



"Big Brother is watching you"

A critical examination of some key provisions of the Regulation of Interception of Communications and Provision of Communications -Related Information Act (70 of 2002) from the perspective of the right to privacy and freedom of expression

By Simon Kimani Ndung'u¹

Head: Anti-Censorship Programme

FXI

10 September, 2004

1. Introduction

Some of us in this room may be familiar with the writings George Orwell, the English writer and more particularly with his most renowned work "1984" from which the concept of Big Brother originated and which over the years has grown to become part of our daily lexicon.

Of course Orwell also gave us other popular terms, which we so liberally apply in our discourse such as; "thought police" "double think" and "double speak". Indeed, you'll often hear people say a particular thing is 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 "Internet Week" organised by the Internet Service Providers' Association (ISPA) and UniForum SA, 15-18 September 2004, at Glenburn Lodge Johannesburg.

In the political satire "1984", Orwell's central character Winston Smith, a 39 year old worker in 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

This is the scenario, which we could be faced with one day if the Regulation of Interception of Communications Act (Interception and Monitoring Act, "IMA") is fully implemented. The IMA in essence contemplates the existence of a "super-surveillance system" in South Africa and by its use of 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.

In their joint submission during the Interception and Monitoring Bill's discussions in Parliament, the Freedom of Expression Institute and the Media Institute of Southern Africa-SA chapter expressed their opposition to *"The extensive increase in the power of*

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

the authorities to act in secret against the citizens of the country." The two organisations went on to argue 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 will revert to a police state."*³

What then are the issues of concern in regards to this new law? Before we interrogate this point at depth however, let us first look at two of the key fundamental rights and freedoms that stand to be violated through the implementation of the IMA.

2. Constitutional rights

2.1. Right to privacy

Section 14 of the Constitution states that:

"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".*

So fundamental is the right to privacy that the Constitutional Court (CC) sees it as one of the constitutive aspects of a 'persons dignity'. Additionally, the CC held in the case of **Bernstein v Bester NO4** that breaches of privacy include entry into private premises, the

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

⁴ 1996 (2) SA 751 (CC),

reading of private communications/documents, listening into private communications, the shadowing of a person and the wire-tapping or bugging of private communications.

Furthermore, the Court also held that the scope of the right to privacy is not absolute; that it has to be demarcated with reference to the rights of others and the interests of the community subject however, to lawful conduct and lawful justification.

2.2. Right to freedom of expression

Section 16 of our Constitution provides for the right to freedom of expression by stating that:

(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.

Though the right to freedom of expression, as is the case also with the right to privacy, is not absolute, it may only be limited in terms of the parameters set out by the Constitution (propaganda for war, incitement of imminent violence and hate speech are prohibited)⁵. Any other form of limitation must conform with the criteria laid down in the general limitations clause. Such limitation must perforce, be reasonable and justifiable in an open and democratic society based on human dignity, equality, and freedom. The limitation must also take into account a number of factors including the nature and extent of the

⁵ Section 16(2).

proposed limitation and any less restrictive means of achieving the purpose of that limitation.⁶

Any law that provides for an infringement of the right to privacy, almost *a priori*, exerts pressure on other associated rights including in this instance, the right to freedom of expression. This is not only because legal and administrative action may be instituted against certain of those whose communications are intercepted, monitored or deciphered but because the knowledge that private communications are subject to interception, monitoring and deciphering causes self-censorship.

Should the law that enables interception, monitoring and deciphering be too wide in application and the procedures that authorise the same be too loose in oversight, many reasonable and informed people may safely be assumed not to express certain views or opinions. The essential question, however, 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.

3. Definition of some key terms and concepts

To monitor includes the recording of communications by a ‘monitoring device’.

A ‘monitoring’ device is any equipment to ‘listen to or record’.

To intercept means the monitoring or acquisition or diversion of the contents of any communication, including the diversion of communication from its intended destination.

A party to a communication includes a participating or active party, a person in whose immediate presence a direct communication occurs regardless of whether the communication is directed to the person and intended senders or intended recipients.

⁶ Section 36 of the Constitution.

