LAW ENFORCEMENT OFFICIALS' PERCEPTIONS OF RICA AS A LEGISLATIVE TOOL TO COMBAT CRIME

by

Subryne Govender

A research report submitted to the Faculty of Management, University of Witwatersrand, in 25% fulfilment of the requirements for the degree of Master of Management (in the field of Security) - MM-S

Supervisor: Prof. Anthoni Van Nieuwkerk

May 2019.

Abstract

Regulation of the Interception of Communications and Provision of Communication-Related Information Act (RICA) was enacted in 2002 to regulate the monitoring and interception of communications and to assist law enforcement officers in gathering evidence. This exploratory study aimed to gain an understanding of the perceptions of law enforcement officials towards RICA as a crime combatting tool. One of the main findings of this study was that the implementation and compliance to RICA was the central concerns raised by law enforcement officials. The study found that non-compliance to RICA resulted in outdated and inaccurate information being kept and supplied to law enforcement from Telecommunication Service Providers (TSPs). The findings of the study also uncovered that unregistered SIM cards (especially pre-paid) SIM cards also provided law enforcement officials with methods of communications without being detected especially during intelligence gathering operations.

In terms of compliance shortcomings of RICA the following are recommended to make RICA more effective to law enforcement:

- There needs to be a concerted, joint effort between affected South African government departments to make sure compliance to RICA is compulsory and occurs correctly and
- Concurrently South African TSPs should be obliged to not allow local or foreign SIM cards to access their networks which have not been correctly registered as per RICA.

In terms of the RICA application process itself the following are suggested:

- More approvers of RICA applications need to be made available, either more retired judges need to be appointed or a panel of judges.
- The RICA process for law enforcement officials need to standardized, where the automation of the process up to the approval judge would decrease turnaround times vastly.

Declaration

I declare that this report is my own, unaided work. It is submitted in partial fulfilment of the requirements of the degree of Master of Management (in the field of Security) in the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in any other university.

_____

Subryne Govender

May 2019

Dedication

I dedicate this to my wife, Marcini and my boys Shreeyan and Shivayan thank you for the unconditional support during my studies. You'll remain my inspiration.

To my Mum and Dad thank you for believing in me through all my failures.

Acknowledgments

I will always remain grateful to my supervisor, Prof. Anthoni Van Nieuwkerk. Prof. thank you for always being available to provide assistance to me on occasion at such irregular hours and for responding to all the "*silly*" little questions that I have asked over the past two years. You have helped get me over the finish line. Thank you.

A big thank you to the State Security Agency for allowing me to conduct this study within its environment, using its employees.

A huge thank you to Ms. Giovanna Guerra for all the help with the editorial done to the document.

CONTENTS

LIST OF ABBREVIATIONS

AISP	Association of Information System Programs
ANC	African National Congress
CI	Crime Intelligence
DC	Department of Communications
DPP	Director of Public Prosecutions
Email	Electronic Mail
ICASA	Independent Communications Authority of South Africa
IG	Inspector General
IMP	Interception and Monitoring Prohibition Act 127 of 1992
ISS	Institute for Security Studies
ITU	International Telecommunication Union
JSCI	Joint Standing Committee on Intelligence
NCC	National Communications Centre
NGO	Non-Government Organization
NP	National Party
NPA	National Prosecution Agency
OIC	Office of the Interception Centre
OIGI	Office of the Inspector General for Intelligence
RIA	Research ICT Africa
RICA	Regulation of the Interception of Communications and Provision of Communication-Related Information Act , 2002
RIPA	Regulation of Investigating Powers Act of 2000
RSA	Republic of South Africa
SALC	South African Law Reform Commission
SAPS	South African Police Service
SIM	Subscriber Identification Module

SMS	Short Message Service
SSA	State Security Agency
UCC	Ugandan Communications Commission
UK	United Kingdom
UN	United Nations
US	United States of America
WW	World War

Chapter 1

General Introduction

1.1 Introduction

Advances in global politics, economics and technology have altered sophisticated crime patterns around the world. This has given criminals the opportunity to take advantage of the advancements in technology to communicate more effectively in order to perpetrate their crimes and to remain undetected. In 2002 South Africa enacted the Regulation of the Interception of Communications and Provision of Communication-Related Information Act (RICA), in order to regulate the monitoring and interception of communications and to assist law enforcement officers in gathering evidence during investigations. Although the introduction of RICA raised expectations amongst South African law enforcement authorities in relation to being able to combat the increased criminal use of advanced technology to communicate, the advent of RICA also created a platform for abuse by South African intelligence gathering agencies for political purposes and in the case highlighted by Duncan (2017), to “hassle” journalists in regard to their investigations. This study will explore the extent to which RICA has been useful to law enforcement officials in order to combat crime in South Africa.

Generally the term Law enforcement would be making reference to typically the Police. This study uses a broader definition of law enforcement as alluded to by Schmalleger (1996). Schmalleger described law enforcement as “any system by which some members of society act in an organized manner to enforce the law by discovering, deterring, rehabilitating, or punishing people who violate or intend to violate the rules and norms governing that society”. Intelligence services in South Africa are mandated to play a pivotal role in the “discovering” (as alluded to by Schmalleger) the drivers of crime. Hence in this context members of the SSA were viewed as part of broader law enforcement and were interviewed in this study.

1.2 Problem Statement

Since its inception in 2002, RICA and its application has received negative attention from the media and the general public (Duncan, 2017; Hunter, 2014; Smillie & Hosken, 2015 and Swart, 2016). Academically there have been no definitive conclusions drawn as to whether RICA is doing what it was promulgated to do.

As alluded to by Hutton (2007) and Nathan (2009), academic studies conducted on RICA have tended to focus primarily on two broad topics; first, how RICA can be exploited (by law enforcement officials) for personal or political gain and second, how RICA infringes on the rights of South Africans to privacy as upheld by the Constitution. Currently, no statistics are available on the number of authorised interceptions in terms of RICA that has led to arrests or convictions. This, together with the lack of academic assessments on the uses of RICA in law enforcement investigations, makes it difficult to gauge the effectiveness of RICA in its ultimate aim of preventing crime and maintaining national security.

This study will explore the perceptions of law enforcement officials from the State Security Agency (SSA) who uses RICA as part of their investigative tradecraft. The SSA is mandated with utilising predominantly proactive intelligence driven operations, which provides the researcher the ideal context and opportunity to center this study on how effectively RICA is used in preventing crime before it occurs.

This study will attempt to provide an academic account on the effectiveness of RICA through the perceptions and experiences of these SSA members.

1.3 Purpose Statement

The purpose of this study is to gain an understanding of the perceptions of law enforcement officials towards RICA as a crime combatting tool.

1.4 Research Questions

The research question that guided this research is:
What are law enforcement officials' perceptions towards RICA as a legislative tool to combat criminal activity in South Africa?

1.5 Impact of the Research

Conducting this study will help in identifying benefits or limitations of RICA and could pinpoint areas of the legislation that need to be improved in order to assist law enforcement officials in their crime prevention activities. The findings of this study will also identify best practices or the contrary in relation to applying RICA successfully in profiling offenders and leading to eventual successful prosecutions (since the focus of this study is on law enforcement officials and their perception of RICA). These practices identified could be incorporated into specific SSA training initiates aimed at profilers/analysts and investigators so they can be trained on how they can effectively use RICA in investigations.

1.6 Conclusion

In this initial chapter the study was presented and explained. The problem statement as well as the purpose of this study was presented. The research question was specified as well as the impact of this study. The following chapter will provide the literature review which will be followed by the chapter on the research methodology used, followed by the report in chapter three. The fourth chapter will present the results concluding with chapter five which will present the overall analysis of the research and subsequent recommendations.

Chapter 2

Literature Review

2.1 Introduction

Since the advent of democracy in South Africa, legislation and numerous policies have been implemented by the government in the criminal justice sector with a view to help combat crime and develop criminal justice functioning (Du Plessis & Louw, 2005). Pistorius (2009) and Thornton (2006) identified the Regulation of Interception of Communications and Provision of Communications – Related Information Act of 2002 (RICA) as being one of the new pieces of legislation promulgated to assist law enforcement in combatting crime.

This chapter presents a review of academic literature on telecommunication interception law, which will serve as a basis for the research study to evaluate the effectiveness of RICA in law enforcement investigations. The review begins with a broad look at telecommunication, its evolution over time, telecommunication law and its definition in a South African and international context. Interception of communication legislation (domestic and international) is also examined, along with the role it plays in crime prevention. International literature was sourced to provide a global context on telecommunication law and its application, paying particular attention to laws that were introduced to intercept communications, i.e. international legislation similar to RICA. The review then narrows its focus to RICA and emerging issues and limitations that include human rights and policy regulation issues.

This review should not be viewed as being comprehensive in terms of telecommunication law, as vast amounts of literature are available on international interception legislation; however, very limited academic literature was found on RICA specifically. Consequently, grey source literature emanating from experts in the field and other professional bodies has been selected for inclusion based on the literature

having been through a process of peer review. Grey source literature used in this literature review include working papers, research reports, conference proceedings, white papers and reports/articles produced by government departments, academics, business and industry which were not published by commercial publishers. The literature emanating from the Institute for Security Studies (ISS) is a case in point. The overall aim of this review is to provide an insight (international and local) into the major themes associated with telecommunication legislation that involve interception of communications laws.

This literature review looks at telecommunication law, telecommunication regulation, interception of communication laws, RICA itself and law enforcement policies relating to communication interception with emphasis on Africa and more specifically South Africa where applicable and if at all possible.

2.2 Defining Telecommunications

Before the introduction of telecommunications, communication between individuals was restricted by “distance” and the “speed” with which the message could be shared. The evolution of telecommunications has shown how swiftly things have progressed since the advent of the telegraph in 1835 (Brierley in Thornton, 2006).

In 1997 the Association of Information Systems Professionals (AISP) at the University of Wisconsin defined telecommunication as the process of electronic transfer of information from one place to another. For many commentators this definition was too simplistic and lacked any reference to how the transfer would occur hence, this definition was further expanded to include examples of instruments such as telephone systems, mobile phones and facsimile transmissions (O’Neil & Everett in Chien, 2007). Since then there have been numerous definitions of telecommunication however, the most popularly quoted academic definition described telecommunication as, “*The art and science of communicating over a*

distance by telephone, telegraph and radio. The transmission, reception, and the switching of signals such as electrical or optical, by wire, fibre or electromagnetic–through the air" (Newton, 2002:733). Thornton (2006:17) further emphasised the two telecommunication concepts derived from Newton's definition, i.e. the "act" and "means**"** of communicating, where act refers to the words (sending or receiving information) and the means to the infrastructure used to communicate.

Other academics attempted to define telecommunications from its etymology. Balbi (2009) explained that "tele" referred to distance, as in telephone and telegraph, and "communication" to the different methods of communicating such as internet, mobile phone and radio further emphasising the point of the "Act" and the "means" as introduced by Thornton (2006).

The Telecommunications Act of 1996 defines telecommunications as "the emission, transmission or reception of a signal from one point to another by means of electricity, magnetism, radio, other electromagnetic waves or any agency of a like nature whether with or without the aid of tangible conductors". This definition was criticised by academics for being too narrow and not being equipped to keep up to date with the ever-changing technological advancements Snail (2009). The need for regulation is not apparent in these definitions apart from the potential risk posed by the words, i.e. the "act" of communication as mentioned above.

2.3 Why regulate Telecommunications?

The International Telecommunication Union (ITU), an agency of the United Nations (UN), continues to coordinate the regulation of telecommunications internationally; whilst in South Africa the Telecommunications Act of 1996 and the Independent Communications Authority of South Africa (ICASA) regulate telecommunications in South Africa. The Telecommunications Act provides for the regulation and control of telecommunication matters in the public interest by setting out rules for the

telecommunication industry in South Africa and establishing a regulatory mechanism that must institute other rules and regulations for the telecommunications industry (Telecommunications Act of 1996: Law & Legislative History, 2001). Thornton (2006) perceived telecommunication as being borderless in nature and not being restricted to any national or international space. This vision of telecommunications partially explains why regulation of telecommunication in South Africa, like in any other country, is required using international law through the ITU owing to signal propagation transcending different countries. According to Begum, Murad & Hoque (2016) the mandate of the ITU also includes the regulation of telecommunication equipment in member countries and ensures for compatibility to allow for cross-border communication, which in turn would enable easier telecommunication interception in member states. This could be referenced back to Thornton's definition, where the "means" described also would relate to equipment and an institutional body that would ensure compatibility.

Thornton (2006:18), writing from a policy evaluation perspective, identified three reasons why telecommunications need to be well regulated:

- Telecommunications is seen as a **public utility** with governments considering it in their mandates to share these utilities equally among citizens. The White Paper on Telecommunications in 1996 emphasised how important the development of communication was in South Africa.
- Thornton perceived governments to treat national telecommunication as their "**natural monopoly**", doing all they could to protect it by not allowing rivals to be licenced.
- It is critical to regulate telecoms to **protect the radio frequency spectrum** in countries. Without strict control over the spectrum, chaos could ensue with the dominant individuals having total control of it. Radio frequency spectrums are considered one of the state's important scarce resources that is being utilised in the daily activities of its citizens. These activities include radio broadcast and television services, mobile cellular phone services, public safety services, disaster relief activities etc. ("NTRA", 2017). The Minister of Communications

provides direction to the band plan which sets out the uses to which the various frequency bands can be used for. The Minister is tasked with ensuring that the frequency spectrum is strictly controlled to avoid a monopoly being able to control radio frequency spectrums (Drake, 1990).

