



"Careful...Big Brother is watching "

An examination of some key provisions of the Regulation of Interception of Communications and Provision of Communications -Related Information Act (70 of 2002) in light of the right to privacy and freedom of expression

Summarised version

By Simon Kimani Ndung'u¹

Head: Anti-Censorship Programme

FXI

18 September, 2004

Introduction

George Orwell, famous English writer invented the concept of "Big Brother". Over the years it has grown to become part of our lexicon.

Orwell also gave us other popular terms that we so liberally apply in our daily discourse such as; "thought police" "double think" and "double speak". Indeed, people often talk of something being likely to lead to an "Orwellian situation".

¹ The writer is the head of the Anti-Censorship Programme at the Freedom of Expression Institute in Johannesburg. This paper was presented at the "Highway Africa" conference organised by the Open Society Institute for Southern Africa (OSISA) and held between 15-18 September 2004 in Grahamstown, South Africa.

In "1984", Orwell's central character Winston Smith, a 39 year old employee of the "Ministry of Truth" takes the reader through the pressure crucible that is the daily experience of living under the watchful eye of Big Brother. Regarding the surveillance system deployed by Big Brother in people's homes to monitor their activities, Smith says that it:

*" ...received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision, which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live -- did live, from habit that became instinct -- in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."*²

We could be faced with this scenario one-day if the Regulation of Interception of Communications Act (Interception and Monitoring Act, "IMA") is implemented.

IMA in essence seeks to put in place a **"super-surveillance system"** in South Africa.

IMA uses **wide and over-reaching definitions of key terms such as "communication", "party to a communication", and "serious offence"**. It ensures that, as in the case of Winston Smith, any sound or image of any nature (including a whisper) will be picked up by Big Brother.

FXI's and Misa's joint submission on the IM Bill warned of *"The extensive increase in the power of the authorities to act in secret against the citizens of the country."*

² George Orwell, (1949), 1984, Chapter19, p2.

Also added that:

*"There are good grounds for believing that the powers requested are so extensive that, if granted by the acceptance of this Bill by Parliament, South Africa [could] revert to a police state."*³

1. Constitutional rights

1.1. Right to privacy

Section 14 of the Constitution:

"Everyone has the right to privacy, which shall include the right not to have-

- (a) their person or home searched;*
- (b) their property searched;*
- (c) their possessions seized;*
- (d) the privacy of their communications infringed".*

Right to privacy is fundamental. Constitutional Court (CC) sees it as one of the constitutive aspects of a '**persons dignity**'.

CC held in the case of **Bernstein v Bester NO4** that breaches of privacy include entry into private premises, the reading of private communications/documents, listening into private communications, the shadowing of a person and the wire-tapping or bugging of private communications.

Right to privacy may only be limited in the interests of the community subject however, to lawful conduct and lawful justification.

³ FXI, MISA-SA submission to the Justice and Constitutional Affairs Portfolio Committee, 26 August 2001.

⁴ 1996 (2) SA 751 (CC),

1.2. Right to freedom of expression

Section 16 of our Constitution:

(1) Everyone has the right to freedom of expression, which includes-

(a) Freedom of the press and other media;

(b) Freedom to receive or impart information or ideas;

(c) Freedom of artistic creativity; and,

(d) Academic freedom and freedom of scientific research.

Right to freedom of expression can be limited (propaganda for war, incitement of imminent violence and hate speech are prohibited)⁵.

Any other form of limitation must be reasonable and justifiable in an open and democratic society based on human dignity, equality, and freedom and take into account a number of factors including the nature and extent of the proposed limitation and any less restrictive means of achieving the purpose of that limitation.⁶

Important question is, whether the IMA constitutes a lawful limitation to the rights of privacy as well as freedom of expression. An examination of many of its key provisions proves that it does not.

⁵ Section 16(2).

⁶ Section 36 of the Constitution.

2. The Act's general approach (chapter 2)

The general rule is to prohibit interceptions by third parties. No person may, without the knowledge or permission of the communicator intercept or monitor a past, occurring or intended communication.

Immediately thereafter however, the Act deals at length with the various exceptions to this general rule under which it will be perfectly legal to monitor and intercept all forms of communication between people in South Africa.

This general rule seems rather like **a red herring or a fig leaf** because the Act in the main is concerned primarily with the monitoring and interception of communications by the State.

I will therefore concentrate my attention on the State in this discussion.

3. The State as your Big Brother

IMA gives the state extensive powers to pry into, record, seize and or divert the private postal, electronic, computer communications and websurfing habits of any person.

Tap follows the person, not the telephone or room as in the old days. Further, in the main, people will be unaware that they have been the subject of an interception or intrusive surveillance.

