

## Guide to monitoring e-communications in SA

The information contained in this document has been prepared by Michalsons Attorneys and is intended for general information purposes only. Do not make any business decisions on the basis of this information without consulting an appropriately qualified lawyer who can analyse your precise requirements.

### Introduction

There has been a lot of debate as to where employee rights to privacy end, and where employer rights to monitor electronic communications begins. An analysis of the case law shows that there are no clear guidelines, and matters have been made worse by the signing of the new Interception Act in December 2002. This Act has created considerable confusion as to what law applies to monitoring, what employee communications can be monitored, and what has to be done to comply with the relevant law.

### The current situation

At present (July 2004) the monitoring and interception of employee communications is governed by the old Monitoring Act (called the **Interception and Monitoring Prohibition Act**, 127 of 1992 (the old monitoring Act) and not the new Monitoring Act (called the **Regulation of Interception of Communications and Provision of Communication Related Information Act**, 70 of 2002 (the new monitoring Act). The new monitoring Act was signed into law on 30 December 2002, but no commencement date as yet has been determined. This is why the old monitoring Act is still the governing piece of legislation.

It is important to point out that when the old monitoring Act was enacted in 1992, email and the widespread use of the Internet were largely unknown in South Africa. Therefore, many argue that the main focus of the old monitoring Act is on the monitoring and interception of telephone conversations, as opposed to email and Internet communications.

### The Constitution

Most of the cases that have dealt with unlawful monitoring in South Africa were heard after 1996, when the right to privacy was recognised as a fundamental right under the Constitution (the **Constitution of the Republic of South Africa Act** 108 of 1996 (the Constitution). All of the reported cases in the High Court and Constitutional Court involved the recording of telephone calls, in particular whether the alleged recording of the telephone calls constituted a breach of the right to privacy under the Constitution.

Section 14(d) of the Constitution prohibits employers from intercepting and monitoring employee's private face-to-face conversations or telephone conversations and other private communications, unless the employee has consented to such monitoring, or where the breach of privacy is justified by necessity or in terms of the limitation clause in section 36 of the Constitution. (The Constitution contains a so-called "limitations clause" which provides that inroads into the rights contained in the Constitution can be made by the enactment of the other laws and where it would be reasonable and justifiable to do so).

### The new Monitoring Act

The new monitoring Act follows on the old monitoring Act, but the provisions have been made significantly more sophisticated, and they apply to all forms of communication, both direct (face-to-face) and indirect (including post and all forms of electronic communication or telecommunication, such as telephone, fax, email, network or Internet messaging, etc.).

The new monitoring Act begins with a general prohibition on intercepting any communication in section 2. Contravening section 2 is an offence that carries heavy penalties: a fine of not more than R2 million or imprisonment of not more than ten years.

There are **four main exceptions** to this general prohibition:

1. Where a person is a party to the communication (such as where participants in a meeting consent to the meeting being recorded),
2. Where the parties to the communication give their prior written consent to the interception (section 5),
3. Where a law enforcement officer obtains an interception directive from a judicial officer because of a suspicion that a serious crime has been committed or is about to be committed,
4. Where any person or entity intercepts certain communications for business purposes only – the so-called “business exception” (section 6).

There are certain criteria that have to be adhered to in order for the monitoring to be lawful. Unlike section 5, section 6 does not require the written consent to intercept. What is required is that the employer make “reasonable efforts” to inform an employee in advance that interception may take place, or to obtain the “express or implied consent” of the employee.

The scope and effect of section 6 is far from clear, and it will require detailed interpretation by the Courts in the future. Contravening section 6 is an offence that also carries heavy penalties: a fine not exceeding R2 million or imprisonment for a period not exceeding ten years.

### What do the cases say?

South Africa follows the doctrine of “precedent”. The general rule is that all courts are bound by the decisions of the courts superior to them, and that courts will follow their own decisions unless they are clearly wrong. In applying legal precedent, a detailed process of analysis is followed: some cases are more authoritative than others. The High Court of Appeal and the Constitutional Courts rank the highest and all lower courts are, for example, bound by their decisions.

There are no known reported decisions relating to monitoring and interception of email in the workplace emanating from the Labour Court, High Court, the High Court of Appeal or the Constitutional Court. They have only been heard in alternate dispute resolution forums where the system of precedent does not operate (e.g. the CCMA and arbitration tribunals). This has resulted in there being no case-law and clear guidelines to follow, as the latter tribunals’ decisions do not constitute binding or even persuasive decisions which our other courts would be bound to follow.

Analyses of a sample of some arbitration decisions reveal that there appears to be a trend towards accommodating the employer who unlawfully monitors the email activities of employees.

### The Choice

In order not to run foul of the law, employers must decide whether or not they are going to base their thinking around the old monitoring Act (which currently governs the situation) or the new monitoring Act (which has yet to become law and there are no indications as to when this will happen). What’s more, if employers are going to rely on the new monitoring Act, they must decide whether they will choose to base their implementation plans on section 5 or section 6.

Ultimately, if employers take the provisions of section 5 and/or 6 into account, they can monitor and intercept communications in the workplace provided that, where they seek to rely on a particular provision (ex post facto), they have complied with the provisions contained in that section. This is key to implementing the monitoring provisions.

#### **Employee consent**

Irrespective of whether employers choose to base their thinking around the old monitoring Act or the new monitoring Act, one element is common to both the old monitoring Act and the new monitoring Act, and to sections 5 and 6 of the new monitoring Act: The element of **employee consent**.

The best approach will always be to seek employee consent for the purposes of monitoring and interception. Once this consent has been obtained, issues relating to the right to privacy and compliance with the new monitoring Act largely fall away, save for the fact that the communication can only nevertheless be intercepted in the course of the carrying on of the business of the employer, and for one of the purposes mentioned in section 6, when the employer seeks to rely on section 6.

Therefore, the first prize for employers would be to obtain the written consent of employees. The second prize is that the employer should be able to demonstrate that “reasonable efforts” were taken to inform the employee that the employer will monitor email communications.

These would include the following:

1. All users being provided with an electronic copy of the company Monitoring Policy;
2. The employer informing employees that it intends monitoring electronic communications from time to time;
3. Making sure that this is brought to the attention of all employees;
4. Being able to demonstrate that the employees received the communication;
5. Requiring users to confirm that they have read and understand the Monitoring Policy each time they access the employer’s information systems;
6. Making this part of all new employee’s induction training; and
7. Reminding employees from time to time by way of “alerts” that their communications will be monitored.

Ultimately, the employer’s monitoring provisions must be both legally sound and reasonable, to balance the interests of both parties.

**For further information please contact:**

**Lance Michalson**

Tel: (021) 438-6323  
Fax: (011) 507-5284  
E-mail: [lance@michalson.com](mailto:lance@michalson.com)  
Web site: [www.michalson.com](http://www.michalson.com)

**Brendan Hughes**

(021) 438-6323  
(011) 507-5284  
[brendan@michalson.com](mailto:brendan@michalson.com)  
[www.michalson.com](http://www.michalson.com)