2.4 Interception and Monitoring of Telecommunication

Rapid changes in global economic, political and technological arenas have transformed sophisticated crime patterns around the world. This has given criminals the opportunity to take advantage of the advancements in technology to help them perpetrate their crimes more efficiently and to avoid detection (Gürkaynak, Yilmaz & Taskiran, 2014).

Advancements in telecommunications in the last decade have seen numerous countries improve their telecommunication interception and monitoring laws (Akdeniz, Taylor & Walker, 2000). Following the 11 September 2001 terror attacks, many countries started to use or improve telecommunication interceptions to protect themselves against terrorist and other related activities (Bloss, 2007).

The concept of interception originated from the European Council Resolution of 1995 that defined the global requirements for the lawful interception of telecommunications (European Council Resolution, 1995). The development of international interception and telecommunication law was largely due to the work done by governments in Europe in conjunction with the United States, New Zealand Australia and Canadian governments (Chien, 2007).

Benkler in Kisswani (2010) describes interception as an authorised process whereby network service providers/network operators provide law enforcement access to communications, in the form of telephone calls, emails, etc. Many academics were critical of Benkler as they assessed that interceptions were being conducted with or

without consent in their respective countries (Hemeson, 2012). Akdeniz, Taylor & Walker (2000) alluded to a swift growth in crimes using sophisticated technology for which lawful interception of telecommunication could play an integral part in helping law enforcement combat these crimes but they cautioned that a distinction needed to be drawn between legitimate and illegitimate interception.

Cohen (2001) alleged that the development of interception and monitoring laws in South Africa originated from the previous National Party (NP)-led government's fascination with security legislation. Cohen (2001), Hemeson (2012) and Taylor (2002) argued that improvements in technology also made it easier for illegal interception and monitoring of telecommunications by the state and private individuals. The Interception and Monitoring Prohibition Act of 1992 was implemented to help negate the risk, as emphasised by Cohen and Hemeson (Interception and Monitoring Prohibition Act of 1992).

2.5 Need for Intercepting and Monitoring Telecommunication

Some academics writing on the interception and monitoring of communication describe the purpose of (legally) intercepting and monitoring telecommunications as: the need to collect information in the interests of national security and law enforcement these academics include Hutton (2007); Kisswani (2011) and Taylor (2002).

2.5.1 National Security

According to Kisswani (2011), the definition of national security has broadened significantly over time. Inkster (2010) supports this view and alludes to the fact that national security has always been seen as the protection of the state and its crucial interests however, the dependence of global economies on each other and the escalating complexity of criminal activity require a broader view and definition of

what national security is. An example of this would be the United States' (US) 2006 National Security Strategy that included the issue of diffusing regional conflicts as being a matter of national security (United States National Security Strategy, 2006). While many could not understand how a conflict in a region far away from US soil could have a critical effect on national security, Inkster (2010) highlighted that instability in any region of the world would have global implications owing to the interconnected nature (technological and socioeconomic) of the world we live in.

Telecommunication interception has been used to maintain national security since the advent of World War (WW) II. The collaboration between the US and the United Kingdom (UK) during WWII formed the early foundation for national security interception practices that are still being employed by many countries currently (Kisswani, 2011). Watney (2015) maintains that the need for interception by state organs is critical to the uncovering of threats to national security that may include terrorism or sabotage. With this argument in mind, it should also be noted that the concept of national security is a varied subject for various academics – ranging from preventing terrorist activity, controlling of borders, detecting fraud to even protection of a state against disease (Hemeson, 2012; Hutton, 2007; Taylor, 2002). In South Africa, national security is defined in the General Intelligence Law Amendment Act of 2013 to include the protection of the people and the territorial integrity of South Africa (General Intelligence Laws Amendment Act, 2013).

2.5.2 Law Enforcement

With the advancement of telecommunications tools and telecommunications-related crimes, law enforcement officials have sought to empower themselves with effective protocols to investigate crime and preserve national security (Kisswani, 2011). Kisswani argued that the interception and monitoring of telecommunications should place equal importance on privacy matters, counterterrorism operations, national security, criminal investigation and growth of economies.

After the terror attacks of 11 September 2001 in the US, many countries took initiatives to assist law enforcement to obtain information that could help prevent criminal or terror-related activities (Bloss, 2007). Bloss further argued that since terrorists and criminals know they are being monitored, they look to use advanced communication technology themselves to avoid detection.

National security and law enforcement issues are catered for differently in the provisions of interception and monitoring legislation internationally (Kisswani, 2010). Interception and monitoring warrants are easier to obtain in cases where there is sufficient evidence provided that the interception would help prevent serious criminal offences or threats to the security of the state (Tripp, 2001).

2.6 Subscriber Identification Module (SIM) Card Registration in Africa

Africa is considered as the fastest developing telecommunications market in the world however, concerns over the use of mobile telecommunications for illegal purposes have led to many African countries introducing SIM card registration policies (Hemeson, 2012). Hemeson highlights the fact that mobile communication has been used in ransom demands and to perpetrate serious criminal activities on the African continent. This obliged many governments in Africa, in association with their telecommunication operators, to implement SIM card registration to safeguard the use of their networks (Hemeson, 2012). In October 2014, South African mobile phone company MTN was fined $3.9 billion for not disconnecting unregistered SIM cards from their network. The Nigerian President alleged that not disconnecting unregistered SIM cards had fuelled Boko Haram insurgency in North East Nigeria ("Nigeria's Buhari says MTN fuelled Boko Haram insurgency - BBC News", 2016).

In the Ugandan milieu Dr Alison Gillwald (Executive Director of Research ICT Africa)- believes that the Uganda Communications Commission’s (UCC) move to force individuals to register SIM cards in Uganda is misguided. Dr Gillwald indicated

that, "*despite little evidence that mandatory SIM registration contributes to safeguarding our digital security and physical safety it has become a universal regulatory standard in Africa to facilitate the monitoring and interception of communications. With little to no public debate about the wider social or political effects and in the face of evidence of the negative effects on connectivity*." (Gillwald, 2017). Pater (2006) agrees with Dr Gillwald's uncertainty on the usefulness of SIM card registration. Pater is of the opinion that the only motive mobile operators will implement SIM registrations are because of an obligatory regulatory requisite, not for the intended purposes such as reducing crime, etc. (as is the case in South Africa).

2.7 Regulation of the Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 (RICA)

Grey source information was vital to this section on RICA. At the time of writing, limited academic works on RICA have been concluded in South Africa. Public policy assessment relies on many different resources including scholarly/academic work and also grey literature, which normally makes up the majority of references (Pappas & Williams, 2011). Briefs and other sources produced by governments, non-governmental organisations (NGOs) and think tanks are critical in forming an evidentiary base especially in assessing public policy. This holds true especial in this type of study where limited academic work has been done on RICA specifically.

2.7.1 Need for RICA

In 1999 the South African Law Reform Commission (SALC) found the predecessor to RICA, the Interception and Monitoring (IMP) Act 127 of 1992, to be inadequate to deal with the increased criminal use of advanced technology to communicate in South Africa. The SALC recommended that advancements in South Africa's telecommunication interception legislation were required to **enable law enforcement agencies to combat crimes that used telecommunications as well as other associated crimes including money laundering** (South African Law

Commission Report, 1999:26). Bawa in Thornton (2006:297) claimed that the SALC decision to review the IMP Act was due to the Acts inability to effectively combat crimes that used sophisticated technology that included computer/satellite/cellular communications through electronic mail (email) and other delivery mechanisms.

South African Law Commission's Recommendations

- The term "*communication*" should be broadened to include other types of developing conversation methods. (These included email and fax communication at the time. Of which fax communications have become outdated and not so widely used at present).
- Further offences should be added to what is defined in the IMP act as "*serious offences*".
- Communication between lawyers and clients should only be monitored or intercepted when there are reasonable grounds (and approval of a judge) that the lawyer or client is involved in serious violations or violations that threaten the security of the State.
- Law enforcement agencies should develop and possibly share central monitoring centres for the authorised monitoring communications.
- Telecommunication service providers should keep accurate records of customers (both contract and pre-paid) in relation to their identities and place of residence. This information should be provided to law enforcement agencies upon authorised (by a judge) requests.
- Use of intercepted information in court proceedings should be subject to the decision of the **Director of Public Prosecutions (DPP**) or an equal relevant authority.

2.7.2 Origins of RICA

RICA was conceptualised along the lines of similar legislation in Australia, France, Holland, Belgium, Germany, United Kingdom (UK), the United States (US), Hong

Kong, Australia and Canada (Thorton, 2006). The UK, Australia and the US legislations were important due to these countries concluding processes of reviewing and improving their interception and monitoring laws in relation to the ease with which cellular phones SIM card were purchased and used in criminal activities (Mirugi-Mukundi, 2010).

Summary of International Laws that Guided Development of RICA

Australia. The Telecommunications Interception Legislation Amendment Act of 2002 (TI Act) allows law enforcement to attain telecommunication interception warrants when information cannot be attained through other less infringing means. The TI Act gives law enforcement extensive powers to capture telephonic, computer and postal communications and more importantly the authority to question and detain suspects (Telecommunications Interception Legislation Amendment Act, 2002).

United States. The US Patriot Act significantly widened surveillance powers to include terror-related crimes, use of weapons of mass destruction, use of chemical weapons, terror financing and killing Americans outside the US (Patriot Act, 2001).

United Kingdom. The Regulation of Investigatory Powers Act of 2000 (RIPA Act) regulates the majority of interception and surveillance of communication in the UK. RIPA provides less latitude for law enforcement officers when compared to the laws of the US. RIPA was created to update legislation on interception of communication in line with technological advancements and human rights grievances (Regulation of Investigatory Powers Act, 2000).

2.7.3 Purpose of RICA

Michalson (2009), Pistorius (2009) and Thornton (2006) summarised RICA as a law **aimed at regulating the interception and monitoring of communications and the surveillance of *direct* and *indirect* communications by law-enforcement officers and other agencies for the purpose of gathering evidence during the investigation of crime.** Luck (2015) classified communications as, but not limited to, mobile phone communication, electronic mail (e-mail), text, data and visual mail communications or a combination. Ncube (2006), defined communication more broadly to include:

- Conversations between individuals with or without employing technology;
- Fixed line or portable phone conversations;
- Electronic mail (e-mail);
- Postcards, books, parcels and letters;
- Text messages (SMSs) or instant messages;
- Message services or answering machines;
- Pod casts or streaming
- Video, text or audio downloads or uploads
- Communications in prison;
- Communication on blogs, search engines chat rooms or on the worldwide web; and
- Two way radio communication.

The following provisions / chapters of RICA highlight more of the broader aims of RICA especially in relation to *law enforcement* and *crime prevention* activities:

Chapter 2 of RICA

Chapter 2 of RICA allows law enforcement to intercept and monitor communications only when authorised by a specified designated judge. The authorisation is granted

by the judge based on reasonable grounds that an offence has or will be committed (Mawson, 2015; Swart, 2011; Watney, 2015). However, Duncan (2014), Luck (2015), Mukadam & Meyer (2012), De Vos (2011) have highlighted concern when interceptions are conducted with an agenda other than what is provided for in RICA.

Chapter 3 of RICA

The office of the Interception Centre (OIC) and the National Communications Centre (NCC) were established in terms of Chapter 3 of RICA (RICA, 2002). According to Chapter 3, the OIC serves the interception and monitoring needs of the National Prosecuting Agency (NPA) and other South African intelligence agencies, while the NCC conducts bulk monitoring and interception of foreign signals that emanate or terminate in South Africa. Swart (2011) argued that the large number of interceptions conducted by the OIC and NCC makes oversight very challenging and almost impossible; hence, making it difficult to identify illegal interceptions.

Watney (2015) contended that the functioning of the NCC is undisclosed; hence, it is not possible to establish how interception is conducted on diplomats and ordinary citizens and if it is indeed judge-sanctioned interceptions. Watney further disputed that since the NCC intercepts **foreign** bulk communication, it does not fall within the realm of RICA. Nathan (2009) agreed with Watney's argument and claims that if the NCC is not within the realm of RICA then it is operating unconstitutionally.

Chapter 7 of RICA

RICA gained media popularity when section 40 of chapter 7 of RICA came into effect on 01 July 2009. It required prepaid mobile users to register their devices' SIM cards or face termination from the network (Mukadam & Meyer, 2012). Mirugi-Mukundi (2010) justified the implementation of these sections of RICA by insisting that registering an identity for prepaid SIM cards and tracking their usage would help authorities to deal with criminal activity and would assist in reducing crime. Duncan (2014) and Von Solms in Watney (2015) disagreed and viewed RICA and similar

laws in other countries as ineffective as criminals could steal identities to get their SIMs registered; hence, increasing the risks of identity theft. Mirugi-Mukundi (2010) and Hemeson (2012) agreed highlighting one of their key concerns is subscribers' information falling into criminal hands for use in perpetrating other crimes as well. Former Deputy Minister of Communications, Obed Bapela, gave assurances that the public's information would be protected as it was still kept securely by the service providers and would be divulged only with authorisation of a judge ("Traders warned against breaking RICA laws SA News", 2011).

2.8 Limitations of RICA

2.8.1 Human Rights Violations

Hutton (2007), Kisswani (2011) and Nathan (2009), agree that almost all democracies find it a challenge balancing human rights and freedoms with providing security and countering threats to a state. Mobbs in Hutton (2007) emphasised that the most crucial development since the rise of democracy is the change of state's focus from monitoring external threats to the monitoring of its own citizens. Watney (2015) argued that since surveillance imposes on citizens' rights, transparency is critical to ensure trust in law enforcement and ultimately government's surveillance practices.