A serious offence, is any offence mentioned in the Schedule (or any offence that is allegedly being or has or will probably be committed by a person or group or syndicate acting in an organised fashion) which includes involvement in at least two incidents of criminal or unlawful conduct or conduct which could result in substantial financial gain or an attempt to commit any of the aforementioned.

Schedule offences, are listed as high treason, any offence relating to terrorism, any offence involving sabotage, sedition, any offence which could result in the loss of a person's life or serious risk of loss of a person's life, any offence in the Rome Statute of the International Criminal Court, any specified offence defined in the National Prosecuting Authority Act.

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

At the outset, the Act deigns to prohibit the interception as well as the intentional monitoring of communications by third parties. The general rule is that 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. For the sake of this discussion however, I will only deal with acts of interception and monitoring by the State, as that is where the new "super-surveillance" system will be erected. This general rule therefore seems rather like a red herring or a fig leaf since it appears in all of one paragraph in the Act while the rest of the statute is concerned primarily with the monitoring and interception of communications.

5. The State as your Big Brother

In a nutshell the 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. And because of the nature of the equipment used by all parties, the 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.

What becomes painfully obvious is that the scope of the interception and monitoring that the state can conduct is extremely wide. For instance the state will now legally be able to monitor and intercept communications on the basis of a crime 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 such 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.

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

6.1. 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 29 of the IMA requires any person to

decrypt data on demand and the use of the word “must” in the section indicates that if called upon, the person will be under a mandatory duty to do comply with the enforcement officer. The state will probably use s205 of the Criminal Procedure Act (on the subpoenaing of witnesses to give evidence which the Act seeks to amend), in this process.

6.2. 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. Considering the wide definition of ‘telecommunications service provider’ this could mean that if someone operates a website, email server or any other service which uses telecommunications, he or she could be deemed a provider and required to foot a substantial bill for monitoring equipment.

6.3. 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. It appears that no separate warrant application is required to obtain such information.

Failure to obtain and keep and hand over such information may render the provider guilty of an offence and liable to a fine not exceeding R200 000 (s15).

6.4. 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.

Any person who acquires possession of such an item from another without having reasonable cause for believing that the item is the property of the person is guilty of an offence. In the absence of proof to the contrary, possession is sufficient evidence of the absence of reasonable cause.

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

Under these two sections, no person may manufacture, assemble, possess, sell, purchase or advertise any equipment listed under section 44. This includes equipment of an electronic, electromagnetic, acoustic, mechanical or other nature, which the Minister of Justice under section 44, has declared to be listed. The Minister may however make some exceptions.

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

Notwithstanding any penalty imposed or which may be imposed by a court, the Minister of Communications may revoke the licence of a provider who contravenes a directive more than once.

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

This section, 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.

7. 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 in situations of emergency.⁷

So what 'judicial oversight' is this which the Act supposedly puts in place to ensure that there is no unwarranted violation of people's right to privacy and expression. Let us turn our attention to this entity called the "designated judge" for better understanding.

7.1. 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. The Act purports to allay any fears in this regard and to provide "checks and balances" by bringing into being an institution or, as it turns out, an individual of oversight who is called a "designated judge" and who 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.”

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

It is to this judge that *ex parte* applications will be brought to permit the said acts of monitoring and interception. 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.

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

When dealing with the appointment of 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, 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 a status of relationship to others, particularly to the Executive branch of government, that rests on objective conditions or guarantees.

Regarding what constitutes a proper and independent judicial authority, the Court found that the functioning of the judicial officer in an independent court is necessary. It further found that the material requirement for an independent judiciary (and thus a ‘judge’) was

⁸ 2002 (8) BCLR 810 (CC)

an independent organisation that was responsible for the appointment and removal of judicial officers and security of tenure.

The court went on to stress that judges and magistrates who serve in the courts could be said to be independent and part of an independent judiciary because the JSC and the Magistrates' Commission recommended them for appointment. The nature of the panels made them relatively un-open to political abuse. Importantly the Commissions' objectives included ensuring that the appointment, promotion, transfer or discharge took place without political favour or prejudice. Thus there were important safeguards of judicial independence. There were also constitutional and judicial safeguards in place to prevent interference with the Commission by the executive or the legislature.