Interception will be done not only for **crimes that happen** or are **very likely to happen**, but also for those that **"will probably"** be committed at some point in the future.

Whether such crime is eventually committed or not is, in the eyes of the Act, immaterial. The point is that the State will have the powers and very wide discretion to decide to intercept communications on some rather sketchy basis.

A series of interception and monitoring centres will be established by the State for use by the police, the defence force, intelligence agencies and the Directorate of Special Operations established under the National Prosecuting Authority.

Harsh penalties are provided for persons and businesses who contravene the Act including those who fail to co-operate in investigations or who fail to comply with directives issued under the Act.

4. Provisions that bolster or assist the state in its monitoring and interception activities

4.1. Assistance by decryption key holders –s29

Any person who has the password to access communication material or equipment or the ability or knowledge to decipher communication material is legally bound to actively assist the **enforcing officer**. Section uses the word "must".

4.2. Prohibition on certain telecommunication services (s30)

No service provider may provide a service which is not capable of being monitored or intercepted. Every service provider has to acquire, at its own cost, the necessary equipment and facilities to enable such monitoring and interception.

4.3. Service providers have to obtain and stockpile a wide category of client information (s39 &40)

A service provider has to obtain the full names, all addresses, identification numbers and registrations details of its clients or customers. Clients include contract and prepaid cellular phone users. The service provider is obliged to provide such information to the enforcing officer.

4.4. Legal duty to report lost, stolen or destroyed cell phones or SIM cards (s41)

The duty falls on the owner or person in possession or control of a cellphone or SIM card to report to the police in case of loss, theft or destruction. The person must obtain a case number upon doing so. Any individual found in possession of a suspected stolen cellphone or SIM card and who is unable to give a satisfactory account of such possession is guilty of an offence.

4.5. Prohibition on the manufacture, possession and advertising of listed interception and monitoring equipment (s45 and 46)

No person may manufacture, assemble, possess, sell, purchase or advertise any equipment, which has been declared as listed by the Minister of Justice. Minister may however make some exceptions.

4.6. Revocation of the licence of service providers (s56)

Minister of Communications may revoke the licence of a provider who contravenes a directive more than once.

4.7. S205 of the Criminal Procedure Act (51 of 1977) (s59)

S205 which enables the state to subpoena any person and subject them to questioning in a bid to obtain evidence, will be amended by the IMA to provide for the subpoena of any person in respect of an investigation under the Act also.

5. Purported judicial oversight and safeguards: The "designated judge"

When the **IM Bill** was passed by the National Assembly on 17 September 2002, the then Deputy Minister of Justice **Cheryl Gillwald** in responding to wide criticism against the Bill was quoted in the media as having said that "*sufficient safeguards*" had been

built into the law and that furthermore, *"judicial sanction is required for all interceptions or monitoring"*. (Except of course in situations of emergency.⁷)

Let us examine this 'judicial oversight'.

5.1. Role of "designated judge"

A 'designated judge' is the person who will play the sort of judicial oversight role that Deputy Minister Gillwald spoke about in defence of the new legislation.

A "designated judge" is defined by the IMA as:

“any Judge of a High Court discharged from active service under section 3(2) of the Judges Remuneration and Conditions of Employment Act, 2001 (Act No. 47 of 2001), or any retired judge, who is designated by the Minister to perform the functions of a designated judge for the purposes of this Act.”

Applications for interception directives will be made to this judge.

The question is whether this authorising authority is a proper judicial authority and whether a reasonable person will perceive him or her to be an independent authority. In terms of the analysis below it would seem not.

5.2. The Constitution and the appointment of judges and judicial officers

The Constitution distinguishes between judges and other judicial officers. Judges are appointed through procedures involving the **Judicial Service Commission (s174 (6)** of the Constitution). The composition of the Judicial Service Commission includes a **Constitutional Court judge, High Court judges, lawyers in private practice,**

⁷ The Citizen, 'Eavesdrop Bill gets support', 18 September 2002, p4.

members of the National Assembly, including members of the opposition and an academic.

Other judicial officers (e.g. magistrates):

“must be appointed in terms of an Act of Parliament which must ensure that the appointment, promotion, transfer or dismissal of, or disciplinary steps against, these judicial officers take place without favour or prejudice” (s174(7)).

Judicial officers are required to act independently and impartially and at an institutional level it requires structures to protect courts and judicial officers against external interference.

As the Constitutional Court emphasised in the case **Van Rooyen & others v S and others**,⁸:

“judicial independence connotes not merely a state of mind or attitude in the actual exercise of judicial functions, but it is a status of relationship to others, particularly to the Executive branch of government, that rests on objective conditions or guarantees.”