Right to Privacy

Bazan in Kisswani (2011) explains that although the interception and monitoring of communication were efficient tools for protecting the security of states and its people, this type of investigative trade craft by design lends itself to intruding into the privacy of the intended target and associates with whom the target communicates.

Nathan (2009) reiterated that the South African Constitution requires law enforcement officials to conduct themselves in accordance with the Constitution and

that enforcement of laws relating to national security should be completed within the boundaries of the Constitution and relevant laws. Section 14 of the Constitution guarantees citizens the right to privacy that includes not having their home or person searched, belongings seized or their communications intercepted (South African Constitution, 1996). For Bawa in Thornton (2006:304), Blunn (2005) and De Vos (2011) RICA limits this constitutional right. De Vos argued that an **independent** monitoring body was required to ensure that RICA had not transgressed human rights. Blunn (2005) claims that balancing the right to privacy with crime prevention and national security has and will always be debated in interception law debates as long as there is no independent oversight mechanism that is *truly* independent of government.

Although RICA was implemented to equip law enforcement officers to combat crimes that involve sophisticated technology, it also regulates most aspects pertaining to the interception and monitoring of telecommunications – both in the work environment and in the public space (Bawa in Thornton, 2006). Bawa argued that by allowing such interception and monitoring, RICA does not provide adequate safeguards to citizen's constitutional right to privacy.

Duncan (2014) explained that RICA's flaw was that no one was alerted to the fact that their communications had been intercepted or monitored, even after the investigation had been completed. A 2015 Privacy International report highlighted the point made by Duncan in relation to the lack of transparency in RICA, noting how section 42 of RICA prohibits the disclosure of any intercept-related information (Privacy International, 2015). Duncan further argued that section 42 of RICA compared unfavourably to US interception legislation that required that the person whose communication was being intercepted be made aware within 90 days of the termination of the investigation – this to Duncan and Bawa in Thornton (2006:304) could be a viable recommendation to improve the transparency of RICA and act as a further oversight mechanism of law enforcement agencies. Individuals whose communications have been intercepted according to RICA have never been alerted to the fact that they have been monitored even when the monitoring led to no arrests

or prosecutions in South Africa- hence not adopting a similar approach to US interception legislation.

Right to Freedom of Expression

The Constitution protects freedom of speech and expression including communication and telecommunication. Bawa in Thornton (2006:305) argued that any limitation caused by interception and monitoring is an encroachment on the right to communicate and right to freedom of expression. Bawa assessed that the large costs imposed on telecommunication service providers in the application of RICA could cause service providers to decrease in number; thereby limiting the availability of telecommunication services to citizens of South Africa. Although South African telecommunication service providers have not decreased in number, Bawa still believes that it could be a possible infringement of the right to freedom of expression if platforms for expression become limited to citizens.

Hilton Tarrant writing on behalf of Moneyweb identified that millions of South Africans do not have formal proof of residential address; hence, providing such proof for RICA purposes could pose a challenge to these individuals (Tarrant, 2009). Further media reports have highlighted how some South African indigents would have a challenge to provide proof of address particularly as they reside in informal settlements and proof thereof would be hard to obtain (Day, 2013; Duncan, 2015; Kruger, 2009). Hence, the right to communication would be infringed should RICA be applied strictly.

2.8.2 Pre- RICA'ed Sim Cards

Pre-RICA'ed SIM cards are registered before they are purchased and cannot be traced back to the users as they are not registered in their names ("R2K Wants Review Of RICA Laws After Journalists' Phones 'tapped'," 2016). In most cases numerous SIM cards are registered to the seller of the SIMs and are sold as pre-

RICA'ed SIMs. Investigations by *The Times* in 2015 found that pre-RICA'ed SIMs were freely available in Johannesburg and Pretoria. Journalists were able to buy functional SIM cards of all service providers without any documentation that was necessary under Section 40(5) of RICA (Hosken & Smillie, 2015). Hosken & Smillie argued that these activities were in contravention of RICA and these retailers were liable to a fine of R60 000 or imprisonment for one year; however, no statistics were available on arrests or convictions in relation to RICA violations.

2.8.3 Instrument for Political or Personal Gain

Historically, there has been proof that South African politicians and law enforcement officials have abused their access to interception and monitoring powers for political or personal purposes (Nathan, 2009). Nathan surmised that this abuse was to intimidate political opponents (intra- and inter-party) and to manipulate intelligence to influence state decision making.

In a 2018 article, by Professor. Jane Duncan entitled: "What Ramaphosa needs to do to fix state spying, Part 2 – mass and tactical surveillance", Duncan alluded to the State Security Agency (SSA) using mass surveillance (or surveillance targeting several people even if there was no realistic suspicion of wrongdoing) and other surveillance tools because they are so badly regulated (Duncan, 2018). Duncan initially in 2014 and again in 2017 made reference to how the in effectivity of the regulation of RICA has led to inter party and more common intra party interceptions that were conducted leading up to the ruling African National Congress (ANC) party conferences or national / local elections to discredit a particular nominee.

2.9 Oversight of RICA

2.9.1 Legislative Oversight: The Joint Standing Committee on Intelligence

The Joint Standing Committee on Intelligence (JSCI) was established by the Intelligence Services Oversight Act of 1994. It is comprised of approximately 13 parliamentarians whose mandate includes the maintenance of civilian oversight of the intelligence community (Hartley, 2014; Hutton, 2007). One of the main functions of the JSCI is to table a report before parliament by the 31st of March each year, which details the previous year's activity (Intelligence Services Oversight Act, 1994). Hartley (2014), Swart (2011) and Watney (2015) are critical of the lack of transparency of the JSCI. The criticism by Hartley, Swart and Watney stems from the fact that JSCI reports are not made public timeously and the fact that the JSCI meets in secret and the members (irrespective of party) are sworn to secrecy. Nathan (2009) reiterates the same dissatisfaction and identifies the Intelligence Services Oversight Act of 1994 as giving the JSCI the mandate to operate in secrecy. The Intelligence Services Oversight Act of 1994 recommends that only members of the JSCI be present during the proceedings of the committee and that these meetings be held in secret.

Hutton (2007) raises the additional concern that members of the JSCI are appointed by the President and a majority party can hold up to eight seats in the JSCI; hence, threatening the objectivity of the committee.

The JSCI's oversight report in April 2014, the first report in over three years, indicated a sharp rise in the use of surveillance capabilities, with approximately three million interceptions having been carried out in 2010, however only 882 RICA warrants were issued for the same period (Joint Standing Committee on Intelligence, 2010 and 2011–2012, 2014). It was noted by Watney (2012), that there is a total lack of empirical evidence as to whether these RICA warrants were actually useful or not to law enforcement in the investigations they were utilised in. From this statistic Watney inferred that either each warrant was associated with thousands of interceptions or surveillance was conducted without the necessary authorisation. As the statistics only consider how often the RICA judge issues a warrant to intercept

communication, the possibility remains that interception occurred without a judge's approval (R2K State of the Nation report, 2014). Watney (2015) and Swart (2011) have reiterated that the lack of efficiency studies on RICA together with the limited public oversight of interception leaves it and its capacity open to abuse, as was the case of the interception statistics.

2.9.2 Civilian Oversight: Office of the Inspector General for Intelligence

The Office of the Inspector General for Intelligence (OIGI) was established in accordance to the Intelligence Services Oversight Act of 1994. The Inspector General (IG) is nominated by the JSCI and appointed by the President after approval from Parliament (Intelligence Services Oversight Act 40 of 1994).

The Intelligence Services Oversight Act of 1994 allows for complaints to be lodged with the OIGI in cases were members of the public are suspicious of unlawful interception. If interception was conducted covertly, it would only become known once it was disclosed or declassified (Watney, 2015). Watney uses the example of the 2015 SSA Spy cable leaks when Mr Kumi Naidoo (head of Greenpeace at the time) became aware that he was viewed as a threat during a G20 meeting in South Korea. Had the information not been divulged, Mr Naidoo would not have known he had been seen as a potential threat and was being monitored.

2.10 Conclusion to Chapter 2

The outcome of this review indicates that although there have been prior studies done on the limitations of RICA, no assessment has been done from a purely law enforcement perspective. The sections above have illustrated several understandings and explanations from a telecommunications perspective broadly, tapering down to RICA and its manifestations. International literatures on similar laws

have shown to have comparable limitations as RICA, with the right to privacy vs security debate being the most common. The reviewed literature highlights the need for legislative initiatives to be able to deal with advancements in sophisticated technology as well as provide law enforcement officers with sufficient mandate to effectively fight crime and maintain national security. This study will engage law enfacement officers to explore their perceptions of RICA as a crime combatting tool in South Africa.

Chapter 3

Research Methodology

3.1 Introduction

All studies require a comprehensive research approach to achieve its goal (Guba & Lincoln, 1999). This chapter explains the approach to be used to answer the research question and to meet the general research objectives.

Chapter 3 describes the research methodology used, which includes explaining the research concepts, the research paradigm and the research design that the study makes use of. This chapter further explains the appropriateness of the methodology used (sampling, administration of the interviews, collection of data, analysis of data etc.).

This study on RICA as a legislative tool to combat crime in South Africa is qualitative in nature. A qualitative study is often used to attain detailed information about a respondent's thoughts, reasoning, perceptions and motivations with the researcher probing with questions that make it possible for respondents to answer in their own words about how they perceive the issue being studied (Holloway, 1997). Peshkin in Leedy & Ormrod (2015) alluded to qualitative research being unique, as information collected is meant to be described and not predictive. Bryman (2012) further highlighted the importance of the use of words during the gathering and examination of the data collected. In line with the thoughts of Bryman, Holloway and Peshkin a qualitative method was be used in this study in order to describe, evaluate and capture expressive (first hand) data from law enforcement officials that may not have been forthcoming if a quantitative approach was utilised.

3.2 Research Approach

There are many methods that can be utilised in order to collect data using a qualitative method. This study used a phenomenological approach. Twentieth

century philosophers such as Sarte and Marleau-Ponty described the discipline of phenomenology as the study of the way we experience things. Since RICA is an act used by law enforcement officials, their experience with RICA will help understand if RICA is an effective legislative tool to help law enforcement combat crime in South Africa.

As this study aims to detect the difficulties and challenges experienced by law enforcement officials with RICA, a phenomenological method was advantageous as phenomenology usually tries to understand the individual's "real life" experiences. Not only have the difficulties and challenges posed by RICA been identified but also the responses of law enforcement officials to these difficulties and challengers have been noted. Gelman & Nolan (2017) claims that, difficulties and challenges with legislation are every so often due to something that is not working as it was intended to. Hence this study also explores the likely causes of the difficulties and challenges that law enforcement officials experience with RICA and highlights these causal factors, i.e. possible legislative enforcement / development failure.

3.3 Research Strategy

As indicated previously this study was conducted using a qualitative method. Given the fact that no academic work was conducted on RICA (specifically from a law enforcement perspective), the nature of this study is exploratory – which lends itself to a qualitative approach according to Silverman (2017). The answers provided by respondents were qualitative in nature, where experiences were described. Bryman (2012) alludes to strategies in qualitative studies as typically being "constructivist, inductive and interpretivist". However Bryman warns all three elements are not always evident in qualitative studies. In line with the thoughts of Bryman, this study was conducted from an interpretivist/constructivist view, where human nature / feelings were described and understood in relation to the research questions (i.e. the perceptions of law enforcement officials of RICA which emanated from the data collected from law enforcement officials themselves in their natural environment). Merriam (2016), explains that a qualitative researcher collects and analyses data and will build new understanding based on a constructivist interpretation in order to

make sense of a phenomenon assuming that there is not much information on that phenomenon, as is the case with RICA. The main notion surrounding this qualitative strategy is that by using description, knowledge is acquired and through practice that knowledge is created socially whereby the actuality is built by respondents and their experiences who partook in the study (Hill & Wright, 2001).

3.4 Research Design

A Basic Interpretive approach was used in this study, where the researcher was concerned with understanding how law enforcement officials made meaning of RICA and its effectivity in their investigations. Since this study aimed to explore, describe and understand people's perceptions of RICA, the data collected originated from individuals (law enforcement officials) whose experiences, perceptions and understanding were described within the context of the realities that they experienced, as alluded to by Merriam (2016). The researcher himself was responsible for the gathering, analysis and interpretation of the data collected and personally provided a comprehensive account of the results of this study.

3.5 Data Collection

Interviews were used to collect data for this study. As the study is focused around law enforcement officials, data was collected from members of the State Security Agency (SSA). Seven members of the SSA participated in the study. These members ranged from investigators and operational members to members from management- all with the commonality of employing RICA in their respective line functions. As an active member of the SSA, the researcher successfully applied for and gained the necessary approval from the SSA to interview members. A formal request was sent to potential respondents to take part in the study. The request indicated that it was not necessary for respondents to identify themselves and participation was completely voluntary with respondents being able to opt out of the study at any time. Responses received were treated with confidentiality.

3.5.1 Primary data collection

Primary data was collected in the form of unstructured interviews. According to Bloom & Crabtree (2006), unstructured interviews are, “more or less equivalent to guided conversations and allow the researcher to pose follow up questions during the interview”. Bricki & Green (2007) further described unstructured interviews as a valuable tool in exploring participant’s perceptions and experiences in relation to a phenomenon for which limited knowledge is available. Using this type of data collection method the researcher obtained information on the experiences of SSA officials, their perceptions and what RICA means to them. It should be stressed that the primary data collected did not contain any sensitive information relating to any current or previous investigations but focused mainly on understanding the use of RICA in the trade craft of members of the SSA and its subsequent effectivity.

