DRAFT REPORT ON THE INTERCEPTION

OF

PRIVATE COMMUNICATIONS!

A NECESSARY EVIL?

By JUSTICE YVONNE MOKGORO

Joint Standing Committee on Intelligence: Parliament

15 August 2012

STRUCTURE

1. INTRODUCTION

Honourable Chairperson and members of the Joint Standing Committee on Intelligence, kindly allow me to present to you this report. The 2011/2012 South African Police Statistical Report has revealed that, approximately 2.1 million violent crimes were registered. Although this figure shows a decline in comparison with the previous financial year, the number remains high. The escalating rate of technological crime has become alarmingly high and sophisticated. The situation has therefore become extremely challenging for law enforcement agencies to fulfil their duties optimally and efficiently. Criminals make use of these technological methods, successfully and with ease.

These methods are mainly utilised to perpetrate serious crimes ranging from:

- Human trafficking;
- Drug dealing and drug trafficking;
- Money laundering;
- Corruption and fraud;
- Kidnappings;
- Assassinations;
- Terrorism;
- Heists; etc

The state of affairs and together with the escalating rate of technological crime and highly sophisticated criminal methods, have made interception a popular method of investigation in the world over. It is then considered a necessary evil.

2. INTERCEPTION

Lawful interception plays a crucial role in helping law enforcement agencies as it represents an indispensable means of gathering information against ruthless criminals. [1] The Interception Act was designed to allow the state to monitor and listen to conversations and communications when it is difficult to gather useful information pertaining to criminal activities. This process becomes legal and the information gathered becomes admissible at court, if it is done in accordance with the relevant piece of legislation.[2]

The Regulation of Interception of Communications provides guidance and requires strict compliance with the procedure that should be undertaken when applying for the interception direction to the Designated Judge.[3] When doing so, the Act further demands thorough appreciation of section 14 of the Constitution, Right to Privacy.

Most importantly, the application process for an interception direction should be considered as the last resort, as the statute seeks to guard against abuse.

3. INTERNATIONAL LAW

Technological crime has always been a global challenge for years. That resulted in the approval of the use of interception devises by the Council of Europe Convention, to which South Africa is a signatory. These devises should only be used when necessary and within the constitutional muster.[4] The Convention had set out acceptable conditions that could necessitate usage of these devices. The law

---

[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

[4] http://conventions.coe.int/treaty/EN/projects/FinalCybercrime.htm

enforcement agency responsible must submit an application that contains a full and complete statement of facts about: The crime that has been, is being, or about to be committed and;

(i) The place, like a private house or office, and/or the communications sought to be intercepted and;

(ii) The identity of the persons committing the crime (if known) and of the persons whose communications is to be intercepted;

(iii) A full and complete statement of whether other investigative procedures have been tried and have failed or why they appear unlikely to succeed or are too dangerous;

(iv) A full and complete statement of the period of time for which the interception is to be maintained; and

(v) A full and complete statement about all previous wiretap applications concerning any of the same persons, facilities, or places.

The order initially lasts for 30 days, and investigators can obtain additional 30-day renewals from the court if they need more time. [5]

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, 127 of 1992. The investigation had shown that, the Act does not deal adequately with the technological forms of committing high-tech crimes.

[5] Surveillance Self-Defence: Getting a court order Authorizing a Wiretap- https://ssd.eff.org/wire/governmentt/wiretapping-authorization

The SALRC recommended that the Monitoring Act be repealed and replaced by Regulations of Interception of Communications Act,[6] to match the diversity and developments in communications' technologies, which include, among others, satellites, optical fibres, computers, cellular technology, e-mail, surveillance equipment, and the electronic transfer of information and date.[7]

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.[8]

4.2 Interception in case 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 telecommunication service provider concerned to intercept any communication to or from the sender in any other manner which the telecommunication deems appropriate.[9]

The service provider concerned must submit to the Designated Judge an affidavit, outlining the steps taken by the service provider in giving effect to the request

---

[6] Regulations of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002

[7] Regulations of the Interception of Communications and Provision of Communication Related Information Act- Nazreen Bawa

[8] Section 2

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

concerned and results thereof, and, any indirect communication or recordings of that indirect communication.[10]

4.3 Application for issuing of 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 the issuing of an interception direction. 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.[11]

To invoke the application of section 36 of the constitution, the Act further requires the applicant to highlight the basis for believing that, evidence relating to the ground on which the application is made will be obtained through the interception.[12] Furthermore, the application must indicate 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.[13]

An interception direction may be granted if the Designated Judge is satisfied that, on the facts provided that, there are reasonable grounds that-

- A serious offence has been or is being or will be committed;
- Gathering of information will assist to curb potential threat to public safety or health;

[10] Section 8(5)(a) and (b)
[11] Section 16
[12] Section 16(2)(ii)
[13] Section 16(2)(e)

- Gathering of information will be used against organised crime or terrorism;[14] etc.