The IMA does not provide for any bodies or process of appointment and discharge of the ‘designated judges’ nor is there a provision that the designated judges will be part of the ordinary judiciary’.

The fact that the person appointed by the Minister to provide oversight of law enforcement officers who wish to intercept and monitor private communications is referred to as a “designated judge” is **disingenuous**. The term “judge” refers strictly to the employment history that the Minister’s chosen delegate must have and not to this

⁸ 2002 (8) BCLR 810 (CC)

person being part of an independent institution or structure or existing in any sort of relationship to the executive that may be described as truly judicial.

For all intents and purposes, he designated judge is, simply and purely, a "**Ministerial appointee**".

The question of judicial independence has been addressed from time to time by our courts of law.

Two years ago, the Pretoria High Court ruled that the conviction and sentence against a **Mr. Thomas van Rooyen** for housebreaking was invalid because the Department of Justice's procedures regarding the appointment of the presiding magistrate was "**unconstitutional**". The court observed that the Magistrate, **Michiel de Kock's** contract with the Department of Justice resulted in the **State being his "boss", which consequently affected his independence.**⁹

5.3. The designated judge's discretion is fettered

The judge's discretion is qualified by words that give concern that he or she will be not able to make a reasonable and objective decision, namely "**on the facts**" "**is satisfied**", "**there are reasonable grounds**" and "**serious offence**" as well as the very broad definition of "**party to a communication**".

A directive is largely dependent on the applicant's own personal views of the situation. The fact that the applicant must, as soon as practicable, furnish the judge with an affidavit

⁹ Citizen, 'Justice Dept may appeal', 13 November 2002, p7. *The article went on to quote the court as having said that "it was clear the issue of validity of Mr. De Kock's appointment was of substantial importance to the public, and in particular the general administration of justice, with wide ranging consequences".*

setting out the results and information obtained from the intercept, will be no comfort to the person whose privacy is secretly being invaded with no process at all.

6. Conclusion & recommendations

6.1. Conclusion

I want to conclude this paper by highlighting a number of important issues in regards to the IMA and also make a few recommendations.

- The IMA stands to violate individual's right to privacy as well as associated rights such as freedom of expression. As FXI and Misa-SA said in their submission to Parliament:

"Media investigations into government corruption and mal-administration will be [compromised] because police will now have the power to intercept communications from informers to the media and communications about such stories It will also nullify the ability of 'whistle-blowers' to operate if not compromise their protection and allow authorities to intrude into newsroom activities and inspect the contents of newspaper reports before they are published."

- The common law and constitutional principles regarding intrusive measures and search and seizure are infringed extensively by the IMA. The provisions that empower the state to intrude into a person's communications, search, seize and dispose of communication data and information contains significant changes to the Criminal Procedure Act (CPA) and the rules of evidence.

- Whereas in a normal situation stringent grounds are established under the CPA for obtaining search or interception warrants, these measures have now been whittled down under the IMA. Under this new law, **a warrant of sorts (the directive)** is obtained. However it is executed without the knowledge of the target and without an opportunity to challenge it.
- There are no provisions for special procedures covering intercept material that is legally or otherwise privileged material, for instance communications between lawyers and clients. The European Court of Human Rights in **Campbell v UK** stated that a high level of protection is to be accorded to these sensitive categories of material.
- By and large, the Act in attempting to strike a balance between individual rights and liberties and the requirements of law enforcement gives overwhelming weight to the latter.

5.4. Recommendations

- Firstly, since the search and seizure provisions violate the right to privacy, they must be justified under the limitation clause of the Constitution. To comply with s36, the IMA must provide clear guidelines within which law enforcement officers are to carry out their functions. Wide discretionary powers must be avoided. As set out above, the enforcing or executing officers have wide discretion and subjective powers in deciding to intercept communications and in executing the directives.
- Secondly, the warrant has to be issued by an impartial and independent judicial authority not an individual who is already an **executive appointee** as happens to be the case with the "**designated judge**".

- Thirdly, any legislation permitting the monitoring and interception of communications by the State must require the judicial authority to be persuaded by **evidence on oath** that there are reasonable grounds, at common law, for believing that something that will afford evidence of the offence may be recovered. The IMA does not make provision for evidence under oath in its written or oral applications.¹⁰

- Fourthly, an objective criteria is needed to assess the necessity of issuing an interception direction or entry warrant and for this reason, words such as ‘in his/her opinion’, or ‘as soon as is practicable’, as well as the wide definition given to “serious offence” should also be amended or repealed. And finally,

- The IMA should contain a provision, which prohibits covert surveillance of privileged material.

¹⁰ (see SAAPIL v Heath 2000 (10) BCLR 1131 (T), Park-Ross v Director, Office for Serious Economic Offences 1995 (2) BCLR 198 ©).