3.5.2 Sampling

The researcher made use of a non-probability sampling technique and purposefully selected the sample that was made use of. Bryman (2012) alluded to qualitative studies tending to employ purposive sampling due to this type of sampling method being conducted with the goals of the study in mind. Hence this sampling method was used because the individuals sampled were relevant to the research question and was familiar with RICA. The sample used consisted of seven SSA officials. Of the seven officials, two of them were investigators who are involved in active investigations, two are project leaders who are responsible for project management (both admin and investigative functions), two are Acting General Managers in management positions, responsible for decision-making, while the last individual was an operational analyst who is actively involved in tactical analysis. The researcher was open to any recommendations made by respondents to other SSA officials who used RICA in their daily line functions therefore other SSA members were chosen using a snowballing (referral) technique within the SSA.

3.6 Data Analysis

After collecting the necessary data for the study, the data was transcribed and arranged in an orderly, methodological fashion - these steps according to Badenhorst (2007) are the first stages of analysis. Furthermore Lacey & Luff (2001) indicated that the data needs to also be described and summarized. This description and summary referred to by Lacy & Luff, was done by arranging the data collected into smaller manageable units, where the data was, “synthesized”, explored for common patterns and meaning as also employed by Cresswell (2003). The researcher examined and analyzed each transcript methodically, in the process grouping together similar themes and attempting to understand them, and making deductions. Bryman (2012), Maxwell (2012) and Silverman (2017) agree that the process of qualitative data analysis is an iterative one, where one goes back and forth between the collection and analysis of data. Analysis of data commenced soon after collecting some of the initial information and not after the completion of the collection phase. The findings from this initial analysis helped to improve the following stages of the data collection phase.

3.7 Validity and Reliability

During June 2016, a lecture on qualitative research methods given by Dr. Lynn Hewlett described validity and reliability to be concepts that “emerged from quantitative research” (Hewlett, 2016). Mason (1996) described Validity as “whether the researcher is observing, identifying or measuring what she or he claims to be measuring”. McMillan & Schumacher (1993) referred to Reliability as the “consistency of the researcher’s interactive style, data recording, data analysis and interpretation of participants”. Qualitative researchers such as Drost & O'Reilly (2011) Shenton (2004) recommended alternatives to Validity and Reliability because of their quantitative origin’s. Barrett, Mayan, Morse, Olson & Spiers (2002), suggested authenticity and trustworthiness as measures for assessing qualitative studies conducted. As indicated by Mason (1996), Trustworthiness is defined in terms of “credibility, transferability, dependability and confirmability”. For practicality sake this study will be assessed through the concept of credibility, data collected (including

primary interpretations made by researcher) will be taken back to the people involved in the study to verify if what is reflected is correct and plausible, and if there is a nexus between the findings of the study and the actual experiences and perceptions of the respondents. During this process of Member Checking, as referred to by Shenton (2004), problems relating to the correctness of information were corrected as suggested. Difficulties related to the researchers interpretation of information dictated that the data in question be seen as new to the study and was used to examine the inconsistency around interpretation.

As argued by Guba & Lincoln (1999) it is not imperative that the findings of a study are the same as another, but the findings should be consistent with the data that was collected. Subscribing to Guba & Lincoln's argument, data collected was also shared with other colleagues / peers to review how accurate the emerging deductions of the study are. Specialists (employed at the SSA) in the legal and policy and research and development fields were approached for their views on the findings of the study- assisting the reliability of the study.

To help with generalizability of this study the researcher retained detailed notes and write ups in every stage of the research process. These notes and write ups helped explain and describe the context and assumptions that was important to this study and also played a role in reminders to the researcher as at time he did have difficulty recollecting some processes. As qualitative studies are more difficult to replicate in comparison to quantitative studies, other researchers wanting to conduct a similar study could adopt similar methods/techniques/actions (as described in the detailed notes and write ups of the researcher) in order to aid replicating the study.

3.8 Ethical Considerations

Ethics was considered in all stages of this study, from devising ideas, to designing the study, to collecting the data via interviews and will be considered till the final publication of the findings. Since the participants were SSA officials and were asked to reveal information regarding their tradecraft and their perceptions of RICA, some

of their personal views/perceptions on RICA as a crime combatting legislative tool might be disputed especially from a policy implementation failure perspective.

Permission for the study was sought and granted from SSA management in order for the members to participate at ease and voluntarily - with the proviso being that on successful completion of the study the results will be presented to SSA management. SSA members the study were informed that they are under no obligation (even if the researcher is known to them) to participate and do so voluntarily and can opt out at any given time. Permission to partake in the study and to record the interviews electronically was obtained by the researcher in writing. The information was collected via mutual trust and the identities of the respondents will be kept confidential. The researchers' supervisors contact details were shared with all participants (in the consent form) in the event of respondents experiencing any harm or had concerns about the study.

The researcher was previously employed as an operational analyst at the South African Police Service Crime Intelligence Division and is currently employed by the SSA. The researcher is currently a senior situational analyst that does interact with investigators / operational analysts/ Project leaders and General Managers from the SSA. However it should be stressed that there does not exist a power relationship between the researcher and some of the respondents as the researcher has a different line function with its own management structure that is independent of the operational line functions of most of the respondents. Hence there was no compulsion on the respondents to cooperate with the researcher or to answer questions in a way as to appease the researcher.

3.9 Limitations

This study aimed to explore law enforcement official's perceptions of RICA as a legislative tool to combat crime in South Africa, to understand if RICA is actually helpful to law enforcement officials and to see where it can be improved in order to combat crime. This study limited itself to interviews that were conducted with SSA members from Headquarters, members of the Office of the Interception Centre (OIC)

and Gauteng provincial office members. The findings were made from data collected from this population set.

The SAPS were asked for permission to conduct this study however no response was attained. Hence no SAPS members were approached or took part in the study. The non-participation of the SAPS in this study is a noteworthy limitation on its findings, as RICA provides for interceptions to be used by other agencies other than only the SSA.

Although the citation of prior literature on RICA and its role in law enforcement should have formed the basis of the literature review and should have assisted in laying a foundation for understanding the research question and problem, there has been little research conducted on RICA and how it is utilised in law enforcement operations. It is for these reasons that the researcher tended to use a more exploratory rather than an explanatory outlook in the study.

As mentioned previously, the researcher is also an employee of the SSA. The SSA has been characterised in the past as being plagued by high levels of mutual distrust among its employees, hence it would be difficult for the researcher to assert that there was total “mutual trust” between him and the respondents. This could have had an influence on the study -imposing important limitations to the study by the respondents not trusting the researcher enough to fully disclose their views on more sensitive issues. The electronic recordings made (if permission was granted) of the interviews may have been an additional factor that may have contributed to respondents censoring what they have to say.

3.10 Conclusion

This chapter provided a description of the qualitative research method that was utilised in this study. Due to this non response the researcher continued to utilize members of the SSA where members were authorised to participate. The following chapter presents and describes the results of the study. The following chapter will also discuss the findings and recommendations.

Chapter 4

Presentation of Results

4.1 Introduction

This chapter presents the data collected and the researchers' summary of the results. The findings presented are based on the responses to the questions posed by the researcher to the respondents in the study. There was one primary question which was further broken down into sub-questions to arrive at one consolidated answer.

As previously mentioned in Chapter 3, in qualitative studies, data presented needs to be presented in a methodical manner and should be examined and interpreted so as to arrive at a conclusion with recommendations (Badenhorst, 2007). The data presented in this chapter will show what the researcher has learned and will present the themes as well as a descriptive account done by the researcher. Participants' identities will remain anonymous.

4.2 Presentation of Data

The data that follows was attained during the interviews with the seven different participants. The participants were all asked the same questions.

Main question of study: What are law enforcement officials' perceptions towards RICA as a legislative tool to combat criminal activity in South Africa?

4.2.1 Participant 1

Sub-Questions:

4.2.1.1 Describe why was there a need for RICA in law enforcement investigations?

Participant 1 indicated that RICA was needed to regulate intercepts and the manner in which interceptions were done. Before RICA it was easier to get interceptions done, where law enforcement had more time to investigate, as intercept applications were not governed by the three month monitoring period as is currently the case with RICA applications. Participant 1 firmly believed that RICA helped alleviate miss use of interceptions for personal or political motives. According to Participant 1, RICA (if correctly applied and enforced) helps identify individuals that conducted crime using cell phones and other sophisticated technologies. Before RICA individuals could not be identified through their phone number. Participant 1 thought that RICA on its inception, would force telecommunication service providers (TSP) to register all individuals making use of their networks, making it easier for law enforcement to identify individuals that commit crimes using telecommunication devices.

4.2.1.2 How is RICA used in law enforcement?

Participant 1 indicated that RICA is used to identify an individual that uses a specific cellular phone number. That information on the individual is used to motivate for the monitoring of the communications of that specific individual. According to Participant 1, if the phone number in question is registered according to RICA then the information from TSPs such as tower information, address, next of kin and financials become significant to investigations.

4.2.1.3 What are the benefits of RICA to law enforcement?

Participant 1 indicated that RICA is a good piece of legislation and if implemented /enforced correctly will be beneficial to law enforcement in that they would be able to

trace a person through their cellular phone numbers. Currently Participant 1 does not see any advantages of RICA as in most cases RICA applications return negative in that either the incorrect person is registered to a number or the number is not registered at all but still operating on telecommunication networks in South Africa. Participant 1 showed frustration in the loss of valuable time by sometimes tracking down the wrong person that a RICA request has identified. The one benefit that participant 1 sees is that the interception of communication became harder after RICA was implemented, hence making it difficult for interceptions to be conducted for personal or political reasons (limiting misuse).

4.2.1.4 Describe the challenges and short comings of RICA to law enforcement?

Participant 1 indicated that although RICA is clear in what it intends to achieve as a legislation to combat crime, there is no implementation of the act. The issues relating to pre-RICA'ed or un-RICA'ed sims is still a problem for law enforcement officials. According to Participant 1 no one is taking responsibility to stop traders from selling sim cards that are not RICA''Ed or are pre-RICA'ed, because the TSPs will lose revenue if they start blocking un-registered sims on their networks. Participant 1 also referred to the long time that it takes for a RICA application to be signed by the designated RICA judge (in some instances 3 months) - this was owing to the unavailability of the RICA judge or the complicated manual application process. This large time lapse according to Participant 1 could be to the detriment of national security threats – like an act of terror.

4.2.1.5 Has RICA been an effective legislative tool to combat crime in South Africa?

Participant 1 indicated that RICA is not effective, citing the issues relating to un-RICA'ed and pre-RICA'ed sim cards. And another issue is that most individuals being investigated don't use the phone to converse in the traditional manner. Smart phones are used to communicate on different platforms that RICA does not cater for e.g. social media platforms and other messenger services.

4.2.1.6 What improvements in RICA would you like to see that could aid law enforcement in future?

Participant 1 indicated that if more RICA judges could be available that will lessen the time it takes to get RICA applications finalized hence subsequent investigation and telecommunication interceptions will be concluded more timeously. Participant 1 suggested the standardization of the RICA application process, where a sort of "check list" is attached to the RICA application, according to participant 1 this would allow the timeous processing of the application by the judge. Although Participant 1 does not know whose responsibility it should be but RICA has to be enforced and checks and balances have to be done from time to time- especially in the informal trade sector.

Summary Participant 1

Participant 1 believes that RICA is a good legislation in theory, however due to the lack of enforcement of the legislation it is currently ineffective in assisting law enforcement to combat crime in South Africa. She was most critical of the process involved in applying for RICA information, citing that the appointment of one RICA judge to look at all applications makes the process long and ineffective, which could possibly having a negative effect on investigations dealing with imminent threats to South Africa in future. Participant 1 recommended a streamlining of the RICA application process, and the addition of more judges to assess RICA applications from law enforcement.

4.2.2 Participant 2

Sub-Questions:

4.2.2.1 Describe why was there a need for RICA in law enforcement investigations?

Participant 2 said that the previous legislation before RICA, the Interception and Monitoring Prohibition Act 127 of 1992 was open to monitoring and interceptions that infringed on the human rights, hence participant 2 believes that RICA was needed to in order to stop the exploitation of human rights. According to Participant 2 in the past crimes were perpetrated simplistically, with the advancement of technology criminals started to make use of more complex and sophisticated technologies to commit crime and to remain undetected. RICA was supposed to help law enforcement combat crimes using these types of new technologies- by tracing individuals that make use of devices such as cellular phones to commit crime. Participant 2 simplified the statement to say, “By putting a name to a cellular number”.

4.2.2.2 How is RICA used in law enforcement?

Participant 2 indicated that he used RICA to identify the user / owner of a specific cellular number. Participant 2 also referred to information such as itemized billing (which is also attained through a RICA request) being very useful in that it helps the participant to identify associates of the suspect and ultimately this information is used to motivate for an interception of that specific number.

4.2.2.3 What are the benefits of RICA to law enforcement?

Participant 2 began his answer to this question by indicating that RICA will be very useful to him if the act is adhered to correctly. If the act was correctly implemented and adhered to then as a law enforcement official RICA would be able to help build up a picture and would assist the participant in basing his future operational planning on the information he would have attained from RICA applications- and most importantly being able to put a name to a cellular number user. However according to participant 2 in the present state RICA is in, it has very limited advantages or benefits.

