INTERCEPTION OF ELECTRONIC COMMUNICATIONS IN THE WORKPLACE

1 Introduction

The need to intercept and monitor communications arose in the context of security legislation. However, the use of e-mail and the Internet in the workplace has raised concerns about the privacy of employees' e-mail and web browsing activities. On the one hand, despite the fact that the employer's resources are being used, employees still have an expectation that there is some measure of privacy pertaining to their communications. On the other hand, information and communications technology in the workplace raises questions about the supervision of its use.

The Regulation of Interception of Communications and the Provision of Communication-related Information Act (70 of 2002 – "the RIC Act") has recently been enacted. The effect of this Act on interception of e-mail in the workplace has been the subject of a media flurry and differences of opinion amongst information technology (IT) lawyers. Owing to uncertainties flowing from this Act, it has yet to come into operation.

The aim of this note is to provide a cursory overview of the effect of the RIC Act on interception of e-mail in the workplace, to highlight the issues raised by the Act and to make recommendations on how some of these obstacles can be overcome.

2 Interception

The RIC Act has repealed the Prohibition of Interception and Monitoring Act (127 of 1992 – "the Prohibition of Interception Act") (see s 62 (1)). The Interception and Monitoring Bill followed the Prohibition of Interception Act, but was the subject of criticism and debate (see *eg*, Lawack-Davids "Interception and Monitoring Bill – Is Big Brother Watching?" 2001 *Obiter* 347). This led to the RIC Act, whose focus is slightly different from the Bill. The object of the RIC Act is to prohibit the intentional interception of any communication (both direct and indirect communications as defined in s 1 of the Act).

The word "intercept" is defined in the Act as "the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication". It includes the monitoring of any communication by means of a monitoring device, viewing, examination or inspection of the contents of any indirect communication and diversion of any indirect communication from its intended destination to any other destination. "Interception" has a corresponding meaning (s 1). Unlike its

predecessor, the RIC Act includes monitoring as part of interception. One could, therefore, monitor indirect communications as part of the interception process. The concept "indirect communications" is sufficiently wide to include e-mail and Internet browsing activities.

2 1 The prohibition

Section 2 contains a general prohibition. In terms of this section, no person may intentionally intercept or attempt to intercept, or authorise or 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. The general prohibition is similar to the prohibition contained in the Prohibition on Interception Act.

2 2 The exceptions

There are two exceptions to the prohibition in section 2 which have a bearing on electronic communications and interception in the workplace.

In terms of the first exception, any person other than a law enforcement officer may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception, unless the communication is intercepted by such person for purposes of committing an offence (see s 5(1)).

The second exception relates to interception of an indirect communication in connection with the carrying on of business. An indirect communication includes e-mail and Internet browsing activities (see the definition of "indirect communications" in s 1). The RIC Act provides that any person may, in the course of the carrying on of any business, intercept any communication in the course of its transmission over a telecommunication system. This indirect communication has to relate to one of the following:

- a transaction is entered into in the course of that business by means of such indirect communication;
- it otherwise relates to that business; or
- it otherwise takes place in the course of the carrying on of that business (see s 6(1)(a)-(c)).

In addition to the above, a person may only intercept an indirect communication if certain requirements are complied with. Firstly, such interception has to be effected by, or with the express or implied consent of, the system controller. A system controller refers to the chief executive officer or equivalent officer or a person who is acting as such, except in the case of the different spheres of government, where the designation is different (see the definition in s 1). Secondly, such interception has to occur for *specific purposes*, which are:

- for the monitoring or keeping a record of indirect communications
  - in order to establish the existence of facts,
  - for purposes of investigating or detecting the unauthorised use of that telecommunication system, or

  - where it is undertaken in order to secure, or as an inherent part of, the effective operation of the system; or
- monitoring indirect communications made to a confidential voice-telephony counselling or support service which is free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that users may remain anonymous if they so choose;
- if the telecommunication system concerned is provided for use wholly or partly in connection with that business; and
- if the system controller has made all reasonable efforts to inform in advance a person, who intends to use the telecommunication system concerned, that indirect communications transmitted by means thereof may be intercepted or if such indirect communication is intercepted with the express or implied consent of the person who uses that telecommunication system (s 6(2)(a)-(d)).

3 To consent or not?

Upon an analysis of the above provisions, IT lawyers have immediately highlighted the requirement of prior written consent as controversial. On the one hand, it is argued that it is absolutely essential for an employer to obtain the prior consent of its employee in writing before such employer may intercept the electronic communications such as e-mail or short messages (SMS's) of an employee. On the other hand, it is argued that the only time that such prior written consent is required is in section 5, where the employee as a party to the communication has to give such consent. As a result of this requirement in section 5, many IT lawyers have read the need for prior written consent into section 6. However, section 6 does not expressly require prior written consent. Clearly, if the employee has consented in advance, it can be taken that the system controller has made all reasonable efforts to inform in advance that indirect communications transmitted by means of a telecommunication system may be intercepted. Likewise, if written consent has been obtained, it will be viewed as interception with the express consent of the employee who uses the system (s 6(2)(d)).

