REPORT ON INTERCEPTION

OF

PRIVATE COMMUNICATIONS

PERIOD 2013/2014

JUSTICE YVONNE MOKGORO

Joint Standing Committee on Intelligence: Parliament

STRUCTURE

1. INTRODUCTION

2. INTERCEPTION

3. INTERNATIONAL LAW

4. SOUTH AFRICAN LEGISLATIVE FRAMEWORK

4.1 PROHIBITION OF INTERCEPTION OF COMMUNICATION

4.2 INTERCEPTION IN CASE OF EMERGENCY

4.3 APPLICATION FOR ISSUING OF DIRECTIVES AND ENTRY WARRANTS

5. RECORD - KEEPING BY HEADS OF INTERCEPTIONS

6. SUPPLEMENTARY DIRECTIVES REGARDING APPLICATIONS

7. THE ACT vs CONSTITUTONAL RIGHTS TO PRIVACY, HUMAN DIGNITY AND FREEDOM

8. CHALLENGES

9. RICA AND THE FUTURE

10. FULL STATISTICAL INFORMATION OF APPLICATIONS

10.1 THE SOUTH AFRICAN NATIONAL INTELLIGENCE AGENCY

10.2 THE SOUTH AFRICAN POLICE SERVICES

10.3 THE SOUTH AFRICAN NATIONAL DEFENCE FORCE

11. ADMINISTRATION: OFFICE FOR INTERCEPTION

11.1 STAFFING

11.2 OFFICE INFRASTRUCTURE

11.3 CONCLUSION

1. INTRODUCTION

The 2013/2014 South African Police Statistical Report has revealed that, approximately 2.1 million violent crimes were registered in the last financial year. Although this figure shows a decline in comparison with the previous financial year, the number remains high.

The escalating rate of organised crime and crimes where electronic technology is used have also increased significantly and are becoming more and more sophisticated. The latter situations pose severe challenges to law enforcement agencies to fulfil their role duties optimally efficiently and to protect society effectively. Perpetrators of crime utilize electronic technology abundantly, successfully and with ease.

The electronic methods are frequently utilised in the planning and perpetration of serious crimes ranging from:

- Human trafficking;
- Drug dealing and drug trafficking;
- Money laundering;
- Corruption and fraud;
- Kidnappings;
- Assassinations;
- Terrorism;
- Cash in transit heists;
- Rhino –poaching; etc

This state of affairs, together with the escalating rate of organised and technological crime and highly sophisticated criminal methods have made interception a lawful and popular method of investigation, not only in the Republic of South Africa but in most countries worldwide. Interception of private communications is generally considered a "necessary evil" to protect law abiding people from the criminal conduct of others.

In the South African context, an interception of this nature has the potential for unconstitutionality, bringing the State into much disrepute. For this reason, interception is an investigative method of last resort and not there for the taking.

2. INTERCEPTION

Lawful interception nonetheless plays a crucial role in advancing the investigative process. It represents an indispensable means of gathering criminal and other intelligence. [1] The Regulation of Interception of Communications and Communication-related Information Act, 2002 (Act 70 of 2002), (the "RICA"), was designed to allow the State to intercept communications and provide communication-related information during the investigation of serious crimes. This process becomes legal and the information gathered becomes admissible in court, if performed in accordance with the RICA.[2]

The RICA provides guidance and requires strict compliance with the procedure when applying for an interception directive from the designated judge.[3] When doing so, the RICA requires thorough consideration and appreciation of at least

[1] Notes on OECS Interception of Communications' Bill, page 6 found at: http://unpan1.un.org/inradoc/groups/public/documents/TASF/UNPAN024636.pdf

[2] S v Naidoo and Another 1998 (1) SACR 479 (N)-It was argued that the tape recordings were made in contravention of IM Act of 1992 and thus be declared inadmissible.

[3] Regulations of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 RICA is the successor to the Interception and Monitoring Act 127 of 1992.

Sections 10 and 14 of the Constitution, which relate to the protection of the right to privacy and human dignity respectively.