4.2.2.4 Describe the challenges and short comings of RICA to law enforcement?

The main problem with RICA for participant 2 was that of Pre-RICA'ed and sim cards that are not RICA'ed. By not being able to identify a user in most instances, participant 2 views this as being contrary to what RICA was created for. However participant 2 made an interesting statement indicating that his tradecraft also included the use of sim cards that have not been RICA'ed in order to execute his operational plans without detection. The time it takes for a RICA application to be approved is also lengthy in the opinion of participant 2. Participant 2 also highlighted the fact that foreign sim cards are used on South African TSPs networks. It becomes concerning to law enforcement as these foreign sim cards don't fall under the scope of RICA, and when South African law enforcement revert back to that foreign TSP to which that sim belongs for details nothing is forthcoming.

4.2.2.5 Has RICA been an effective legislative tool to combat crime in South Africa?

In the opinion of participant 2, RICA is not and will not be an effective tool until it is implemented and adhered to correctly. Participant 2 confessed that although he is not a lawyer, he feels that RICA, when scrutinized is very conducive to helping law enforcement combatting crime however he sees the "stumbling block" being adherence to and the implementation of RICA.

4.2.2.6 What improvements in RICA would you like to see that could aid law enforcement in future?

Participant 2 reiterated that if RICA was enforced especially in relation to pre-RICA'ed and un-RICA'ed sims then this would help law enforcement with profiling offenders positively. Participant 2 recommends more RICA judges or a RICA panel be appointed in order to assess and grant RICA applications- this would speed up the process. Participant 2 also recommended the actual RICA application should be sped up and the recommendation was to look into a "sort of automated application process". Participant 2 also felt strongly about improving RICA in order for the

legislation to take into account international sims used in RSA. Participant 2 recommended that international sims also be registered in the same way that domestic TSP sims are required to be registered- as outlined in RICA.

Summary Participant 2

Participant 2 believes that RICA as it is presently applied is not effective in helping law enforcement officials. However if RICA is properly implemented and enforced RICA would definitely help combat crimes. Participant 2 highlighted concerns in relation to foreign and local sim cards that were not RICA'ed or Pre-RICA'ed and how this in most instances wastes time of investigations. Participant 2 also highlighted the importance of this loophole in RICA which works to his advantage in his operational initiatives. Participant 2 also complained about the time it takes for a RICA application to be completed recommending a more "automated" process which could include the addition of more RICA judges.

4.2.3 Participant 3

4.2.3.1 Describe why was there a need for RICA in law enforcement investigations?

Participant 3 indicated that RICA allowed for the regulation of how telecommunication was intercepted. In the opinion of participant 3 RICA set out to assist law enforcement in combatting crimes perpetrated using cellular phones.

4.2.3.2 How is RICA used in law enforcement?

Participant 3 indicated that he mainly used RICA in order to try to identify the user of a cellular phone number. However participant 3 admitted that he does not use RICA much presently as past experience using RICA led him on "goose chases" which wasted his time and didn't lead to any major breakthroughs. More positive identification of cellular numbers was made using avenues such as credit inform or tracepts.

4.2.3.3 What are the benefits of RICA to law enforcement?

Participant 3 explained that in his experience with RICA there is no benefit to law enforcement at present. RICA currently wastes time due to most people identified through RICA process being the incorrect person- hence according to participant 3 most RICA information on registered users received from TSPs cannot be trusted.

4.2.3.4 Describe the challenges and short comings of RICA to law enforcement?

Participant 3 described his frustration with the RICA application process and the length of time it takes to get an application approved. Another challenge faced by participant 3 was the motivation needed by the Judge to approve a RICA request. In some cases the judge needed full disclosure and strong motivations and on other occasions the judge approved with just a brief motivation. According to participant 3 there was no standardized procedure in the application process. In the experience of participant 3 most pre-paid sim cards used by suspects were never RICA'ed or were registered to the wrong person- hence his frustration with the time wasted in tracking the wrong person identified by RICA application.

4.2.3.5 Has RICA been an effective legislative tool to combat crime in South Africa?

Participant 3 indicated that for him RICA was not an effective tool to combat crime in South Africa. Participant said that in some cases he spent more time investigating and verifying RICA information just to check its accuracy.

4.2.3.6 What improvements in RICA would you like to see that could aid law enforcement in future?

According to Participant 3 although he is frustrated by RICA he believes that the legislation is a sound legislation with enforcement of it being the primary problem. Participant 3 would like to see TSPs making sure to register all sims on their networks, making sure that the sims are registered according to RICA alleviating the

problems of Pre and un- RICA'ed sim cards. Awareness programs should be implemented especially within the informal business sector to help with the understanding and interpretation of RICA and what the penalties are for non-compliance. Then penalties should be enforced for noncompliance especially in light of businesses knowing what they needed to do to abide to RICA- hence reducing claims of ignorance due to not knowing.

Summary Participant 3

Although participant 3 didn't take issue with RICA as legislation, he was scathing of RICA in its implementation and enforcement, indicating that it is not effective to the extent that he rarely applies for RICA information currently. In the past the participant used to apply for RICA information however information provided to him was inaccurate and the process of a RICA application took a long time. The participant recommended enforcement of RICA be duly exercised, with TSPs taking more responsibility for the registration of pre-paid sim cards using their networks.

4.2.4 Participant 4

4.2.4.1 Describe why was there a need for RICA in law enforcement investigations?

According to participant 4, the Interception and Monitoring Prohibition Act 127 of 1992 did not accommodate for the compulsory registration of sim cards- making it difficult for law enforcement to identify the users of specific cellular numbers during criminal investigation. Participant indicated that although prior to RICA being enacted, the user of a specific number could be identified operationally (e.g. through surveillance). It took a lot of time and posed legal challenges when in a court of law. Participant 4 believed that RICA was created in order to assist law enforcement in tracing and profiling individuals that made use of cellular phones in carry out their criminal activities.

4.2.4.2 How is RICA used in law enforcement?

Participant 4 uses RICA as an investigative tool- to identify individuals and to get hold of information from TSPs that assists in building a profile of a person of interest. Participant offered an example of tower information that could confirm where the suspect was, thereby allowing the participant to allocate operational resources to that specific area highlighted by the tower information- hence saving time and resources.

4.2.4.3 What are the benefits of RICA to law enforcement?

Participant 4 confidently indicated that RICA has assisted him in investigations that he conducted. He made references to investigations relating to dated issues where RICA was used to identify individuals and associates and their travel patterns (through the person's location). Participant 4 indicated that the benefits of using RICA are only seen in investigations when RICA is correctly enforced and applied, without which identifying a person through RICA would not yielded positive results and would be ineffective.

4.2.4.4 Describe the challenges and short comings of RICA to law enforcement?

Compliance to RICA and its implementation is the biggest shortcoming highlighted by participant 4. According to participant 4, un-registered sim cards and wrongly registered sims (pre-RICA'ed sims) are the eventualities of RICA not being enforced and complied with. This issue is the biggest "headache" for participant 4 as loads of time is wasted in going through the RICA application process and then receiving information from TSPs that is inaccurate which is investigated on leading to time loss. The time it takes to get a RICA application concluded is also of concern to participant 4, as in cases where there is an imminent threat the process will hold back investigations. Participant 4 also highlighted the problems he encountered when trying to get ownership information pertaining to foreign sim cards that are using South African telecommunication networks- in nearly all cases no information was attainable due to foreign mobile operator denying request.

4.2.4.5 Has RICA been an effective legislative tool to combat crime in South Africa?

Although participant 4 has seen some breakthroughs using RICA, he believes that if RICA was correctly enforced it would be an even more effective in helping law enforcement, however at present it is not as effective as it was intended to be due to issues such as the use of un-registered and pre-RICA'ed sim cards.

4.2.4.6 What improvements in RICA would you like to see that could aid law enforcement in future?

First and foremost participant 4 indicated that the compliance of RICA needs to be looked at. According to participant 4, if compliance is sorted out then most of the issues he has would be taken care of (such as the proliferation of pre-RICA'ed and un-registered sim cards). Participant 4 believes that the TSPs needs to take responsibility for enforcing RICA, however also understands that the TSPs wouldn't want to owing to the potential loss of revenue. Participant 4 also recommended that RICA enforce the registration of foreign sim cards in order for tracing to occur if needs be. As an operational member participant 4 would also like to see the RICA application process be simplified and shortened in order for urgent issues to be dealt with.

Summary Participant 4

Participant 4 indicated that RICA was intended to help track and trace criminals that utilized cellular phones to commit crime. Participant 4 predominantly uses RICA to attempt to match a cellular number to an individual and also indicated tower information from RICA applications being very important to his investigations. Although participant 4 did experience some breakthroughs in cases using RICA, he confessed that these cases were very few and was down to RICA being implemented and enforced correctly. Participant 4 was concerned with the length of the RICA application process and recommended speeding up the process. The ineffectively of obtaining information on foreign sim cards operating in South Africa was also highlighted by participant 4, with participant 4 wanting these sims to be

subjected to some sort of registration process as well before using mobile networks in South Africa.

4.2.5 Participant 5

4.2.5.1 Describe why was there a need for RICA in law enforcement investigations?

According to participant 5, RICA was needed to combat the challenge posed by unregistered sim cards used in the planning and execution of crime in South Africa.

4.2.5.2 How is RICA used in law enforcement?

Participant 5 uses RICA as an intelligence gathering tool to attain information on a person linked to a specific cellular number, which is then used to motivate for the interception of communications of that individual. The information derived from interceptions allows participant 5 to piece together the individuals' activities, movements and future plans, however this is depended on what the suspect discusses on the phone. In some investigations tower information (as provided by RICA application) was critical in apprehending the suspects.

4.2.5.3 What are the benefits of RICA to law enforcement?

For participant 5, RICA is sometimes beneficial in that it helps in identifying associates of suspects, gives you forewarning of their travels and on a few occasions has supplied information on planned criminal activities. RICA has been helpful to participant 5 in reconstruction exercises, where data from detailed billing was used.

4.2.5.4 Describe the challenges and short comings of RICA to law enforcement?

Participant 5 described the “lag time” between the application, approval and actual implementation of the RICA request being its biggest disadvantage to law enforcement officers. In the participants view this was down to there being only one RICA judge nationally.

Participant 5 also highlighted the limitation she found in RICA not being geared to attain information carried through data (e.g. social media and other messaging services using data). The participant indicated that she didn’t know if this was a legislative or technological flaw but mentioned, “in this day and age most people communicate this way”, hence this information remains critical however the participant cannot get access to this type of information.

4.2.5.5 Has RICA been an effective legislative tool to combat crime in South Africa?

Participant 5 indicated that RICA is not as effective as it is far too easy to circumvent it. Often participant 5 has found that numbers are in fact not registered or are registered to the incorrect people, but still operate on South Africa’s TSP networks.

4.2.5.6 What improvements in RICA would you like to see that could aid law enforcement in future?

Participant 5 would like to see RICA being enforced and she puts the onous on the TSPs to enforce the act. According to the participant there has to be a large financial penalty for non compliance. The participant also recomneded that RICA needs to be ammended to limit the number of sim cards that an indiviual can own- hence stopping batch pre-RICA’ed sims from entering the market. The partiicpant also recomends the RICA application process to be shortend with an addition of RICA judges or making the application process electronic. Participant 5 also would like to see that TSPs verify the information that customers provide to them for RICA

purposes-as this would help limit in-acurate information being provided to law enforcement from TSPs .

Summary Participant 5

Participant 5 believed that RICA was introduced in order to deal with unregistered sim cards. Participant uses RICA as an intelligence gathering tool and places importance on the identity information as well as the tower information that a RICA application returns. In the short time that participant 5 has used RICA she believes it is sometimes very beneficial to her and has helped her with mostly reconstruction of events in cases however overall it is not as beneficial as RICA is very easily circumvented. Participant 5 would like to see RICA enforced more stringently and places the onus on the TSPs in South Africa to make sure of compliance. Participant 5 also recommend that more RICA judges be added and the process to become an electronic one in order to make the process quicker.

4.2.6 Participant 6

4.2.6.1 Describe why was there a need for RICA in law enforcement investigations?

Participant 6 indicated that in the past, the Interception and Monitoring Prohibition Act 127 of 1992, was geared towards fixed line interceptions only. There was a need to be able to intercept more sophisticated /modern modes of communication- which RICA was created to help with. There was also a need to centralize all interceptions that were done in RSA. The Office of the Interception Centre (OIC) was created for this purpose under RICA.

4.2.6.2 How is RICA used in law enforcement?

Participant 6 indicated that at an operational level RICA is mostly used to identify the user of a specific cellular number. In some cases information from TSPs that was attained through RICA requests, was used to build profiles of criminals. Participant 6

also alluded to the OIC, which was borne out of RICA, giving law enforcement officials a central point to conduct legitimate interceptions- with no interceptions conducted without approval from the RICA judge.

4.2.6.3 What are the benefits of RICA to law enforcement?

Participant 6 said that RICA is beneficial to law enforcement in their profiling and identification processes. However the participant quantified this by saying that only if RICA was complied with, law enforcement officials would be able to identify the user of a specific number and be able to get some critical information from TSPs related to that user.

