ANNUAL REPORT ON INTERCEPTION

OF

PRIVATE COMMUNICATIONS

PERIOD 2014/2015

By JUSTICE YVONNE MOKGORO

Designated Judge

To : Joint Standing Committee on Intelligence: Parliament

Date: 15 October 2015

STRUCTURE

1. INTRODUCTION

The need for good quality and timely intelligence to counter crime and security threats cannot be exaggerated. For that reason, good quality must include reliability of the intelligence gathered. Although the interception of electronic communications has for a number of obvious reasons become a preferred method of gathering crime intelligence, it is critical to be cognisant of the constitutional limitations of an intelligence method of interception as a first-even in the face of highly organised criminal syndicates.

The idea is to continuously strike the fine balance between ensuring legal compliance without frustrating effective intelligence method. This test is that of justification, finding good cause, based on the facts of the particular case as required in Section 16(2)(a) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), Act 70 of 2002.

Further, the escalation of cyber-crime and its increasing sophistication continue to pose grave challenges to law enforcement agencies fulfilling their duties optimally and most efficiently. Crime syndicates in particular, utilize these technologies successfully and with ease, planning and perpetrating serious crimes like:

- Human trafficking;
- drug dealing and drug trafficking;
- money laundering;
- corruption and fraud;
- kidnappings;
- assassinations;
- terrorism;
- heists; etc

This state of affairs, together with the escalating rate of technological crime and highly sophisticated criminal methods has made interception a popular method of investigation not only in South Africa but in almost every country in the world. Thus, the world over, interception of communications relative to the right to privacy and human dignity, is generally considered a necessary evil to protect law abiding citizens from criminal conduct.

2. INTERCEPTION

Lawful interception plays a crucial role in advancing intelligence as part of gathering the investigative method. It represents an indispensable means of gathering criminal intelligence. [1] The Regulation of Interception of Communications and Communication-related Information Act, 2002 (Act 70 of 2002), ("RICA"), was designed

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

to allow the State to intercept communications and provide communication-related information during the investigation of serious crimes. The process must, however be legal in that it must be authorised by the designated judge.

The RICA provides the necessary guidance and requires strict compliance with the procedure that should be undertaken when applying for an interception direction from the designated judge.[2] When doing so, the RICA demands thorough appreciation and application of section 14 of the Constitution, which relates to the right to Privacy.

For that reason, the application for an interception direction must be considered as a last resort, as the RICA seeks to guard against its abuse and the violation of constitutionally protected rights.

3. INTERNATIONAL LAW

To detect and investigate crimes that are committed through the use of electronic technology has been a global challenge for years. This resulted in the approval of the use of interception devises by the Council of Europe Convention, to which South Africa is a signatory. Almost all countries in the world, for example, the United Kingdom

[2] 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.

(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 etc, have adopted legislation to regulate the lawfully intercepted communications in order to combat criminal activities. In general the interception and monitoring of communications in all these countries balance the subject's right to privacy with that of the need to investigate and detect crime. Interception of communications in these countries is only allowed if it is judicially sanctioned or approved by an independent higher authority.

4. SOUTH AFRICAN LEGISLATIVE FRAMEWORK

To deal with the question of finding better mechanisms in addressing this challenge, the South African Law Reform Commission (SALRC) felt it was important to undertake a review of the effectiveness 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 deal with 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, was replaced by the RICA. The aims of the RICA are, inter alia, to:

(a) Protect subjects of the Republic against the unlawful interception of communications;
(b) oblige all electronic communications service providers (ECSPS) to provide a service which is interceptable and which is able to store communication related information;
(c) provide for a structure which is responsible for the lawful interception of communications;
(d) oblige ECSPS to record and store information which can be used to identify their customers;
(e) prohibit the possession and manufacturing of interception devises;
(f) provide for the lawful interception of communications in emergency situations;
(g) provide that the interception of communications must, unless the RICA provides otherwise, be approved by a designated judge.

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

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.[3]

4.2 Interception in cases of emergency

In a case of an emergency, where there are reasonable grounds to believe that an emergency exists by reason of the fact that the life of another person is being endangered, the applicant can orally request the ECSP concerned to intercept any communication to or from the sender in any other manner which the telecommunication deems appropriate or provide such assistance as may be necessary to determine the location of such a person (sections 7 and 8 of the RICA).[4]

These processes are however subject to judicial scrutiny in that the information obtained as well as affidavits from the ECSPS and law enforcement officers who requested the information must be submitted to the designated judge for scrutiny.