Most importantly, an application for interception must not be lightly taken as it has the potential of making severe inroads into the above rights of the targets. Besides, a directive for interception is not there for the taking. It is obtained only under the strict conditions of the Constitution and the provisions of the relevant legislation, including the RICA.

3. INTERNATIONAL LAW

The detection and investigation of crimes committed through the use of electronic technology has been a global challenge for years. Thus the use of interception devises was approved by the Council of Europe Convention, to which South Africa is a signatory. Almost all countries in the world, for example, the United Kingdom (Regulation of Investigatory Powers Act, 2000), the United States of America (inter alia, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 as amended), Australia (Telecommunications (Interception) Act 1979), New Zeeland (Crimes Act and Misuse of Drugs Act), various countries in Europe, Zimbabwe, Namibia, Uganda, Kenya, Rwanda, Tanzania and Ethiopia have adopted legislation to regulate the lawful interception of private communications in order to combat criminal activities. In general the interception and monitoring of communications in all these countries create a balance between the subject's right to privacy and the need to detect and investigate crime for the protection of society. The Interception of communications in these countries, like in South Africa, is only permitted if it is judicially sanctioned or approved by an independent higher authority and in terms of relevant law.

4. SOUTH AFRICAN LEGISLATIVE FRAMEWORK

To deal with the question of finding better mechanisms in addressing this global challenge of the use of technology in criminal activity, the South African Law Reform Commission (SALRC) felt it important to undertake a review of the efficacy of the then Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992). The investigation had shown that the Interception and Monitoring Prohibition Act was outdated in that it did not adequately provide for new developments in the field of electronic technology and the use thereof in the commission of crimes.

As a result of the recommendations of the SALRC, the Interception and Monitoring Prohibition Act, of 1992 was replaced by the RICA. The aims of the RICA , among others, are:

(a) provide for applications for lawful interception; (Section 4)

(b) provide for a structure which is responsible for the interception of communications; (Section 32)

(c) provide for the interception of communications in emergency situations; (Section 8)

(d) protect people in the Republic against the unlawful interception of communications; (Section 2)

(e) oblige all electronic communications service providers (ECSPS) to provide a service which is interceptable and which is able to store communication related information; (Section 30)

(f) oblige ECSPS to record and store information which can be used to identify

their customers; (Section 37)

(g) prohibit the possession and manufacturing of interception devises; (Section 45)

(h) provide that the interception of communications must, unless the RICA provides otherwise, be approved by a judge. (Section (1)(1)

Some of these aspects are dealt with in more detail below:

Creation of the Office of the Designated Judge:

The Designated Judge is appointed in terms of Section 1 of RICA, and he/she functions under the Department of Justice and Correctional Services. The Judge must ensure that all applications for interception are in strict compliance with the RICA and are constitutionally justified.

Role and Functions

In terms of Section 2 of RICA, it provides that no person may intentionally monitor any conversation or communication by means of a monitoring device so as to gather confidential information concerning any persons, body or organisation.

The Regulation of Interception of Communications and Provision of Communication-related Information Act of 200 (Rica), which came into effect in 2005, makes it illegal for any authority to intercept communication without the permission of a judge designated to rule specifically on all interception applications in South Africa.

4.1 Prohibition of interception of communication

The Regulations on Interception of Communications prohibit any person to intentionally intercept or attempt to intercept, or otherwise procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission unless it is done in terms of the provisions of the RICA.[4]

4.2 Criminal Procedure Act

Another way of accessing information related to communication is provided for in section 205 of the Criminal Procedures Act 51 of 1977, which allows a law enforcement agency to apply to a high court judge, a regional court magistrate or a magistrate to grant access to cellphone records, telephone records or information about billing and ownership of a cellphone.

It also provides for a person's whereabouts to be tracked through his or her cellphone. This information has to be provided by a telecommunications service provider, which cannot legally release such privileged customer information without being ordered to do so under section 205.