Due to the varying interpretations and the resulting uncertainty, it is submitted that from a practical point of view, it would be advisable for an employer to obtain the prior written consent of all its employees who use its telecommunication system that their communications may be intercepted in accordance with an electronic communications or office communications policy. However, because such prior written consent is not required by section 6, it may happen that an employee refuses to give his/her consent. In such an instance, an employer has to have alternative means of ensuring that its system controller has made all reasonable efforts to inform in advance a person who intends to use the system that indirect communications transmitted by means thereof may be intercepted. This may entail a disclaimer or even a click-wrap agreement, which the employee has to accept before he/she is granted the use of the employer's telecommunication system. It has to be noted that the consent may also be obtained by electronic means, such as in the instance of a click-wrap

agreement, due to the legal recognition and enforceability afforded by the Electronic Communications and Transactions Act (25 of 2002 – see in this regard s 11).

4 An electronic communications policy

As alluded to above, in view of the uncertainties raised by the RIC Act, it is imperative that employers issue instructions on proper use of e-mail and the Internet by employees. It is evident that without instructions the proper use of e-mail and web browsing may not be clear in the workplace. Hence, good practice suggests that a solid electronic communications policy be in place that clearly stipulates permitted electronic communications conduct to employees. From an evidential point of view, it is by far the first prize.

It is submitted that such an electronic communications policy should deal, *inter alia*, with the following matters. Firstly, the employer has to describe authorised and unauthorised electronic communications conduct to employees. Secondly, the policy needs to stipulate the circumstances under which employees' e-mails may be intercepted, for example, as part of managing the system, for the establishment of facts (such as in disciplinary actions), investigations, problem-solving *etcetera*. Thirdly, the policy has to contain the manner in which interception will take place. If this is not included in the policy, it may be a good idea to have procedures in place which describe how administrators may intercept and also when administrators of the system may intercept. This can be done by establishing a panel, which decides on interception requests, in particular requests for interception for the establishment of facts or investigations. This is a means of protecting the system administrators, who can be assured that they intercept electronic communications subsequent to a valid request for interception and the employer, against potential vicarious liability. Likewise, the employee will know that interception took place subsequent to a proper procedure having been followed.

5 The effect of the Act on the individual employment relationship

5 1 Misconduct

It is apparent that section 5 of the RIC Act allows an employer to intercept a communication if one of the parties to the communication has given his or her prior written consent to such interception. As pointed out before, section 6 provides that any person may, in the course of carrying on of any business, intercept any indirect communication. This refers to communication in the process of moving through the Internet or employer's Intranet. In this latter instance an employer is required to make reasonable efforts to inform any employee that uses the employer's e-mail system that interception may take place, or obtain the consent of such an employee, expressly or impliedly.

Once consent is obtained, or the provisions of section 6 concerning the interception of indirect communication apply, the misuse of the Internet or

e-mail will constitute misconduct by the employee. A sprinkling of cases have emanated from the Commission for Conciliation, Mediation and Arbitration in this regard. In *WT Griffiths v VW* (EC16174 unreported) an employee was warned for visiting pornographic sites at work. Subsequently, he used the computer of a fellow employee and visited similar sites. He was dismissed for wilful disobedience. A CCMA Commissioner held that the dismissal was substantively fair. In *Cronje v Toyota Manufacturing* ([2001] 3 BALR 213 CCMA) the applicant was dismissed for distribution of racist and inflammatory material, violation of the company's internal policy and behaviour unbecoming of a manager. The applicant had forwarded a petition requesting President Mbeki to intervene in the Zimbabwe crisis to a number of colleagues. Attached to the petition was a derogatory cartoon depicting a gorilla with President Mugabe's head. The applicant also printed the cartoon and took it to a meeting to show colleagues. The Commissioner held that the cartoon was racist and inflammatory and concluded that the respondent had a fair reason to dismiss the applicant. This award was subsequently confirmed on review by the Labour Court (*Cronje v CCMA* [2002] BLLR 855 (LC)). In *Bamford v Energizer SA Ltd* ([2001] 12 BALR 1251(P)) a private arbitrator held that the dismissal of employees who had used company computers to receive and forward racist, sexist and pornographic material was substantively fair; and in *MWU obo Coetzer v Champions Casino* (unreported MP16821) the CCMA held that the dismissal of an employee for accessing the electronic mail of her superiors without their consent had been fair. (For a detailed discussion of these awards, see Modiba "Intercepting and Monitoring Employees' e-Mail Communications and Internet Access" 2003 *SA Merc LJ* 363 366-370; and Van Eck "Misuse of the Internet at the Workplace" 2001 *De Jure* 364 366-369).