4.3 Application for issuing of directions and entry warrants

Under the RICA, a designated judge may authorise –

---

[3] Section 2
[4] Section 8(1)(b) and (aa)

(a) the interception of direct or indirect communications by way of an interception direction in terms of section 16 of the RICA;(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;

(b) the combined interception of of direct or indirect communications, real-time communication-related and provision of archived communication-related information by means of a direction in terms of section 18 of RICA;

(c) the decryption of intercepted information by means of a decryption direction in terms of section section 21 of RICA; and

(d) entry warrants for the purposes of entering a premises for the placing of interception devices in terms of section 22 of RICA.

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

With regard to an interception direction, the Act compels any person who is authorised to intercept communication, to complete an application and submit it to the designated judge for consideration. The application should clearly indicate, *inter alia,* the identity of the

applicant, the identity of the law enforcement officer, the person whose communication is required and the telecommunication service provider to whom the direction must be addressed.[5]

To invoke the application of section 36 of the Constitution, the Act further requires the applicant, in his or her application, to include the basis for believing that evidence relating to the ground on which the application is made will be obtained through the interception applied for.[6] Furthermore, the application must indicate, where applicable, whether other investigative procedures have been applied and failed to produce the required evidence and why other investigative means are unlikely to succeed or appear to be too dangerous.[7]

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 public health or safety 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

[5] Section 16
[6] Section 16(2)(d)(ii)
[7] Section 16(2)(e)

- other investigative methods had been unsuccessful or too dangerous.

5. KEEPING OF RECORDS BY HEADS OF INTERCEPTION

The head of an interception centre (i.e The OIC) must on a quarterly basis submit to the State Security Agency (SSA) a written report of the records kept, abuses in connection with execution of directions and any defect in any electronic communications system which has been discovered.[8]

This obligation is there to ensure that there is full compliance with the RICA at all times.

6. SUPPLEMENTARY DIRECTIONS REGARDING APPLICATIONS

A designated judge or designated judges, jointly, after consultation with the respective Judges-President of the High Courts, may issue directives to supplement the procedure for making applications for the issuing of directions or entry warrants and the directive issued must be submitted to parliament.[9] During the period of this report, no

[8] Section 37(1)(2)(a)(i-iii)
[9] Section 58(1) and (3)

supplementary directions have been found necessary. Therefore, none has been issued.

7. THE ACT *vs* THE RIGHT TO PRIVACY

Section 14 of the Constitution protects everyone's right to privacy, which includes the right not to have "the privacy of their communications infringed".[10] Furthermore, 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.[11]

Article 8 of the Convention on Human Rights explicitly states that, "there shall be no interference by a public authority with the exercise of this right 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] The Constitution of the Republic of South Africa, 1996

[11] 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 forfeit their right to privacy.[12]

In our Constitution, no right is absolute. All rights, including the right to privacy are limited, but 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.[13]

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 the state of crime rates in South Africa] 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".[14]

---

[12] European Convention on Human Rights for the Protection of Human Rights and Fundamental Freedom-www.hrcr.org/docs/Eur convention/euroconv3.html

[13] The Constitution of the Republic of South, section 36(1) 1996-Limitation Clause

[14] Lawful interception-Andres Rojab-centre for advanced Internet Architectures Swinburne University of Technology-Feb 9 2006- http://caia.swin.edu.au

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 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..."*[15], *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..."*[16]

8. CHALLENGES

There is a continued general public perception that some law enforcement and other institutions and/or officers use these intrusive interception methods to advance their own interests with no regard to the rights and values the RICA aims to protect in the context of the Constitution. The media, in particular the social networks, are

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

inundated with reports, allegations and comments of manipulation and abuse of the interception system by officials and even individuals, ranging from-

- obtaining of information in less than 36 hours, without the Designated Judge's knowledge;
- acquisition of cell phone billing and ownership records through crime intelligence, without the Judge's knowledge or approval, in order to expedite the investigation;
- obtaining text messages and cell phone billing records needed for personal reasons, through a contact at crime intelligence and/or the service providers;
- the popularity of interception method which is preferred over conventional methods of investigation;
- 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 application for interception;

- 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 therefore the taking and
- wide allegations of bribery of contacts at banks and telecommunications service providers etc.[17]

Not all of these challenges may be resolved through legislative amendments. Some may only be resolved through the dedication, commitment, full understanding and appreciation of the important role of investigation officers gathering crime 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 enforcement officers comes to mind - no doubt an important aspect of contemporary policing.