[4] Section 2

4.3 Interception in Cases of Emergency

In the case of an emergency, where there are reasonable grounds to believe that a person's life is imminently being endangered, the applicant can make an oral request to intercept any communication to or from the sender in any manner which the telecommunication makes appropriate. The applicant may also request a directive as may be necessary to determine the location of such a person (Sections 7 and 8 of the RICA respectively).[5]

The information obtained as well as affidavits from law enforcement officers who requested the information must be submitted to the designated judge for scrutiny within 48 hours.

4.4 Application for issuing of directions and entry warrants

Under the RICA, a designated judge may justifiably authorise –

(a) the interception of direct or indirect communications by way of an interception direction in terms of Section 16 of the RICA; e.g. (getting permission to intercept or tap someone's communication);

(b) the interception of real-time communication-related information on an ongoing basis by means of a direction in terms of Section 17 of the RICA; e.g. (getting permission to access any mode of telecommunication);

(c) the combined interception of direct or indirect communications, real-time communication-related and the provision of archived communication-

[5] Section 8(1)(b) and (aa)

related information by means of a direction in terms of Section 18 of the RICA; e.g. (getting hold of stored information of a person like a hard copy);

(d) the decryption of intercepted information by means of a decryption direction in terms of section Section 21 of RICA; e.g. (getting permission for the descriptive keyholder to disclose a disclose a descriptive key/password);

(d) entry warrants for the purposes of entering the premises of a target for the placing of interception devices in terms of Section 22 of the RICA; e.g (placing devices into the private home or places of employment of the targets).

The above-mentioned directions or entry warrant can only be granted after the law enforcement agency make a formal application to the designated judge. In considering such an application, the RICA imposes various conditions that must be considered by the designated judge before he or she may grant a direction or entry warrant.

The application for a direction should clearly indicate, *inter alia,* the identity of the applicant, the identity of the law enforcement officer, the identity of the target including the references or the telephone, all phone (number) and address of premises where relevant, communication is required to be intercepted and the telecommunication service provider to whom the direction must be addressed.[6]

To invoke the implementation of section 36 of the Constitution, the Act further requires an applicant, to include in the application, the basis for believing that evidence relating to the ground on which the application is made ***will*** be obtained

[6] Section 16

through the interception applied for.[7] Furthermore, the application must indicate, where applicable, whether other conventional investigative procedures have been applied and had failed to produce the required evidence. The applicant must also indicate why other investigative measures and or approaches are unlikely to succeed or appear to be too risky.[8] In order words, each application must be duly justified.

An interception direction may be granted if the designated judge is satisfied that:

- A serious offence has been or is being or will be committed or the health or safety of the public is threatened etc;
- the interception will provide information regarding the offence or threat;
- the facilities from which the communications will be intercepted are usually used by the person; and
- other conventional investigative methods had been unsuccessful and ineffective and are too risky.

5. KEEPING OF RECORDS BY HEADS OF INTERCEPTION

The head of an interception centre must on a quarterly basis submit a written report to the designated judge of the records kept, abuses in connection with the execution of directions and any defect in any electronic communications system which has been discovered.[9]

There is therefore an obligation to monitor and ensure full compliance with the RICA.

---

[7] Section 16(2)(d)(ii)
[8] Section 16(2)(e)
[9] Section 37(1)(2)(a)(i-iii)

6. SUPPLEMENTARY DIRECTIVES REGARDING APPLICATIONS

A designated judge or designated judges, jointly, after consultation with the respective Judges-President of the High Courts, may issue "directions" to supplement the application procedures for the issuing of directions or entry warrants. The "directions" issued must be submitted to parliament.[10]

7. THE ACT *vs* THE CONSTITUTIONAL RIGHT TO PRIVACY AND HUMAN DIGNITY

Section 14 of our Constitution protects everyone's right to privacy, which includes the right not to have "the privacy of their communications infringed".[11] Privacy is a fundamental human right recognised internationally in instruments like the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights, and regionally in the African Charter on Peoples' Rights, etc. It underpins human dignity and other key values such as freedom of association and freedom of speech and expression.[12] These values are fundamental to sustain functional democracies and the rule of law.

