



the doj & cd

Department:
Justice and Constitutional Development
REPUBLIC OF SOUTH AFRICA

Office for Interception and Monitoring of Communications

Please quote our full reference number in all correspondence

P O Box 57155, ARCADIA, 0007• 523 Church Street, Provisus Building, ARCADIA, 0083
Tel (012) 341 0650, Fax (012) 341 0620

Ref: 7/21/2

Enq: The Honourable Mr Justice J A M Khumalo

**REPORT TO JOINT STANDING COMMITTEE ON INTELLIGENCE
FOR THE PERIOD 1 APRIL 2010 TO 31 OCTOBER 2011**

Honourable Chairperson of the Joint Standing Committee on Intelligence, Honourable Members, ladies and gentlemen, it is an honour for me to present this report and my statistical information to you. I have not dealt with the merits of individual applications for the reason that these are top secrets which the Act protects from disclosure. These applications mostly involve difficulties experienced by agencies in the investigation of serious crimes such as:-

- Drug dealing and Drug trafficking,
- Vehicle thefts and car hijacks,
- Armed robberies,
- Corruption and Fraud,
- Assassinations, murder, terrorism, etc.

Interception involves the gathering of intelligence by secret surveillance; because of its nature it should never be allowed to become an end in itself. It should be used as a last resort in investigating crime. The Act regulates the making of applications for and, the issuing of, directions authorising the interception of communications and the provision of

communication-related information. The Act also regulates the execution of directions and entry warrants by law enforcement officers. It helps in combating the ever-present threat of serious crime including terrorism.

1. Constitutional Background

Section 14 of the Constitution of the Republic of South Africa guarantees as a fundamental right, the right of privacy which includes the right not to have the privacy of communication infringed. It stands to reason therefore, that the function of the designated Judge is also to protect innocent members of the public from unwarranted interception, and infringement of their right to privacy. A direction is therefore not easy to obtain because, as the courts have stated:-

“The potential to obtain such a direction is very strictly controlled. It could, for example hardly be issued on mere suspicion unsupported by hard facts.”

Other democratic countries have similar provisions protecting privacy. Section 8 of the European Convention on Human Rights provides an example. In keeping with the constitutional right and the limitation clause the Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002 was enacted as a law of general application. Section 2 thereof prohibits interception communications by third parties. Only stipulated state agents may apply to obtain a direction from a designated Judge to intercept a communication. The Act makes provision in sections 16, 17, 18, 20, 21 and 22 for various substantive applications and directions each with its own requirements. There is also provision for the monitoring of postal communications. The following directions may be issued by the designated Judge:-

- (i) *Interception direction in respect of a direct or indirect communication e.g. cell-*

phone. (Section 16).

- (ii) *Real-time communication-related direction, (Section 17) i.e. information stored by a service provider for 90 days.*
- (iii) *Interception direction combining real-time and archived communication-related information. (Section 18).*
- (iv) *Archived communication-related direction. (Section 19) i.e. information stored by a service provider for a period determined in a ministerial directive referred to in section 30(2) of the Act.*
- (v) *A direction authorising an entry warrant into premises for the purposes of:-*
 - (a) *Intercepting a posted article or communication, or*
 - (b) *Installing and maintaining an interception device on, and removing an interception device from the premises and this includes an oral warrant issued under section 23 of the Act.*

The duration of a direction and its extensions can only be three months. It is issued without any notice to the person or customer to whom it applies. For this reason a designated Judge has to be very careful when considering granting a direction. He will only grant a direction if he is satisfied that any of the grounds set out in sections 16(5), 17(4) and 19(4) of the Act are mentioned in the affidavit. The right of privacy of the person concerned must however be borne in mind.

2. Meetings with Office of Interception Centres, Service Providers and Law Enforcement Officers:

Whenever problems concerning any of the abovementioned instances arise meetings are held with responsible officers and problems are resolved. This helps to improve the quality

of work. The timeous delivery of directions to the Office for Interception Control which is now being delivered by one of the Clerks attached to the designated Judge's office has taken effect from 29/06/2011. From 18/01/2011 to 24/06/2011 the Office for Interception Centres came to fetch directions directly from our office, this arrangement was made between the designated Judge's office and Director Koopedi from the OIC to ensure that the correct directions reach the OIC and that the directions are triggered correctly before the Service Providers activate their triggers.

The Department of Defence have requested assistance to seek interception of communication in appropriate cases and my officials expressed their willingness to assist. Two of the problems which have given rise to these meetings are:-

2.1 The submission of documents mentioned in section 8(5) of the Act. It appears that my predecessors did not insist on their submission or check compliance with the Act. Section 8 deals with interception of communication for purposes of determining location in cases of emergencies resulting mainly from threat to life and limb. The section requires the following to be submitted by the service provider concerned and the Law Enforcement Agencies:-

- "(a) a copy of a written confirmation of request made by the law enforcement officer to a service provider,*
- (b) an affidavit by the law enforcement officer setting forth the results of the request and information,*
- (c) an affidavit of the service provider setting forth the steps taken by the service provider in giving effect to the request of the law enforcement officer and the results and information obtained from such steps, and*
- (d) if such steps included the interception of an indirect communication, any*

recording of that indirect communication that has been obtained by means of that interception, any full or partial transcript of the recording and any notes made by the telecommunication service provider of that indirect communication.”