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

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

in South Africa, moving away from the dispensation envisaged in the RICA, where there is a clear, distinction based on a fixed line, internet and mobile cellular communications based on the Telecommunications Act, 1996 (Act No. 103 of 1996). The RICA should therefore 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 services, which is mostly Internet based, which is clearly not interceptable, and even if it were interceptable, the encryption that is applied to such services makes it nearly impossible for the law enforcement agencies to obtain any information on the content of a communication. This aspect must be further investigated in order to find a solution.

The RICA needs to be revised in light of the obligations which the Republic 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 if possible regularly be revised in order to ensure that it keeps pace with ongoing developments.

9.1 Amendments to the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act 70 of 2002) (the RICA)

The Department of Justice and Constitutional Development has indicated that legislation which affects various amendments to the RICA is on the legislative program of the Department for the 2016/2017 financial year. Amendments which are considered are, among others, amendments which are aimed at –

(a) facilitating an electronic process for applications for directions and service of directions contemplated in Chapter 3 of the RICA;

(b) ensuring the integrity of the process of obtaining customer information;

(c) further regulating listed equipment provided for in sections 44, 45 and 46 of the RICA;

(d) complimenting information sharing between electronic communications service providers and Government agencies;

(e) further providing for interception capabilities of law enforcement agencies;

(f) imposing obligations on electronic communications service providers who provide an internet service to record and store call related information; and

(g) appoint a regulatory body to ensure compliance with the RICA by the electronic communications service providers.

The terminology used in the RICA will also be reviewed to address interpretation problems which are being experienced.

A specific problem was identified which relates to the RICA registration process, provided for in section 40, where the particulars of customers were incorrectly captured. According to available information, certain persons RICAed various SIM-cards in their name and thereafter sold the SIM-cards to other persons without complying with section 40(5) of RICA. In terms of section 40(5) of the RICA, any person who sells or in any manner provides an activated SIM-card to another person (other than a family member), as well as the person who receives the SIM-card, must, immediately upon the sale or provision of the SIM-card, provide the relevant electronic communication service provider with their full names, surnames and identity numbers. Specific amendments are introduced to address this shortcoming in the RICA.

9.2 The Cybercrimes and Cybersecurity Bill, 2015 (the Bill)

The Department of Justice and Constitutional Development has recently published the Bill for public comment. The Bill –

(a) comprehensively criminalises offences which can be committed in cyberspace;

(b) provides for expanded jurisdiction;

(c) gives law enforcement agencies cyber specific investigative powers;

(d) deals with international co-operation in matters relating to cybercrime;

(e) provides for the establishment of various structures in Government to deal with cybercrime and cybersecurity;

(f) provides for the protection of critical information infrastructures;

(g) deals with certain aspects of evidence;

(h) imposes obligations on electronic communications service providers to report cybercrime and to provide assistance to their clients to curb cybercrime; and

(i) provides for international agreements between the Republic and foreign States or territories.

The Bill also affects amendments to other legislation, among others, the RICA.

The Bill contains provisions which ensure that there is synergy between the RICA and the Bill in so far as it relates to information

which must be obtained to investigate or prove cybercrimes (clauses 39, 40 and 41).

In so far as international co-operation is concerned the Bill introduces new processes, which involve the office of the designated Judge, see clauses 41(3) to (11) (disclosure of data) and clauses 46 to 48 (requests for international co-operation). If Parliament follows the course proposed in the Bill it will mean that the workload of the office of the designated judge will increase substantially and it is hoped that the office of the designated judge will be expanded accordingly.

In terms of clause 66 of the Bill, the Schedule to the RICA is amended by the inclusion of the various offences contemplated in the Bill in the Schedule to the RICA. The Schedule to the RICA is further amended to include offences which are substantially similar to the offences provided for in the Bill, which are or was committed in a foreign State or territory. The effect of these amendments is that the RICA can be used to intercept indirect communications, real-time communication-related information and archived communication-related information in respect to the offences provided for in the Bill.

10. NEW LAW ENFORCEMENT AGENCY (NLEA)

Two additional agencies namely South African National Defence Force (SANDF) and Financial Intelligence Centre (FIC) has started to submit applications for interception during 2014. The Designated Judge has provided the necessary workshop to both these agencies, with a view to heighten the consciousness, understanding and appreciation of the need for the submission of RICA compliance application at all times.

11. SOME INFORMATION ON "GRABBER" AND OTHER LISTENING DEVICES.

Under the RICA Act, the devices utilised by various Law Enforcement Agencies do not require the designated Judge's authorisation. Once authorisation has been obtained to install a listening device, the nature of the device does not require approval of the designated judge. Whatever challenges are experienced in that regard can be explained by the particular agencies.