Article 8 of the Convention on Human Rights explicitly states that, "there shall be no interference by a public authority with the exercise of the right to privacy except in accordance with the law and to the extent that it is necessary in a democratic society and in the interests of national security, public safety or the economic well-being of the country. The right to privacy in this regard may also be limited in preventing disorder or crime, for the protection of health, or the rights and freedom of others".

---

[10] Section 58(1) and (3)
[11] The Constitution of the Republic of South Africa, 1996
[12] Privacy and Human Rights-An International Survey and Privacy Laws-http://gilc.org/privacy/survey/intro.html

The Article makes it clear that the information collected by enforcement agencies, must only relate to that which is identified by the warrant issued, such that, only persons or people who are suspected of committing serious offences or participating in activities against the interests of national security, may lose their right to privacy.[13]

LIMITATION OF RIGHTS

In our Constitution, no right is absolute. All rights, including the right to privacy, human dignity and freedom may be limited, This limitation may however take place only in terms of a law of general application, to the extent that the limitation is reasonable and justifiable in an open and democratic society, based on human dignity, equality and freedom, taking into account all relevant factors.[14]

Indeed, "the shift in balance towards absolute individual privacy is in itself a threat to security and the consequence of this choice will [in the context of high [crime rates] affect our personal safety, our right to live in a society where lawlessness is not tolerated and the ability of law enforcement to prevent serious and other violent criminal activity"[15][is frustrated]

In the matter of *The Investigating Directorate and Others v Hyundai Motor Distributions,* Justice Langa DP held that

"It is a notorious fact that the rate of crime in South Africa is unacceptably high. There are frequent reports of violent crime and incessant disclosures of fraudulent activity. This has a serious effect not only on the security of citizens and morale of the community but also

[13] European Convention on Human Rights for the Protection of Human Rights and Fundamental Freedom- www.hrcr.org/docs/Eur convention/euroconv3.html
[14] The Constitution of the Republic of South, section 36(1) 1996-Limitation Clause
[15] Lawful interception-Andres Rojab-centre for advanced Internet Architectures Swinburne University of Technology- Feb 9 2006- http://caia.swin.edu.au

on the country's economy. This ultimately affects the government's ability to address the pressing social welfare problems in South Africa. The need to fight crime is thus an important objective in our society..."[16], *and then,*

in *Califonia v Ciraolo* the court held,

> *"The right to privacy is not meant to shield criminal activities or to conceal evidence of crime from the criminal justice process, however, state officials are not entitled without good cause to invade the premises of persons for purposes of searching and seizing property..."*[17]

It is thus recognised that the interception of private communications is most invasive, but may be necessary for the protection of the public. Each case however, must be justified in terms of the law.

8. CHALLENGES

There is a general public perception that some law enforcement agencies and other institutions use these intrusive methods to advance their own interests with no regard to the rights and values in the Constitution. The media, in particular the social networks, are riddled with, allegations, and perceptions or comments of manipulation and abuse of the interception system by officials and even private individuals, ranging from-

- obtaining private information without the knowledge of the Designated Judge; (Section 204/205 of the CPA?)

[16] The Investigating Directorate and Others v Hyundai Motor Distributions (PTY) (LTD) 2001 (1) SA 545 (CC)
[17] California v Ciraolo 476 US 207 (1985) at 213-4

- acquisition of cell phone billing and ownership records through crime intelligence, without the Judge's knowledge or approval, in order to expedite their investigations; (Section 204/205 of CPA?)
- obtaining text messages and cell phone billing records needed for personal reasons, through "State contacts";

- the popularity of interception methods which are preferred over conventional method;
- the apparent lack of trust of the Designated Judge with regard to information gathered through crime intelligence;
- failure of applicants to provide fact-based justification for an application to the Judge;
- applicant's need to comprehend that suspicion of crime without any factual basis is not sufficient for interception applications;
- the tendency for vagueness of basis for an application, the cut and paste approach to an affidavit and the tendency to regard the authorisation for interception as a given; and
- wide allegations of bribery of contacts at banks and telecommunications service providers;[18] etc

