy in digital age

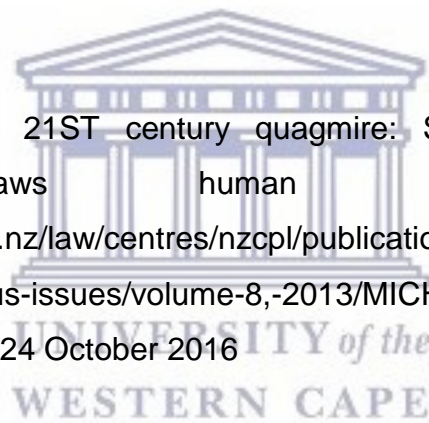
United Nation Human Rights Council (2017) Report of the Special Rapporteur on the right to privacy

Van der Bank C M (2012) 'The right to privacy – South African and comparative perspectives' 1(6) *European Journal of Business and Social Sciences* 77-86

Vincent S (2014) *International law and secret surveillance: Binding restrictions upon state monitoring of telephone and internet activity* Centre for Democracy and Technology: United Nations High Commissioner for Human Rights

Warren S.D and L D. Brandeis L.D (1890) 'The Right to Privacy' 4(5) *Harvard Law Review* 193-220.

White C (undated) A 21ST century quagmire: Surveillance laws and international laws human rights norms  
<<https://www.victoria.ac.nz/law/centres/nzcpl/publications/human-rights-research-journal/previous-issues/volume-8,-2013/MICHAEL-WHITE-HRR-2013.pdf>> accessed on 24 October 2016



### **Legislation**

The Constitution of the Republic of South Africa (1996)

Interception and Monitoring Prohibition Act 127 of (1992)

Post Office Act No. 44 of 1958

Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of (2002)

USA Patriot Act (H.R 3162) < <https://epic.org/privacy/terrorism/hr3162.html>> accessed on 10 August 2017

## **Treaties**

American Convention on Human Rights, "Pact of San Jose ", Costa Rica, 22 November 1969

European Convention for Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos 11 and 14 November 1950

International Covenant on Civil and Political Rights. Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976,

The Convention on the Rights of the Child Adopted and opened for signature, ratification and accession by the General Assembly resolution 44/25 November 1989 entry into force 2 September 1990

The Convention on the Protection of the Right of All Migrant Workers and Members of Their Families (ICRMW). Adopted by General Assembly resolution 45/158 of 18 December 1990 entry into force 2003)

Universal Declaration of Human Rights (UDHR) 1948

## **Case law**

*Bernstein and Others v Bester NO and Others* (CCT23/95) [1996] ZACC 2; 1996 (4) BCLR 449; 1996 (2) SA 751 (27 March 1996)

*De Lille & another v Speaker of the National Assembly*, 1998 (3) SA 430 (C), 1998 (7) BCLR 916 (C).

*Klass and Others v. Germany*, no. 5029/71, 6 September 1978

*Klein v Attorney-General, WLD, & another* 1995 (3) SA 848 (W) at 865

*Malone v United Kingdom* 1984] ECHR 10]

*National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others* (CCT11/98) [1998] ZACC 15; 1999 (1) SA 6; 1998 (12) BCLR 1517 (9 October 1998).

*S v Kidson* 1999 (1) SACR 338 (W)

*Roe v. Wade*, 410 U.S. 113 (1973)

*Rojas Garcia v. Colombia*, Communication No.687/1996, U.N. Doc. CCPR/C/71/D/687/1996 (2001).

*Roman Zakharov vs Russia* no.47143/06.

*Tristán Donoso v. Panamá, H.R.* (ser. C) No. 193, 56 (2009)

*Van Hulst v The Netherlands, HUMAN RIGHTS COMM.*, Communication No. 903/1999, 7, U.N. Doc. CCPR/C/82/D/903/1999 (2004).