4.2.6.4 Describe the challenges and short comings of RICA to law enforcement?

Participant 6 expressed his dismay at the current state of RICA. In the view of participant 6, the lack of enforcement and compliance to RICA has led to it to being largely ineffective in helping law enforcement officials to fight crime. According to participant 6, RICA is a good piece of legislation to assist law enforcement however without having the technical capabilities to allow for effective RICA application, could render the legislation in effective- as is the case at present. Participant 6 summarized his view by saying “the legislation and the technical capabilities available at present must be taken into consideration”. From an OIC perspective participant 6 indicated that there currently exists too outdated technology to effectively service RICA applications from law enforcement officials. Participant 6 also believes that the 3 months interception period that RICA permits do not allow for the full range of interceptions as this time period is too short to attain decent information for law enforcement. The manual administration process and the time it takes to get a RICA application approved is also a challenge for participant 6. Participant 6 indicates this is not good when there is an imminent threat to national security. Participant 6 also highlighted how the noncompliance and enforcement of RICA has led to the rise in the availability of pre-RICA’ed and un registered sim cards in South Africa, however according to participant 6 this phenomenon is more applicable to pre-paid sim cards and not contracted ones. Not only does this waste

the time of law enforcement officials but also the OICs', whose staff sometimes go through the process of intercepting communications as per a RICA request only to be later told by investigators that it was the wrong individual identified. Participant 6 also raised concerned that the registration of a sim according to RICA is not verified to be correct, if customer provides an address then no checks are done to see if it is a legitimate address or if the identity of a client is actually authentic.

4.2.6.5 Has RICA been an effective legislative tool to combat crime in South Africa?

Participant 6 indicated that to a certain extent RICA has successfully identified perpetrators; however this was when RICA was fully complied with. However in most investigations at present RICA is not complied with, making it very difficult for law enforcement to obtain credible information – hence rendering RICA ineffective in crime combatting initiatives presently.

4.2.6.6 What improvements in RICA would you like to see that could aid law enforcement in future?

Participant 6 recommends that RICA needs to be able to keep abreast with the changing world technology, as many technologies (especially in relation to communications) have evolved since RICAs implementation. A verification process needs to be built into RICA where checks on identities and addresses could be done. The participant also wants to see more oversight of RICA, as he believes that RICA data belongs to the state and law enforcements ease of access to the data in extreme cases relating to life and death / national security needs to be prescribed. Lastly participant 6 indicated that the compliance with and enforcement of RICA needs to become the responsibility of TSPs and that fines imposed to TSPs for non-compliance should "outweigh" their potential profits from unregistered sims.

Summary Participant 6

Participant 6 believes RICA was needed in order to intercept more sophisticated modes of communication especially those communication devices that were not

fixed line. RICA also provided for the centralization of all interceptions under the OIC. Participant 1 indicated that RICA is used by law enforcement officers to identify users of specific cellular numbers and to use this information to motivate for an interception of communications. Participant 6 was perturbed at the current state of RICA where mostly, enforcement and compliance issues have rendered RICA in-effective to combat crime in South Africa. Participant 6 recommends that RICA needs to be able to change in line with changing technologies of the day and that verification processes need to be implemented and enforced at sim registration stage.

4.2.7 Participant 7

4.2.7.1 Describe why was there a need for RICA in law enforcement investigations?

Participant 7 indicated that RICA was enacted to regulate interceptions of communications in South Africa, making it less susceptible for abuse and illegal use. The participant also indicated that RICA was implemented to assist law enforcement officials in identifying individuals (for profiling purposes) that made use of cellular phones during criminal activities.

4.2.7.2 How is RICA used in law enforcement?

Participant 7 indicated that he used RICA to identify the user/owner of a particular cellular number. This information was further used to motivate for an interception of the communications of that specific individual under RICA.

4.2.7.3 What are the benefits of RICA to law enforcement?

Participant 7 reiterated that If RICA was adhered to, to the fullest then there would be lots of investigative advantages in using it. It could possibility assist in uncovering the identity of a suspect, their plans as well as other participants in the illegal activity. Participant 7 indicated that he only benefits from RICA in terms of interception

information provided under RICA, where in a few cases, suspects' plans and other associates were identified through their intercepted communications – but participant 7 admitted and wanted to place on record that this happened in very few investigations, highlighting in most cases RICA didn't help.

4.2.7.4 Describe the challenges and short comings of RICA to law enforcement?

According to participant 7, RICA is not beneficial as it has not allowed him to make any major breakthroughs in cases due to incorrect information being supplied from TSPs. Participant 7 made an example of numerous numbers that he tried to link to individuals thorough the RICA process was a waste of time as the information didn't exist (sim was not RICA'ed) or it was the wrong person identified by the TSPs. Participant 7 further indicated the RICA application process to be "slow and bureaucratic". Participant 7 elucidated to say that in some instances when the RICA application is signed and returned to him then a lot of time has already expired in the administration process, limiting his interception time according to what is signed in the warrant.

4.2.7.5 Has RICA been an effective legislative tool to combat crime in South Africa?

According to participant 7, RICA has not being an effective tool to fight crime in South Africa. Participant 7 owed the ineffectiveness of RICA to how it is enforced. Participant 7 indicated that no one is checking if RICA is complied with. According to participant 7 just by making sure that every sim operating on the networks in South Africa is registered with the correct details will make RICA much more effective for law enforcement.

4.2.7.6 What improvements in RICA would you like to see that could aid law enforcement in future?

Participant 7 believes that RICA's biggest problem is its implementation. Participant 7 proposes that there needs to be someone held accountable to enforce RICA.

Participant 7s' view is that the TSPs in South Africa should take full responsibility for making sure that RICA is adhered to and for closing down sim cards that have not being RICA'ed- even though it would hurt their profits.

Participant 7 suggests that the RICA application process should be made more useable and streamlined to allow law enforcement to deal with threats timeously. Participant 7 also recommends that more judges need to be able to approved RICA applications which will help clear "backlogs" of RICA applications.

Summary Participant 7

Participant 7 indicted that RICA was needed in order to regulate and control how interception of communications was conducted. Participant 7 indicated that law enforcement needed RICA specifically for profiling purposes where the cellular number was used to identify the user through a RICA application. Participant 7 believed strongly that if RICA was implemented correctly then the identification of the user of a cellular number through the RICA process would be very profitable for law enforcement officials. However as RICA currently exists, it is not beneficial to law enforcement officials presently according to Participant 7. This is owing to sims not being RICA'ed or the slow pace at which RICA applications are attended to. Participant 7 would like to see RICA implemented more stringently and wants to have accountability in terms of enforcing RICA especially in the informal trade sector.

Chapter 5

Analysis of the Research

5.1 Introduction

This chapter presents the findings of the study. The analysis will encapsulate answers to questions, which were aimed at understanding the perceptions of law enforcement officials' towards RICA as a legislative tool to combat crime in South Africa and eventually gauging the effectiveness of this legislation for law enforcement.

This study concentrated on RICA with the purpose being to identify and describe how law enforcement officials used this act and generally how they felt about this act. Furthermore this study also elucidated possible remedies to the current shortcomings experienced by law enforcement officials when applying RICA in their respective line functions.

Recommendations are made based on the findings from this study. It became apparent from this study that RICA as a legislative tool to fight crime is not without challenges and there is a need for prompt intervention, especially in terms of RICA's implementation and enforcement.

In this section of the study, the findings will be explained, followed by possible recommendations. The chapter will close with deductions / conclusions drawn from this study.

5.2 Findings

The findings that are presented were gathered from the data collected commencing from the literature review conducted, the interviews concluded and the personal understanding of the researcher to the research questions.

5.2.1 Question One: **Describe why was there a need for RICA in law enforcement investigations?**

It is apparent from the data that law enforcement officials believed that the previous Interception and Monitoring Prohibition Act 127 of 1992 catered more for fixed line interceptions and did not cater for the interception of more modern types of technologies therefore new legislation was required to address this. The data collected suggests that RICA was needed by law enforcement in order to keep pace with criminals who were starting to use more complex and sophisticated tools to conduct crimes. The data strongly suggests that RICA was needed to help identify and trace individuals that made use of sophisticated ever-developing technologies, such as cellular phones, to conduct criminal activity. Hence in line with what RICA was implemented to do, law enforcement officials expected RICA to make it mandatory for TSPs to register all users on their networks making it easier for law enforcement officials to identify and trace offenders that made use of cellular phones to commit crime. The collected data indicates that there was also a need to regulate how intercepts were conducted in order to stop illegal use – which manifested in publicized human rights violations. Data illustrates that RICA was also needed in order to provide a mechanism to centralize all interceptions conducted by law enforcement in South Africa. This was done through the creation of the OIC, as mandated by RICA- which was envisioned to help regulate interceptions and ultimately with the oversight of interceptions conducted.

5.2.2 Question Two: **How is RICA currently used in Law Enforcement?**

Data strongly suggests that RICA was primarily used as a simple investigative tool for identification and profiling purposes. With the phrase "*trying to put a name to a cellular number*" being a popular response. RICA information was then used to motivate for permission to intercept the identified number through the OIC. Additional information attained through RICA requests to TSPs are also used to locate an individual, build a profile of the individual or to identify other associates of the individual. An example provided was cellular tower information, which helped locate an individual, allowing law enforcement to allocate resources to that specific area. It was highlighted that although RICA requests might not have successfully confirmed

the user of a SIM, the tower mapping information of the SIM proved very useful when the location of an individual was required.

Data also suggests that due to issues relating to non-compliance with RICA, some law enforcement officials have avoided using RICA to conduct primary checks against cellular numbers. The reasons for this was the loss of valuable time profiling the wrong person or not having any person registered to a cellular number. Other avenues like creditinform, truecaller and tracepts were used instead of RICA, which according to law enforcement officials were more accurate.

It is unmistakable that law enforcement officials do not know or understand RICA in its entirety this explains their simplistic responses of the use of RICA in law enforcement. Respondents were very knowledgeable of Chapter 2 of RICA, which gave law enforcement the power of interception, however the understanding of other facets of RICA legislation was lacking. Knowledge of Chapter 7 of RICA was lacking from law enforcement officials especially to limitations to complying to Chapter 7 by the public.

5.2.3 Question Three: **What are the benefits of RICA to Law Enforcement?**

Law enforcement officials confirm that if RICA was complied with then there would be enormous advantages for them, especially in terms of identifying, locating and profiling offenders and their associates. This is strongly illustrated in the study where any benefits identified were mostly accompanied by the caveat, "*if RICA was implemented and enforced correctly...*" It is apparent that law enforcement officials currently see no or very limited successes /benefits when using RICA in their respective trade craft. The information points strongly to the lack of implementation and enforcement of/compliance to RICA rather than weak legislation, as being the hindrance to law enforcement officials. Benefits identified related mostly to the regulation of intercepts and how it has become more difficult to misuse intercepts, however the oversight in terms of RICA applications approved still remains a concern to the law enforcement officials interviewed-as they still believe that the application process can be manipulated especially by law enforcement.

5.2.4 Question Four: **Describe the challenges and short comings of RICA to law enforcement**

The study has identified the following challengers associated with RICA for law enforcement officials:

Non-Compliance and lack of corrective measures for non-compliance

It was established in the study that law enforcement officials believe that informal and to lesser extent formal traders have the recurring tendency to not comply with RICA, in terms of registering new SIM cards to users. This non-compliance has given rise to the proliferation of pre-RICA'ed and un-registered SIM cards being continuously used on South African telecommunication networks. It was also indicated that South African TSPs and law enforcement do not have any inspection or enforcement initiatives in place to ensure compliance to RICA and in general there is no active corrective measures for non-compliance except the punitive measures stated in RICA, which is largely ignored and to a large degree rarely enforced. To exacerbate this situation there is evidently a grey area as to whose responsibility it is to inspect compliance and assist with corrective measures. As all respondents were from law enforcement the predictable response was that South African TSPs should be made responsible for inspecting for compliance, especially in the informal trade sector.

Law enforcement officials assessed that South African TSPs will lose revenue if they were to act strictly in line with RICA and decommission SIMS that were not registered as per RICA, hence SIM cards (domestic or international) that are not registered in line with RICA are not shut down in South Africa due to the reasons mentioned above. From a law enforcement perspective this is the main concern in terms of potential threats to national security - the case against MTN in Nigeria and the subsequent fine issued was a case in point discussed by most respondents.

Implementation Failure

The study confirms that RICA in its current state was implemented incorrectly. As highlighted in the study, from a law enforcement perspective RICA was established to keep pace with criminals who were starting to use more complex and sophisticated tools to conduct crimes, with the need being to help identify and trace individuals that made use of sophisticated technologies, such as cellular phones, to conduct criminal activity. Based on what the study found, technological support in order to make RICA effective was not developed fully. Outdated interception technology makes it very difficult to intercept newer/modern methods of communications rendering RICA applications sometimes futile. Hence the implementation of RICA and the implementation of a strategy to update interception technology continuously had to go hand in hand.

Lack of Awareness Programs

According to law enforcement officials when businesses were approached for selling SIM cards that were not registered or incorrectly registered in line with RICA, their response was that they didn't understand what was required of them or they had interpreted RICA in correctly. This pointed to a lack of awareness, which should have taken place even before the initial implementation phase of RICA.

RICA application process for law enforcement officials

It was found that the RICA application process is a lengthy one and was a concern to law enforcement officials especially in relation to looming threats. Some of the reasons for the lengthy process related to:

- Only one RICA judge (retired) being appointed who was not always available to sign off on RICA applications. This judges' workload is also large due to just one judge dealing with the numerous RICA applications received. It is logical that to conduct their work efficiently the judge will take time to go over the motivations for the RICA application and to make an informed decision whether to approve the application from law enforcement. The data

unanimously indicated that one judge overseeing RICA applications was not enough.