Not all of these challenges may be resolved through legislative amendments. Some may only be resolved through the legislative compliance, dedication, commitment, full understanding and appreciation of the role of investigation officers in the gathering of crime and security intelligence in a democratic society based on the values of human dignity, freedom and equality. The need to sharpen and constantly improve the investigative skills and prowess of our law

[18] How the government spies on you-Mail and Guardian Online-http://mg.co.za/articles/2011-10-14

enforcement agencies comes to mind. No doubt, those are important aspects of contemporary policing and intelligence gathering.

The need for law enforcement and security agencies to be continuously conscience of the precepts and values of our Constitution and to protect the integrity of the interception system is critical to sustain our democratic ideals.

9. RICA AND THE FUTURE

The RICA was assented to on 30 December 2002 and came into operation on 30 September 2005. From 2002 to date, there have been substantial developments that took place in the electronic communications field. The Electronic Communications Act, 2005 (Act 36 of 2005), introduced a new electronic communications dispensation in South Africa, moving away from the dispensation envisaged in the RICA, where, based on the Telecommunications Act, 1996 (Act No. 103 of 1996) there is a clear, distinction based on fixed line, internet and mobile cellular communications. The RICA should be revamped to bring the terminology in line with the current electronic communications dispensation as is envisaged in the Electronic Communications Act, 2005.

New services are seeing the light, inter alia, Black Berry Messenger Services, BlackBerry Enterprise Services, Skype and a host of other electronic communications services, which is mostly Internet based, and is clearly not interceptable. And even if they were interceptable, the encryption that is applied to such services makes it nearly impossible for the law enforcement agencies to obtain any information about the content of a communication. This aspect should be further investigated in order to find a solution.

The RICA may need to be revised in light of the obligations which the country may incur if we accede to the African Union Convention on the establishment of a credible legal framework for cyber security in Africa, in order to deal with cybercrime.

The RICA should in so far as possible and regularly be revised in order to ensure that it keeps pace with developments. There is reliable information that an electronic process for the application of directions was previously discussed in this Committee. The then Department of Justice and Constitutional Development, who is the State Department responsible for the administration of the RICA, will be approached in due course to consider proposals.

10. STATISTICAL INFORMATION OF APPLICATIONS FOR DIRECTIONS

AGENCIES

10.1 State Security Agency (SSA)

Figures for the period are as follows:

- Applications (New) 28
- Re-applications 34
- Amendments 38
- Extensions 35
- Amendments and Extensions 13
- Entry Warrants 5
- Section (11) 66

- Oral interceptions 2
- Refused 5 (No RICA confirmation)
- **Total** **226**

10.2 THE SOUTH AFRICAN POLICE SERVICES (SAPS)

- Entry Warrant 1
- Applications (New) 158
- Re-applications 23
- Amendments 10
- Extensions 6
- Amendments and Extensions 22

Total **220**

10.3 THE SOUTH AFRICAN SECRET SERVICE(SASS)

- Applications (New) 2

Total **2**

10.4 FINANCIAL INTELLIGENCE CENTRE(FIC)

- Applications (New) 3

Total **3**

10.5 SOUTH AFRICAN NATIONAL DEFENCE FORCE(SANDF)

- Applications (New) 3
- Amendments 1

Total	**4**

Combined figures for NIA, SAPS, SASS, FIC and SANDF are as follow:

• Applications (New)	194
• Re-applications	56
• Amendments	49
• Extensions	41
• Amendments and Extensions	35
• Entry Warrants	5
• Section(11)	66
• Oral intercepts	2
• Refused	5
• **Total**	**453**

11. ADMINISTRATION

The Office for the Control of Interception and Monitoring of Communications, processes applications submitted to the designated Judge in terms of the provisions of the Regulation of Interception of Communications and Communication-related Information Act,2002(Act 70 of 2002) (the RICA).