The IMA does not provide for such 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 nominated 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 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.

Being a judge rests on more than perceptions of an individual's integrity. As suggested above, the ability of the judge to be perceived as neutral and impartial rests on numerous structural factors such as the fact that he or she is part of a collective bench, is selected as part of a process in which the legislature, the profession and academia also have a say and has his or her tenure secured in a manner which limits their exposure to fear or favour.

All of these aspects are absent in respect of the designated judge. The supposed check to executive misuse of the need for a level of interception and monitoring in society is completely vitiated by the fact that the designated judge is, purely and simply, a "**Ministerial appointee**". Since this person is appointed under the authority given to the Minister in terms of the IMA and since there are no provisions for the dismissal of a designated judge, it is to be assumed that such a 'designated judge' ceases to be one when Ministerial authority is withdrawn. While it may be that the Minister him or herself will not replace a "designated judge" because rulings are not going the executive's way, the absence of any structural safeguards to prevent this, in my view, will create in any reasonable person the perception of partiality.

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

The question of who authorises interceptions is considered an important one by international jurists. The European Court of Human Rights has on several occasions stressed the importance of real judicial oversight. In **Klass v Germany** and **Huvig v France** (1990) the courts emphasized that supervisory control must be entrusted to a judge, preferably a senior judge. They were referring to proper judges who were part of the judiciary.

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".

7.3. The designated judge's discretion is fettered

In a written application for a direction, the judge's discretion is qualified by words that give the appearance that he or she will be able to make a reasonable and objective decision, namely "on the facts" "satisfied", "reasonable grounds" and "serious offence". However the decision will have to be made within the definition of a "serious offence". It is submitted that this wide definition negates the "judge's" ability to make a reasonable and objective decision.

Besides the scheduled offences which do include offences that are objectively serious, the definition also covers unspecified offences and conduct which is widely and vaguely defined, for example '...or any offence that is allegedly being or has or will probably be committed. It further covers conduct, which the applicant alleges "probably will" or "could" happen. Thus the subjective opinion of the applicant and the wide definition of "serious offence" is ultimately defining.

The judge's discretion is further fettered by the wide definition of "party to a communication" since it can include persons in whose immediate presence a targeted communication was made. Accordingly the direction or order can cover and make a target for interception and monitoring and seizure of communication material someone who worked with or lived next door to or sat on a park bench with or has been seen in the company of or whose telephone line was called by the main target.

The state can bypass even this limited and dubious "judicial" control and track email and telephone conversations in emergency situations without having to prove probable cause (reasonable belief of the likelihood that a crime has been or is being committed) before a judge or if the applicant is of the opinion that the situation is urgent or if the applicant is of the opinion that serious bodily harm may be committed by a suspect. The word "opinion" denotes a subjective rather than an objective view.

In other words 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 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.

Accordingly there is no objective standard, as determined by a neutral arbiter, for the limitation of the right the IMA supposedly recognises at the onset. It is a tenet of administrative law and the Constitutional Court that objective criteria should be set for the exercise of any executive or administrative function (see **the Van Rooyen case**, p838-9).

The general rule is that the application must be in writing and contain details of all the facts and circumstances in support of the application. However an oral application can be made if the Applicant is of the opinion that it is not reasonably practicable, having regard to the urgency of the matter, to make a written application. The process must be confirmed in writing within 48 hours.

Conclusion & recommendations

7.4. Conclusion

I want to conclude this paper by pointing out a number of issues and also make a few recommendations.

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

"Media investigations into government corruption and mal-administration will be [severely compromise] because police will now have the power to intercept communications from informers to the media and communications about such stories within media companies themselves. 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 in 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.

7.5. Recommendations

- Firstly, since 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 must 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 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 opinion’, or ‘as soon as is practicable’, as well as the wide definition given to “serious offence” should also be deleted.
- Fifthly, the IMA should contain a provision, which prohibits covert surveillance of privileged material, and finally,

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

- Intercept material should not be used as evidence and recourse may be had to Interception Act in the UK (sections 16 and 17), which prohibits the use of such material.