12. STATISTICAL INFORMATION OF APPLICATIONS FOR DIRECTIONS

12.1 State Security Agency (SSA)

Figures for the period are as follows:

	2014/2015	2013/2014

• New Applications	41	28
• Re-applications	52	34
• Amendments	57	38
• Extensions	54	35
• Combined Amendments and Extensions	23	13
• Entry Warrants (Installation of listening devices)	4	5
• Section 11 (Application for RICA information)	103	66
• Refusals	10	5
• Oral Applications for Interceptions (i.t.o Section 7 & 8)	4	2
• **Total**	**348**	**231**

12.2 THE SOUTH AFRICAN POLICE SERVICES (SAPS)

Figures for the period are as follow:

	2014/2015	**2013/2014**
• New Applications	233	158
• Re-applications	35	23
• Amendments	12	10
• Extensions	36	6
• Refusals	0	0
• Amendments and Extensions	70	22
• **Total**	**386**	**385**

12.3 THE SOUTH AFRICAN SECRET SERVICE(SASS)

Figures for the period are as follow:

	2014/2015	2013/2014
• New Applications	2	2
• Refusals	0	0
Total	**2**	**2**

12.4 FINANCIAL INTELLIGENCE CENTRE(FIC)

Figures for the period are as follow:

	2014/2015	2013/2014
• New Applications	6	3
• Amendments	1	
• Extensions	7	
• Amendments & extensions	3	
• Refusals	1	0
Total	**18**	**3**

12.5 SOUTH AFRICAN NATIONAL DEFENCE FORCE(SANDF)

Figures for the period are as follow:

	2014/2015	2013/2014
• New Applications	5	3
• Amendments	1	1

• Refusals	0	0
Total	**6**	**4**

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

	2014/2015	**2013/2014**
• Applications (New)	286	194
• Re-applications	87	56
• Amendments	71	49
• Extensions	97	41
• Amendments and Extensions	96	35
• Entry Warrants	4	5
• Section(11)	103	66
• Oral intercepts	4	2
• Refusals	11	5
• **Total**	**760**	**453**

The total number of all applications for interception in the current financial year has increased by 296 from the total of application in the previous year. Four (4) Entry Warrants, the most invasive of all interceptions had been applied for and granted. All four (4) has been requested by SSA and were therefore obtained for States Security investigations. Similarly in the 2013/2014 financial year five (5) Entry Warrants had been applied for by SSA and were also granted. No other agency had applied for Entry Warrant in the last financial year.

Oral applications are submitted in cases of utmost urgency. Four (4) applications had been submitted and all 4 had been for purposes of the SSA investigations and were approved.

13. THE SUCCESS RATE OF INTERCEPTION.

The rate of success of the interception method in the fight against crime is not easily discernable. It may be argued that the number of successful interceptions is equal to the number of applications for extension of existing interception directions, in that every application for extension requires clear indication of the relevant court – admissible evidence obtained in the last direction and what further information is intended to be obtained to make a case against a target right for prosecution. Besides, the successful prosecution of a particular target does not rely only on information obtained through interception. Success depend on a holistic approach to the investigation of a particular case.

The success of interception as an investigative method is therefore highly subjective.

14. 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).

14.1 **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.

14.2 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.

14.3 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.

14.4 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.

14.5 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.

14.6 Receptionist

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

14.7 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.

14.8 Budget

Historically, the office of the Designated Judge does not have its own budget. It continues to function as a component of the Higher and Record Management Directorate in the Department of Justice and Correctional Services. All requisitions are therefore subject to approval by the Director (PAIA and Records Management) who manages the resources of the Unit in terms of need.

14.9 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.

15. CONCLUSION

Indeed, that the system of lawful interception of private communications may be open to abuse is a likelihood that we should not be blinded to.it could be for expediency where the legal application process may be overly cumbersome. However, abuse in any form cannot be tolerated. However, together the relevant monitoring systems are well-functioning, ever conscious of the need for utmost vigilance.

As a matter of fact, that the approach of the designated judge has been one of capacity-building among others:

- Two annual workshops on the understanding of the interceptions application process and its challenges, in the context of the constitutional provisions and values are planned, and two (2) have been conducted by the designated judge-for the benefit of all sectors and role players in the interception process.
- Individual attention is provided where necessary, 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 case.

This capacity-building method has been highly effective and generally welcomed. The response to the workshops and the above individual attention has borne positive results, e.g mere suspicion is not based on sex generally no longer viewed as basis for an interception application and there is clear appreciation that an application for an interception direction is not there for the taking.