11.1 Staffing.

The staff component comprises of six officials namely Assistant. Director, Legal Administration Officer, Administration Officer, Chief

Administration Clerk, Receptionist and Registry Clerk. Their responsibilities in brief are as follows.

Office Manager (Ass. Director)

Planning and organizing activities of the component. Provide leadership pertaining to financial and administrative Services. Manage processing of applications. Liaising with all stakeholders in Law enforcement. Co-ordinating activities of all law enforcement agencies. Duties also include staff management, asset management, compilation of statistics, ensure high level of confidentiality in the office and provides overall executive support to the office of the designated Judge.

Legal Administration Officer

Provides Legal support to the designated Judge. She is responsible for all the research required by the designated Judge to facilitate the role and functions of the designated Judge, including compilation of information for public presentations, seminars, workshops and conferences.

Administration Officer

Render secretarial and administrative duties to the Judge, provides administrative support for the office as a whole, processes all

payments and assists with efficient management of stores and assists clients daily.

Chief Registry Clerk

Supervision of Registry personnel ensures proper handling of records, ensures proper execution of track and trace list and also ensures that documents are delivered to National Office and Office for Interception Centres.

Receptionist

Performs receptionist functions, performs clerical duties, supports the Judge and other staff members, filing and updating all records.

Registry clerk

Opening, closing and disposing of files according to National Archival Instructions, ensures correct placing of records, maintains proper track and trace lists daily, re-filing daily and related miscellaneous tasks.

Budget

The Office of the Designated Judge does not have its own budget. It is a component of PAIA & Records Management Directorate at National Office. All requisitions are therefore subject to approval by the Director

(PAIA & Records Management) who prioritises and allocates resources based on needs as she deems fit.

Office Infrastructure

Furniture

The Office is in dire need of new office furniture, filing system, new telephone system, official cell phones for Chief Registry Clerk and Administration Officer. A request was made for the purchase of office furniture on the 25/07/2013. The request was forwarded to the Director (PAIA & Interception). In it was approved by the then Acting Deputy Director-General (Corporate Services) on the 01/08/2013.The office was later advised that there is no funding for furniture.

Official cell phones

A request was made for official cellular phones for Chief Registry Clerk and Administration Officer. It was forwarded to the designated official on the 30 July 2013. The office is still awaiting a response in this regard.

Why the need for cell phones?

The office deals with application on a 24hrs basis. The Chief registry Clerk transports the applications daily to the Judge. It is therefore

necessary to be reachable and be able to make contacts by telephone at all times.

Mobile Filing System

Why Mobile Filling System?

The office handles top secret documents which must be stored for a minimum period of 5 years. In order to comply with the Archival Act, storage is a challenge. A mobile filling system will address this difficulty.

A request to purchase mobile filing system was forwarded to the Director on the 30 July 2013. We are still waiting for a response.

12. Conclusion

Indeed, that the system of lawful interception of private communications may be open to abuse is a possibility that we should not be blind to. However, the monitoring systems are well-functioning, ever conscious of the need for utmost vigilance.

As a matter of fact, for the past three years, the approach of the designated judge has been one of capacity-building among others:

- Two annual workshops on understanding the interceptions application process and its challenges, in the context of the

constitutional provisions and values have been conducted by the designated judge-for the benefit of all sectors and role players in the interception process.

- Individual attention is provided giving specific comments on the shortcomings of each application and continuously conscientising applicants of the importance of the realisation that interception directions are not there for the taking and shall be justified by facts which point to the commission of a crime or a crime in process and
- The need to be ever conscious that interception is not an investigative method of first resort. It is employed only once conventional methods have been shown in the application to have been ineffective and or impossible, due to the particular circumstances of the specific criminal activity.

This capacity-building method has been generally welcomed and the response to the instillation of the above values has borne positive results, e.g mere suspicion is generally no longer viewed as basis for an interception application.