- The RICA application process was confirmed to be a manual process, which according to law enforcement officials took up masses of their time to conclude. On many occasions the law enforcement officials are frustrated by the need for lengthy motivations in order to get permission to get primary ownership information from TSPs. The ownership information furnished from TSPs proved on many occasions to be incorrect, leading to investigations proceeding on the wrong trajectories- leading to a total waste of time. The other issue highlighted is one of standardization, in some instances certain information is required by the RICA judge however in other cases this information is not required for approval, this proves to be a point of frustration for law enforcement officials as there is no standard format available as to what is expected from the judge.

5.2.5 Question Five: **Has RICA been an effective legislative tool to combat crime in South Africa?**

The data suggests strongly that RICA in its current state is not an effective legislative tool to combat crime in South Africa. Law enforcement officials perceive RICA as a very good piece of legislation but in terms of implementation, compliance and enforcement it is inefficient. To expand on these concepts by way of example from the data, the proliferation of pre-RICA'ed SIM cards relates to the incorrect interpretation of RICA, where a seller thought that they could register batches of SIM cards in their own names, hence abiding by RICA-this proved a major implementation failure. To exacerbate the situation there is no mechanisms in place to perform compliance checks especially in the informal trade sphere leading to no enforcement and prosecution hence allowing the process to continue unabated.

5.2.6 Question Six: **What improvements in RICA would law enforcement officials like to see in future?**

As noted above, law enforcement officials view RICA as a good legislation for their needs however implementation is problematic. The following improvements were suggested:

- At the **Implementation** phase, more education, information and knowledge need to be shared in terms of the requirements of RICA and how business should comply.
- **Compliance** to RICA needs to be **enforced** thoroughly by South African TSPs, most especially in curtailing the proliferation of unregistered and pre-RICA'ed SIM cards in South Africa. Punitive measures as directed by RICA need to be enforced not only to TSPs but also to formal and informal traders who are not compliant. There was also a recommendation that the number of SIM cards that can be registered to an individual be limited which could help prevent batch registered pre-RICA'ed SIM cards from operating on South Africa networks, however it was acknowledged that this could be seen as an infringement of the right to freely communicate in South Africa and maybe problematic from a human rights perspective.
- RICA application process needed to be made more user-friendly and should be sped up especially in cases related to "life and death situations" or when it comes to threats to national security.
- Technology needs to be constantly updated in order to help the OIC provide essential information in response to RICA applications. A Cyber strategy (especially in terms of improving interception capabilities) needs to continuously evolve and be implemented in order for RICA to be effective and current.

5.3 Discussion of the Findings

The study found that the areas relating to implementation and compliance are the focal concern raised by law enforcement officials. Goba (2017) indicated that

although (security related) policy implementation has being practiced extensively, successful application and implementation of these policies has sometimes been rare. O'Toole (2004), agreed with Goba further emphasizing that policy implementation has for too long being practiced as a "top-down" (at higher echelons of government) activity away from the actual players that the policy was intended to be used by or assist. RICA is a further example where the actual law enforcement officials who were to utilize the legislation were not actively part of the initial participatory phases. Law enforcement actors that participated at the infancy stage of RICA development were not geared with the knowledge of how RICA would be applied into the investigative trade craft of law enforcement as also eluded to by Goba (2017). The discussion around the findings has been adequately introduced by O'Toole and Goba and will follow suit in line with their thoughts on policy implementation.

The study confirmed that non-compliance to RICA resulted in outdated/inaccurate information being kept and supplied to law enforcement from TSPs. In other instances no details are available on users of SIMS which is also a direct consequence of non-compliance. This resulted in law enforcement officials being frustrated by receiving incorrect or no information on SIMS that were used in perpetrating crimes, fueling their negative perceptions of RICA . This had the effect of some law enforcement officials discarding the use of RICA and using other avenues to get a positive identity to a SIM/cellular number.

It is important to note that RICA as a legislation was commended by law enforcement who did not have any concerns relating to what the legislation intended to do (especially from a law enforcement perspective), reiterating the point that if correctly complied with, RICA would be very effective in law enforcement operations. It is however noted that none of the respondents worked within the legal realm hence were not in the best position to evaluate the legislation from a legal frame of reference. As the study was engineered to gain an understanding of the perceptions of law enforcement officials this was not viewed as a major oversight.

The time frame of the RICA application process was also a concern for law enforcement officials as in its current form the RICA application has no template and

the motivation required and the time it takes a judge to approve a request was listed as concerns especially in relation to impending threats. Interception requests that are approved have a three month validity period, in most cases the approval is received by the law enforcement official with much of the three month period already elapsed, giving the law enforcement official and the OIC very limited time to work on the interceptions.

It also became evident in the study that unregistered SIM cards (especially pre-paid) were also very essential to law enforcement officials in their intelligence gathering operations. These SIMS provided law enforcement with methods of communications without being detected. It was pointed out that had RICA been “bullet proof” then this would not have been an effective tool in the trade craft of law enforcement officials, especially in intelligence gathering operations. Hence the researcher got a sense that RICA needed implementation and compliance attention, however law enforcement relied extensively on unregistered SIM cards in their intelligence gathering operations.

As acknowledged earlier the study has a noteworthy limitation where SAPS did not form part of the study. It would be an injustice if an opinion is not provided on whether the findings would be different had SAPS took part in the study. In the course of reviewing literature for the study the researcher has come across many authors who have highlighted what the deficiencies of RICA are. One of these authors was, then SAPS Minister Fikile Mbalula who recognized that the major deficiencies with RICA was relating to poor implementation and to the act (as also highlighted in this study), his opinion was that the lack of reliable information rendered some investigations unfinished and led to dead ends (Mbalula, 2017). With the issues relating to the implementation and compliance of RICA being one of the findings of this study is for this reason that the researcher is of the opinion that the results would not be significantly different if SAPS participated.

5.4 Recommendations

This study was conducted in order to gain an understanding of the perceptions of law enforcement officials towards RICA as a crime combatting tool. The study examined, (from a purely law enforcement perspective) if RICA was effective, what were some of the challenges experienced and what improvements law enforcement officials wanted in order to make RICA more effective for their line functions. The challenges identified by law enforcement officials' forms the basis on which the following recommendations are made:

RICA Compliance:

- Although the issue relating to who takes responsibility for the inspection and enforcement of compliance to RICA remains contentious, with law enforcement officials adamant that South African TSPs be held accountable, there should be a concerted effort to make sure that SIM cards be correctly registered to individuals whose identities and place of residence have been verified. This alone will help alleviate most frustrations that law enforcement officials experience when applying for RICA information. This would allow the law enforcement official to successfully *"..put a name to a cellular number* ". Hence as a starting point there should be a rigorous effort to make sure that new SIMS are registered correctly, as prescribed by RICA, especially within the informal trade sector. A joint project team from law enforcement, the department of Justice and South African TSPs could be initiated in order to inspect for compliance and to promote awareness programs which could help with the correct implementation and enforcement of RICA.
- Concurrently pressure should be put on South African TSPs not to allow unregistered SIMS cards (both local and international) to access their networks. Fines imposed on TSPs could be used as a deterring factor; however these fines would have to outweigh the potential revenue generated by allowing unregistered SIMS to use TSP networks in South Africa-as was the case in Nigeria.

RICA Application Process:

- More RICA judges or a RICA panel of judges should be appointed in order to assist in making the process more timeous. Retired judges could be a good pool to find appropriate individuals for the task.
- A checklist of requirements for a RICA application needs to be made available to law enforcement officials in order to help standardize and streamline the RICA application process, making the RICA judges' and investigators work in the application process more efficient.
- Automating/computerizing the application process for the law enforcement official (as is the case internationally) would save time and would ensure that threats to national security be dealt with timeously. This will also allow the RICA judge to access applications anywhere and at any time. RICA applications could become "real time" where the approval and dissemination back to law enforcement could be instantaneous. This electronic route could also be used to get the approved RICA application from law enforcement to the OIC allowing for maximum time to intercept communications hence building a reliable picture / profile over time.

Further Study:

- Information relating to the use of RICA for political interference or abuse (as was alluded to in this studies literature review and problem statement), were glaringly lacking. It is the researchers' personal opinion that this was due to an institutional review process being instituted at the SSA, which made the respondents including the researcher uncomfortable in discussing issues pertaining to misuse especially in terms of political interference. A future study using another research approach could be initiated to focus on the misuse of RICA, as the researcher believes not enough information was gathered on this aspect.

5.5 Conclusion

The main intention of this study was identifying and describing the challenges faced by law enforcement relating to the use of RICA in their trade craft and to make a few viable recommendations that will address the identified limitations. The main concern raised by law enforcement was that of unreliable or no information being available on cellular numbers that were used to perpetrate crime. This concern was owing to a failure in terms of implementation, compliance and enforcement of RICA. Although the RICA application process was also highlighted as a challenge by law enforcement, ending the proliferation of unregistered and pre-RICA'ed SIM cards through compliance and enforcement initiatives would help alleviate most of the frustrations experienced by law enforcement officials using RICA in their respective line functions.

LIST OF REFERENCES

Akdeniz, Y., Taylor, N., & Walker, C. (2000). State surveillance in the age of information and rights. *Criminal law Review*, *1*(1), 73-90. Retrieved from http://www.leeds.ac.uk/law/staff/law6cw/clrrip06.pdf

Badenhorst, C. (2007). Research writing: Breaking the barriers. Pretoria, South Africa: Van Schaik Publishers.

Balbi, G. (2009). Telecommunications. *The Handbook of Communication History*, *1*(1). doi:10.4324/9780203149119.ch11

Barrett, M., Morse, J, M, Mayan, M., Olson, K., & Spiers, J. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research. International Journal of Qualitative Methods, 1(2), 13-22. doi:10.1177/160940690200100202

Begum, A. M., Murad, M. H., & Hoque, K. A. (2016). Telecommunication Regulation in Bangladesh: An overview. *IIUC Studies*, *10*(11), 157-172. doi:10.3329/iiucs.v10i0.27433

Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. Medical Education, 40(4), 314-321. doi:10.1111/j.1365-2929.2006.02418.

Bloss, W. (2007). Escalating U.S Police Surveillance after 9/11: an Examination of Causes and Effects. *Surveillance and Society*, *4*(3), 208-228. Retrieved from http://0-web.a.ebscohost.com.innopac.wits.ac.za/ehost/detail/detail?vid=4&sid=8868bf96-3fc3-4129-b296-

2115f9499a3a%40sessionmgr4004&hid=4112&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=61893773&db=sih

Blunn, A. S. (2005). Blunn report of the review of the regulation of access to communications - August 2005 | Attorney-General's Department. Retrieved from https://www.ag.gov.au/Publications/Pages/BlunnreportofthereviewoftheregulationofaccesstocommunicationsAugust2005.aspx

Bricki & Green (2007). Green Chemistry, 9(5), 507. doi:10.1039/b706014a

Bryman, A. (2012). Social Research Methods - 4th Ed. Oxford: OXFORD University Press.

Chien, T. (2007). Technical competency needs assessment for telecommunications professional.*The journal of human resource and and adult learning*, *3*(2), 90-96. Retrieved from http://www.hraljournal.com/Page/11%20Tien-Chen%20Chien.pdf

Cohen, T. (2001). But for the nicety of knocking and requesting a right of entry: Surveillance law and privacy in South Africa. *The Southern African Journal of Information and Communication,* 1(1). Retrieved from http://wiredspace.wits.ac.za/bitstream/handle/10539/19841/SAJIC-Issue-1-2000-Cohen.pdf

Cresswell, M. (2003). Logical Form and Language. Australasian Journal of Philosophy, 81(2), 283-284. doi:10.1080/713659616

Day, G. (2013, March 10). RICA Act - another pointless exercise in stupidity & coercion. Retrieved from http://handshake.co.za/2013/rica-act/

De Vos, P. (2011, June 23). RICA: Is it unconstitutional. *Constitutionally speaking*. Retrieved from http://constitutionallyspeaking.co.za/rica-is-it-unconstitutional

Drake, W. J. (1990). The politics of international telecommunications regulations. *Telecommunications Policy*, *14*(3), 264-266. doi:10.1016/0308-5961(90)90047

Drost, I., & O'Reilly Strata Making Data Work Conference. (2011). Scaling data analysis with Apache Mahout. United States?: O'Reilly Media.