4.4 Application for issuing of Real-Time Communication related direction

If no interception direction has been issued and a real-communication-related direction is required, the applicant must tender an application to the Designated Judge and it must be in writing.[15]

4.5 Application for combined interception directions

Where an interception direction is issued and a real-time communication is required to supplement, the applicant must draft an affidavit, which will contain:

- The results obtained from the interception direction;
- Reasonable explanation of the failure to obtain the required results.[16]

4.6 Amendment or extension of existing direction

An affidavit must be attached to an application setting forth reasons why the extension or an amendment is necessary in achieving the objectives of the direction concerned.[17] The tendency to "cut and paste" and the perception that extension is automatic should be eliminated and replaced with fact-based justification. In this regard, the justification test in Section 36 of the Constitution provides good guidance.

[14] Section 16(5)(a)
[15] Section 17(1)
[16] Section 18(2)(b)
[17] Section 20(4)

4.7 Keeping of records by heads of interception heads

The head of an interception centre must on quarterly basis submit a written report on the records kept, abuses in connection with execution of directions and any defect in any telecommunication system which has been discovered.[18]

4.8 Supplementary directives regarding applications

A Designated Judge or Designated Judges, jointly, after consultation with the respective Judges-President of the High Courts, 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.[19]

5. THE REGULATIONS 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".[20] Furthermore, Privacy is a fundamental human right recognised in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights. It underpins human dignity and other key values such as freedom of association and freedom of speech.[21]

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 such is in accordance with the law and is necessary in a democratic society and in the interests of national security, public safety or the economic well-being of the country.

---

[18] Section 37(1)(2)(a)(i-iii)
[19] Section 58(1) and (3)
[20] The Constitution of the Republic of South Africa, 1996
[21] Privacy and Human Rights-An International Survey and Privacy Laws-http://gilc.org/privacy/survey/intro.html

It should also be for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others". [22]

The Rights in the Bill of Rights may be limited only in terms of the 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.[23]

In an article prepared by the Swinburne University on Privacy and Human Rights, it is highlighted that, "the shift in balance towards absolute individual privacy is in itself a threat to security and the consequence of this choice will affect our personal safety, our right to live in a society where lawlessness is not tolerated and ability of law enforcement to prevent serious and other violent criminal activity".[24]

6. CHALLENGES

It is common knowledge and concern that, some institutions use these methods to advance their individual interests and without having regard to the rights and values of the Constitution. The media, particular, has been inundated with reports on the abuse of the interception system by officials. Ranging from-

- Acquiring of information in less than 36 hours, without the Judge's knowledge;
- Acquiring of cell phone billing and ownership records through crime intelligence on numerous occasions, without the Judge's knowledge or approval, in order to expedite the investigation;

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

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

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

- Obtaining of text messages and cell phone billing records that were needed for personal reasons, through a contact at crime intelligence;
- Bribing of contacts at banks and telecommunications service providers;[25] etc

7. FACTORS FOR CONSIDERATION OF APPLICATIONS

- Popularity of interception method is preferred over conventional method;
- The apparent lack of trust of Designated Judge is of paramount importance;
- Failure of applicants to provide fact-based justification;
- Applicant's failure to comprehend that suspicion of crime is not sufficient basis for application for interception. Question is: whether or not applicants truly understand the Act sufficiently;
- The application must carry accurate and honest information and it must further provide reasons that are clear and convincing.

Interception process should not be used as a "short-cut" by applicants who are inept or lazy to execute their mandate through conventional investigative methods, as that can severely taint the image of the law enforcement agencies or the state, the institutions should find mechanisms to:

- sharpen their conventional investigative methods; and
- consider an application for the extension as indictment on investigator's efficiency.

Telecommunication Service Providers should be made aware of the consequences involved when dealing with applications of this magnitude.

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

8. FULL STATISTICAL INFORMATION OF APPLICATIONS

8(1) The National Intelligence

Figures for the period are as follow:

• Applications	24
• Re-applications	41
• Amendments	22
• Extensions	27
• Amendments and Extensions	3
• Refusals	3
• **Total**	**120**

Brief explanation on the refusal of applications: The supporting affidavit was not good enough and the target's telephone number on the annexure did not correspond with the one on the affidavit.

8.2 THE SOUTH AFRICAN POLICE SERVICE

Figures for the period are as follow:

• Applications	87
• Re-applications	40
• Amendments	1
• Extensions	3
• Amendments and Extensions	8
• Refusals	2
• **Total**	**141**

Reasons for refusal: The application was not in good order and the application was not signed.

Combined figures for NIA and SAPS are as follow:

• Applications	111
• Re-applications	81
• Amendments	23
• Extensions	30
• Amendments and Extensions	11
• Refusals	5
• **Total**	**261**