2.2 A designated Judge is required to keep this record for five years. It is important to note that the section allows this interception to take place without prior authorisation by the designated Judge, because of the emergency. If there is no emergency as contemplated by the Act the interception is unlawful. Hence my eagerness to check that such interceptions comply with the Act. At present the police are up to date in their submission of these documents. I have in the meetings insisted on compliance. One of the Service Providers i.e. MTN has not submitted anything. It is anticipated that when compliance has been achieved these voluminous documents will be spot checked instead of them all being checked individually. What complicates the situation is that the section does not stipulate the simultaneous submission of documents by police and service providers to facilitate filing. I have suggested to police to submit these documents simultaneously including those from service providers to facilitate proper filing. Otherwise, the section if properly used is a useful weapon in combating serious crime.

3. Draft Directives in terms of Section 58(1) of the Act

These have been forwarded to the office of the late Advocate Labuschagne for consideration and approval by the Judges President of the Republic. Unfortunately Advocate Labuschagne passed away suddenly and I have not heard from his successor. Section 58(1) of the Act reads as follows:-

“A designated judge or, if there is more than one designated judge, all the designated judges jointly, may, 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 in terms of this Act.”

4. Newspaper reports and articles criticising the Act and its implementation

The designated judge follows criticism of the Act and its implementation which from time to time appear in the media. There have even been suggestions of a commission of enquiry, because of allegations of illegal hacking into citizen’s private telephone conversations. Apart from what I have said in connection with section 8 of the Act, I am personally not aware of any unlawful secret surveillance carried out by any of the state agencies. If such is the case the Departments concerned should investigate as a matter of urgency. Unfortunately no specific individuals are mentioned by the critics. Section 51 of the Act prescribes very severe penalties for transgressions under the Act. For instance any person who intercepts or attempts to intercept, or authorises or procures 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, is guilty of an offence and is on conviction liable to a fine not exceeding R2,000 000 or to imprisonment for a period not exceeding 10 years. I can assure the committee that I have not spoken to any journalist and any enquiries they make are referred to the Department of Justice.

5. Statistical information

My office has a manager, a legal assistant, a secretary and three clerks. It is a good and supportive staff. The designated Judge is required to keep his records for five years. For a reason I do not know, no files have been destroyed by previous designated Judges and I can foresee a time when there will be no space to keep further records.

What now follows is a brief discussion of statistical data pertaining to the work done during the period under review.

There is no backlog in the applications dealt with. The incoming work is dealt with on a daily basis.

The National Intelligence Agency

Figures for the period are as follows:-

• Applications	65	
• Re-applications	27	
• Amendments	38	
• Extensions	38	
• Amendments and Extensions	31	
• Refusals		2
• Total	199	2

The South African Police Force

Figures for the period are as follows:-

• Applications	376	
• Re-applications	94	
• Amendments	111	
• Extensions	42	
• Amendments and Extensions	64	
• Refusals		4
• Total	687	4

The South African National Defence Force

- Application 1

The combined figures for the NIA, SAPS and SANDF are as follows:-

• Applications	442	
• Re-applications	121	
• Amendments	149	
• Extensions	80	
• Amendments and Extensions	95	
• Refusals		6
• Total	887	6

There was an increase of 81 new applications which is approximately 20%. Amendments and extensions on existing files amounted to approximately 50%. 3 217 requests in terms of Section 8 of the Act were dealt with by the South African Police.

A perusal of the above figures shows the following:-

- (a) Most of the work comes from the South African Police followed by the National Intelligence Agency;
- (b) The Department of National Defence has submitted only one application;
- (c) The Independent Complaints Directorate has not submitted any application during the period under review and I submit a nil return;

(d) The figure 887 which includes amendments and extensions is reasonably small considering the large number of cell phones and landline telephones currently in use in the country. This is in keeping with the notion that electronic surveillance is considered as the last resort in crime prevention and gathering of information to ensure the security of the state;

(e) The 20% increase in new applications may be due to a realisation by the law enforcement agencies of the effectiveness of interceptions. This indeed is the case if one thinks of the observation made by the South African Law Commission at page 19 of its project 105 which reads as follows:-

“..... Telecommunications are being used more and more in the organizing and commissioning of crime especially organized crime, heists and other serious violent crimes. Legal provision should be made to give law enforcement agencies the necessary tools to investigate such crime as well as other concomitant crimes such as money–laundering. A review of the Act should ensure that the emphasis in the Act should be on crime.”

6. Recommendations by the Honourable Judge JAM Khumalo

Amendments to section 7 and 8 of the Act should be effected to facilitate filing of documents by police and service providers. Amendments to prevent any possible abuses by State agencies and service providers should be considered.

Lastly I wish to take the opportunity to thank the NIA and SAPS for being careful in supplying information required by the Act when preparing affidavits in support of applications submitted. I also thank the staff for assisting me in the preparation of this report.

J A M KHUMALO
DESIGNATED JUDGE
2011/10/31