Duncan, J. (2014, November 28). RICA erodes your right to privacy. *Techcentral*. Retrieved from http://www.techcentral.co.za/rica-erodes-your-right-to-privacy/52973

Duncan, J. (2015, February 22). Interception of communications in SA – you should be worried. Retrieved from http://mybroadband.co.za/news/security/119280-interception-of-communications-in-sa-you-should-be-worried.html

Duncan, J. (2017, August 17). Op-Ed: How state spying enables state capture | Daily Maverick. Retrieved from https://webcache.googleusercontent.com/search?q=cache:wgMa4AMQlRAJ:https://www.dailymaverick.co.za/article/2017-08-17-op-ed-how-state-spying-enables-state-capture/+&cd=1&hl=en&ct=clnk&gl=za#.WcoKno-CwdU

Duncan, J. (2018, February 19). What Ramaphosa needs to do to fix state spying, Part One: Rica and lawful interception. Daily Maverick. Retrieved from

https://www.dailymaverick.co.za/article/2018-02-19-op-ed-what-ramaphosa-needs-to-do-to-fix-state-spying-part-one-rica-and-lawful-interception/

Du Plessis, A., & Louw, A. (2005). Crime and Crime Prevention in South Africa: 10 Years After. Canadian Journal of Criminology and Criminal justice, 47(2), 427-446. Retrieved from http://dx.doi.org/10.3138/cjccj.47.2.427

European Council Resolution. (1995). EUR-Lex - 31995Y0812(01) - EN. Retrieved from http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995Y0812(01):EN:HTML

Federal Registrar of Legislation Australia, 2001, *Telecommunications Interception Legislation Amendment Act*, https://www.legislation.gov.au/Details/C2004B01047

Gelman, A., &, Nolan D. (2017). Probability. Oxford Scholarship Online. doi:10.1093/oso/9780198785699.003.0008

Gillwald, A. (2017, April 4). Analyst says SIM card registration in Uganda is ill-advised. Retrieved from http://www.itwebafrica.com/ict-and-governance/400-uganda/237652-analyst-says-sim-card-registration-in-uganda-is-ill-advised

Goba N. (2017, August 23). Law enforcement spying on thousands of phones by bypassing Rica. Retrieved from https://www.businesslive.co.za/bd/national/2017-08-23-law-enforcement-spying-on-thousands-of-phones-by-bypassing-rica/

Guba, E., & Lincoln, Y. (1999). Naturalistic and Rationalistic Enquiry. Issues in Educational Research, 141-149. doi:10.1016/b978-008043349-3/50014-1

Gürkaynak, G., Yilmaz, I., & Taskiran, N. P. (2014). Protecting the communication: Data protection and security measures under telecommunications regulations in the digital age. *Computer Law & Security Review*, *30*(2), 179-189. doi:10.1016/j.clsr.2014.01.010

Hartley, H. (2014, March 25). Loopholes in interception law raise red flag. *Business day Live*. Retrieved from http://www.bdlive.co.za/national/2014/03/25/loopholes-in-interceptions-law-raise-red-flag

Hemeson, C. J. (2012). Directive on Consumer Data for SIM Card Registration in the Telecommunications Sector: An African Perspective. *SSRN Electronic Journal*. doi:10.2139/ssrn.1982033

Hewlett L. (2016, June). Validity and Reliability [Presentation].

Hill, J., & Tiu Wright, L. (2001). A qualitative research agenda for small to medium-sized enterprises. Marketing Intelligence & Planning, 19(6), 432-443. doi:10.1108/eum0000000006111

Holloway, S. (1997). Living Skills Pack II. Physiotherapy, 83(1), 45. doi:10.1016/s0031-9406(05)66116-0

Hosken, G. & Smillie, S. (2015, November 6). TimesLIVE Mobile. Retrieved from http://m.timeslive.co.za/thetimes/?articleId=15819911

Hunter, M. (2014, June 13). *Rica in South Africa: How big is Big Brother? GroundUp*. Retrieved from http://www.groundup.org.za/article/rica-south-africa-how-big-big-brother_1882/

Hutton, L. (2007, November 1). Looking beneath the cloak An analysis of intelligence governance in South Africa. Retrieved from https://www.issafrica.org/01-nov-2007-iss-paper-154-looking-beneath-the-cloak-an-analysis-of-intelligence-governance-in-south-africa-lauren-hutton

Hutton, L. (2007). Oh Big Brother, where art thou? On the Internet, of course…The use of intrusive methods of investigation by state intelligence services. *African Security Review*, *16*(4), 111-116. doi:10.1080/10246029.2007.9627451

Inkster, N. (2010). The Protecting State. *Survival*, *52*(5), 203-209. doi:10.1080/00396338.2010.522106

Joint Standing Committee on Intelligence. (2010). ATC100526: Annual Report of the Joint Standing Committee on Intelligence (JSCI) for the financial year ended 31 March 2010, as agreed by the JSCI on 12 May 2010 and submitted in compliance of section 6 of the Intelligence Services Oversight Act, No 40 of 1994 | PMG. Retrieved from https://pmg.org.za/tabled-committee-report/54/

Joint Standing Committee on Intelligence. (2011-2012). ATC140410: Annual Report of the Joint Standing Committee on Intelligence (JSCI) for the Financial Year ending 31 March 2012, PMG. Retrieved from https://pmg.org.za/policy-document/784/

Joint Standing Committee on Intelligence. (2014). Report of the Joint Standing Committee on Intelligence on activities of the Committee after 5 months of establishment, as stipulated in the Intelligence Services oversight Act, Act 40 of 1994, dated 10 February 2015 | PMG. Retrieved from https://pmg.org.za/tabled-committee-report/2307/

Kisswani, N. M. (2010). Telecommunications (interception and access) and its regulation in Arab countries. *IJLSE*, *4*(1), 44. doi:10.1504/ijlse.2011.041289

Kisswani, N.M. (2011). The reasonable necessary for the implement of telecommunications interception and access laws. *International Lawyer,* 45(3), 857-879. Retrieved from http://www.jstor.org/stable/23824395

Kruger, H. (2009, July 7). RICA implemented in South Africa. Retrieved from http://rwrant.co.za/rica-implemented-in-south-africa/

Lacey, A., & Luff, D. (2001). Qualitative Data Analysis. Retrieved from https://www.rds-yh.nihr.ac.uk/wp-content/uploads/2013/05/9_Qualitative_Data_Analysis_Revision_2009.pdf

Leedy, P. D., & Ormrod, J. E. (2015). Practical research: Planning and design.

Luck, R. (2015, June 11). Walking a fine line between crime prevention and protection of rights.*South African Legal Information Institute*. Retrieved from http://www.saflii.org/za/journals/DEREBUS/2014/6.pdf

Mason, J. (1996). Linking qualitative and quantitative data analysis. Analyzing qualitative data, 89. doi:10.4324/9780203413081_chapter_5

Maxwell, D. (2012). Maxwell. London: Oberon Books.

Mbalula, F. (2017, July 24). The fight against crime in South Africa requires collaboration. Daily Maverick. Retrieved from https://www.dailymaverick.co.za/opinionista/2017-07-24-the-fight-against-crime-in-south-africa-requires-collaboration/

McMillan, M., & Schumacher, R. (1993). Retrieved from https://repository.up.ac.za/bitstream/handle/2263/24285/03chapter3.pdf?sequence=4

Mawson, N. (2015, April 29). You are being spied on. *IT Web*. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=142858

Michalson, L. (2009, July 1). Complying with RICA. Retrieved from http://www.michalsons.co.za/blog/complying-with-rica/1157

Merriam, S. B. (2016). Qualitative research: A guide to design and implementation.

Mirugi-Mukundi, G. (2010, September 9). ISS Africa | Mandatory Registration of SIM Cards - Ingenious Idea or Misplaced Focus on Crime Control? Retrieved from https://www.issafrica.org/iss-today/mandatory-registration-of-sim-cards-ingenious-idea-or-misplaced-focus-on-crime-control

Mukadam, S., & Meyer, T. (2012, May 14). ISS Africa | Intrusive Measures Employed by the SA Intelligence Service are Violating the Right to Privacy. Retrieved from https://www.issafrica.org/iss-today/intrusive-measures-employed-by-the-sa-intelligence-service-are-violating-the-right-to-privacy

Nathan, L. (2009). Lighting up the intelligence community: An agenda for intelligence reform in South Africa. *African Security Review*, *18*(1), 91-104. doi:10.1080/10246029.2009.9627518

Ncube, C. B. (2006). Watching the watcher: recent developments in privacy regulation and cyber-surveillance in South Africa. *SCRIP*, *3*(1), 344-354. doi:10.2966/scrip.030406.344

Newton, H. (2002). *Newton's telecom dictionary: The authoritative resource for telecommunications, networking, the internet and information technology* (2nd ed.). New York: CMP Books.

Nigeria's Buhari says MTN fuelled Boko Haram insurgency - BBC News. (2016, March 8). Retrieved from http://www.bbc.com/news/business-35755298

NTRA. (2017). Retrieved from http://www.tra.gov.eg/en/regulation/frequency-spectrum

O'Toole Jr, L. (2004). The Theory-Practice Issue in Policy Implementation Research. Blackwell.

Pappas, C., & Williams, I. (2011). Grey Literature: Its Emerging Importance. *Journal of Hospital Librarianship*, *11*(3), 228-234. doi:10.1080/15323269.2011.587100

Pater, D. (2006, May 24). Rica Compliance May Take a Toll on Resellers. Business Report. Retrieved from https://www.iol.co.za/business-report/opinion/rica-compliance-may-take-a-toll-on-resellers-733352

Pistorius, T. (2009). Monitoring, interception and Big Boss in the workplace: is the devil in the details? *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*,*12*(1), 01-06. doi:10.4314/pelj.v12i1.43046

Privacy International. (2015, January 9). State of Privacy South Africa. Retrieved from https://privacyinternational.org/state-privacy/1010/state-privacy-south-africa

Republic of South Africa (RSA), 1996, *White Paper on Telecommunications*, Government Printer, Pretoria.

Republic of South Africa (RSA), 1992, *Interception and Monitoring Prohibition Act*, Number 127, Government Printer, Pretoria.

Republic of South Africa (RSA), 1994, *Intelligence Services Oversight Act*, Number 40, Government Printer, Pretoria.

Republic of South Africa (RSA), 1996, *Telecommunications Act*, Number 103, Government Printer, Pretoria.

Republic of South Africa (RSA), 2002, *Regulation of Interception of Communications and Provision of Communication-Related Information Act*, 70, Government Printer, Pretoria.

Republic of South Africa (RSA), 2013, *General Intelligence Laws Amendment Act*, Number 11, Government Printer, Pretoria.

R2K State of the Nation Repport (2014). Retrieved from www.r2k.org.za/2014/09/11/secrecy-report-media-coverage/

R2K Wants Review Of RICA Laws After Journalists' Phones 'tapped'. (2016, May 6). Retrieved from https://www.enca.com/south-africa/the-r2k-calls-review-of-rica-laws-after-alleged-phone-tapping-of-two-journalists

Schmalleger, F. (1996). *Criminology Today: An Integrative Introduction* (9th ed.). Prentice Hall.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. Education for Information, 22(2), 63-75. doi:10.3233/efi-2004-22201

Silverman, D. (2017). Doing qualitative research.

Smillie, S., & HOSKEN, G. (2015, November 6). Crooks Rica havoc. Retrieved from https://www.timeslive.co.za/news/south-africa/2015-11-06-crooks-rica-havoc/

Snail, S. (2009). Cyber Crime in South Africa – Hacking, cracking, and other unlawful online activities. *Journal of Information, Law & Technology (JILT), 2009*(1). Retrieved from http://go.warwick.ac.uk/jilt/2009_1/snail

South African Law Commission Report. (1999). South African law Commission 1999 annual report. Retrieved from http://www.justice.gov.za/salrc/anr/1999_ar.pdf

Swart, H. (2011, October). Secret State: Hoe the government spies on you. *Mail and Guardian*. Retrieved from http://mg.co.za/article/2011-10-14-secret-state

Swart, H. (2016, November 10). Missed Call: Rica registration ‘useless’ for crime prevention purposes. *Daily Maverick*. Retrieved from https://www.dailymaverick.co.za/article/2016-11-10-missed-call-rica-registration-useless-for-crime-prevention-purposes/#.WYxIkbeQobo

Tarrant, H. (2009, November 9). Rica smacks Vodacom too - Moneyweb. Retrieved from http://www.moneyweb.co.za/archive/rica-smacks-vodacom-too

Taylor, N. (2002). State Surveillance and the Right to Privacy. *Surveillance and Society*, *1*(1), 66-85. Retrieved from http://www.surveillance-and-society.org

The Telecommunications Act of 1996: Law & Legislative History. (2001). Pike & Fischer - A BNA Company.

Thornton, L. (2006). *Telecommunications law in South Africa* (1st ed.). Retrieved from https://www.wits.ac.za/media/migration/files/TeleLawfull.pdf

Traders warned against breaking RICA laws | SA News. (2011, July 6). Retrieved from http://www.sanews.gov.za/south-africa/traders-warned-against-breaking-rica-laws

Tripp, G. (2001). Interception of Communications. *Information & Communications Technology Law*, *10*(3), 285-292. doi:10.1080/13600830120081881

United Kingdom. (2000). *Regulation of Investigatory Powers Act.* Retrieved from https://www.legislation.gov.uk/ukpga/2000/23

United States. (20016). *National Security Strategy*. Retrieved from http://www.state.gov/documents/organization/64884.pdf

United States. (2001). *The USA PATRIOT Act*. Washington, D.C.: U.S. Dept. of Justice. Retrieved from https://www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf

Watney, M. (2012). EVALUATION OF CYBERCRIME REGULATION IN SOUTH AFRICA [power point].

Watney, M. (2015). State-on-nationals' electronic communication surveillance in South Africa: A murky legal landscape to navigate? *2015 Information Security for South Africa (ISSA)*, *1*(01), 42-54. doi:10.1109/issa.2015.7335047

ANNEXURES

1. Interview Guide/ Schedule used

The following unstructured interview schedule was administered face to face to law enforcement officials that were purposefully sampled (based on their knowledge and use of RICA).

SECTION 1: General Questions

1. General Description of occupation and duties currently performed by respondent? Experience ?
2. How long have you had experience with using RICA?

SECTION 2: Knowledge of RICA in general

1. Are you aware of why RICA was required in RSA? (From a law enforcement point of view or general knowledge?) Explain…
2. How do you utilize RICA in your line function? Explain in terms of tradecraft/methodology.
3. In your experience: Are there any benefits / advantages you have experienced in relation to the use of RICA as crime combatting tool? Please explain them…
4. In your experience: Are there any Disadvantages / limitations you have experienced in relation to the use of RICA as crime combatting tool? Please explain them…
5. In your view /perception has RICA been an effective tool for you to be able to combat criminal activity in RSA? Explain …
6. In your own view how would you improve RICA in order for it to be more effective, if you had the chance?