To determine whether misuse of the Internet and e-mail will constitute misconduct and may warrant dismissal, Item 7 of the Code of Good Practice (Schedule 8 to the Labour Relations Act 1995) should be considered. This item reads as follows:

> "7. Guidelines in cases of dismissal for misconduct.
>
> Any person who is determining whether a dismissal for misconduct is unfair should consider
>
> (a) whether or not the employee contravened a rule or standard regulating conduct in, or of relevance to, the work-place; and
>
> (b) if a rule or standard was contravened, whether or not –
>
> (i) the rule was a valid or reasonable rule or standard;
>
> (ii) the employee was aware, or could reasonably be expected to have been aware, of the rule or standard;
>
> (iii) the rule or standard has been consistently applied by the employer; and
>
> (iv) dismissal is an appropriate sanction for the contravention of the rule or standard."

The guidelines relating to the existence of the rule and knowledge thereof are important to highlight regarding the misconduct involving misuse of Internet and e-mail.

Although certain types of misconduct relating to e-mail and Internet abuse will certainly be covered by other disciplinary rules, for example, continued use for private purposes despite a direct instruction not to do so (failure to obey a lawful instruction/insubordination – *Griffiths v VW* (*supra*)) or distributing racist material through e-mail (racist behaviour – *Cronje v Toyota Manufacturing* (*supra*)), a clear e-mail and Internet use policy should be adopted by employers. Rules regarding e-mail and Internet misconduct should be included in the policy. Policies of this sort may of course differ from employer to employer, on the nature of the Internet and e-mail use, the employer's own view of what constitutes misconduct in this regard, as well as the business of the employer. Certain employers may allow for instance reasonable private use, whilst others prohibit such use altogether. The requirement is that there should exist not only clear, but also legitimate, rules.

It must be remembered that the legitimacy of a rule may be evaluated by an arbitrator in the instance of dismissal for misconduct or the imposition of a lesser sanction for misconduct. Petty rules, or rules contrary to employees' Constitutional rights, may accordingly be set aside as being illegitimate.

A policy containing rules also needs to be clearly communicated to employees in order to meet the requirement of knowledge of the rule. This can be done by providing workshops on the policy, requiring employees to acknowledge receipt thereof, posting the policy on notice boards and periodically reminding them of the policy (see the discussion by Modiba 2003 *SA Merc LJ* 370-371 in this regard).

5 2 Obtaining an Employee's Consent

In terms of section 5 of the Act, communication may be intercepted if prior consent such interception is given in writing by one of the parties to the communication. The question arises as to what the consequences are if an employee refuses to give consent. It may be argued that it is operationally necessary for an employer to intercept communications by e-mail and Internet use of employees. Employees who refuse to give consent may accordingly be dismissed for operational reasons and, provided section 189 of the Labour Relations Act 1995 ("the LRA") is complied with, such dismissal will be fair. The Labour Court has recognised that an employer may fairly retrench employees who refuse to accede to changes in their conditions of employment (*Entertainment Catering Commercial & Allied Workers Union of SA v Shoprite Checkers* 2000 21 *ILJ* 1347 1351). Alternatively, proposed changes to terms and conditions of employment can be classified as an interest dispute. This includes the proposed condition of employment that an employer may intercept e-mail and Internet communications. In terms of the LRA, interest disputes are to be resolved through the collective bargaining process. In appropriate circumstances and upon compliance with the prescribed procedure (s 64 of the LRA), the use of force in the form of a lock-out can possibly be resorted to by the employer with a view to compelling employees to accede to giving the consent required. It must be noted that a lock-out is utilised in a collective bargaining

context, and that the Act requires the consent of each employee. Whether an individual employee can be locked out, is a moot point.

It will, however, be impermissible for an employer to dismiss an employee refusing to give consent coupled with the promise of reinstatement or reemployment if the employee gives the consent. Such a dismissal will be unfair in terms of section 187(1) of the LRA which provides that a dismissal is automatically unfair if the reason for the dismissal is to "compel the employee to accept a demand in respect of any matter of mutual interest between the employer and employee". Since the promulgation of the LRA, the so-called dismissal lock-out is no longer a lawful option for employers to effect changes to conditions of employment (the 1956 LRA allowed for a dismissal lock-out).

6 Conclusion

It is submitted that there is a need for employers to intercept the electronic communications and web browsing activities of their employees. It has been argued above that it would stand employers in good stead to have a good awareness campaign to obtain the buy-in of employees before they consent to their electronic communications being intercepted. From a labour law perspective there are pitfalls in the obtaining of consent and employees and employers need to be aware of the possible consequences of not consenting, and the methods of obtaining consent lawfully. The importance of implementation of a policy which includes clear and legitimate rules regarding Internet and e-mail use should not be underestimated. It is imperative that interception takes place circumspectly and in accordance with rules and procedures, for the protection of all the parties concerned.

Vivienne Lawack-Davids
Research Fellow: Unisa
and
Adriaan van der Walt
Nelson Mandela Metropolitan University, Port Elizabeth