Course Code:	**CML628F**
Course Name:	**ELECTRONIC LAW 2**
Topic:	**The monitoring of e-mail and Internet usage in the South African workplace - The final word**
Date:	**15 SEPTEMBER 2003**
Name:	**STEVEN FERGUSON (FRGSTE002)**
Telephone No.:	**465 9175**

A. INTRODUCTION

A.1. EXECUTIVE SUMMARY

Electronic communication tools are fast becoming the norm in most modern businesses. However, employers encounter a number of risks when they provide e-mail and Internet facilities to their employees. To combat against these risks, and for a number of other legitimate reasons, more and more employers are introducing new methods of electronic monitoring to regulate computer use in the workplace.

Monitoring refers to a range of activities whereby an employer sets out to collect information on their employees by keeping them under some form of observation. Although such activities are generally invasive by nature, they have been recognised in many instances as a necessary component of the employment relationship. At the same time, South Africa and other jurisdictions have recognised that employees have a legitimate expectation to a certain degree of privacy in their working lives, including the right not to have the privacy of their communications infringed. This paper will examine how and when electronic monitoring activities conducted by employers can be justified even when they result in a factual infringement of the employee's right to privacy.

The monitoring of electronic communications may also involve an unlawful "interception" in terms of our law. With the imminent introduction of the **Regulation of Interception of Communications and Provision of Communication Related Information Act of 2002 (RICA)**[1], intercepting indirect communications (such as e-mail) without consent may result in criminal liability for the interceptor.

[1] Act 70 of 2002, signed on 30 December 2002

The application of the new act to the field of employment has sparked a great deal of media attention and debate amongst businesses, government and IT lawyers. Despite the Act including a number of exceptions, some experts have argued that the only way in which employers can comfortably avoid liability in terms of RICA is by obtaining their employee's prior written consent to be monitored. As a result, many employers and employees are now uncertain of what is and is not permitted when it comes to the monitoring of e-mail and Internet usage in the workplace.

I will seek to clarify some of these issues by examining the applicable provisions of RICA in detail and comparing it to similar legislation in the United States and the United Kingdom.

When monitoring also results in the recording and use of an employee's personal information, issues of data protection and information privacy will also become relevant. South Africa does not currently have any specific privacy or data protection legislation; however the issue is currently being addressed by the South African Law Commission.[2] In the meantime, employers will be guided by certain provisions in other legislation, as well as by international data protection law. Valuable assistance can be gained from three new codes of practice on the issue of electronic monitoring which have been introduced in the EU, United Kingdom and Hong Kong over the past year.

Finally, the paper will provide some practical advice and recommendations to employers who currently, or intend to, monitor their employee's e-mail and internet usage. By adopting a best practice approach, employers will not only be able to legitimately protect themselves against the risks involved, but also maintain a relationship of trust with their employees.

---

[2] The SALC is presently conducting an investigation entitled "Privacy and Data Protection" (Project 124) with a view to developing privacy legislation in South Africa in line with international trends. The process began in July 2002 and is expected to take 3-4 years to complete. The Commission has recently released an Issue Paper which unfortunately does not adequately deal with workplace monitoring.

A.2 MONITORING E-MAIL AND INTERNET USAGE

A.2.1 The evolution of workplace monitoring

Monitoring the behaviour, work processes and correspondence of employees has long been accepted as a component of many employment relationships.[3] The traditional methods of supervision adopted by employers typically involve human intervention and usually target specific individuals suspected of some form of workplace misconduct. Now with the development of "spy ware" technology, employers are able to affordably monitor their entire workplace in new, sophisticated ways.[4]

Automated or electronic surveillance may include telephone monitoring or video surveillance using CCTV (closed circuit television). For the purposes of this paper, I will focus on the monitoring of employees' computer activities, particularly e-mail and Internet usage.[5]

A.2.2 The different levels of monitoring

Monitoring in the workplace can be implemented in varying degrees of intensity. **Continuous** or **systematic** monitoring takes place over an undefined period of time and will usually involve the whole or a large section of the workforce. The use of firewall software to scan all e-mail traffic over an employer's information system would be an example of systematic monitoring.[6]

---

[3] The Employment Practices Data Protection Code, Part 3: Monitoring at work, UK Information Commissioner (The UK Code), found at www.dataprotection.gov.uk/dpr/dpdoc.nsf at p.12

[4] See the Privacy Foundation's July 2001 study, titled "The Extent of Systematic Monitoring of Employee E-mail and Internet Use, at http://www.sonic.net/-undoc/extent.htm.

[5] According to the American Management Association's widely publicised report, 78% of companies in the US use some type of surveillance in their workplace, 36% of which involves storing and reviewing computer files.

[6] The UK Code at p.13

Once-off or **occasional** monitoring may also be utilised, usually as a short term measure in response to a particular problem or need, such as monitoring the e-mails of an employee suspected of sexual harassment. This form of monitoring is often implemented after an employer has already conducted certain preliminary investigations.

Many new forms of electronic monitoring may go undetected without employees ever being aware that it has taken place. **Covert monitoring** is often used to gather evidence where there is a very real suspicion of misconduct or criminal activity in the workplace and where notification to the relevant employee/s would prejudice the investigation.

The impact of any monitoring activity will often involve the particular context, however it is generally accepted that continuous and covert monitoring are seen to be more invasive and require closer regulation.

A.2.3 E-mail – the smoking gun of the information age[7]

E-mail as a form of communication is unmatched for speed and efficiency. It is inexpensive and can reach anyone across the globe. Simple messages can be sent with a large variety of multimedia attachments, including music, photos and video clips. E-mail allows businesses to share more information in their workplace than ever before, and communicating with clients has never been this easy.

However, e-mail can also impose a number of serious risks and obligations on employers who provide such facilities. Multimedia file attachments can bleed a company's bandwidth; employees can leak sensitive or confidential information; illegal or unacceptable content can be attributed to the employer; contracts can

[7] Barbara Weil Gall, "Company E-mail and Internet Policies" found at http://www.gigalaw.com/articles/2000/gall

inadvertently be concluded and viruses can be introduced causing severe loss. It is beyond the scope of this paper to examine all of these risks in detail, save to say that any company, regardless of its size, can be plunged into financial ruin as a result of e-mail or Internet abuse by their employees.

Personal use of work e-mail facilities will not usually result in any added overheads for an employer. Most businesses have moved away from dial-up accounts and are now using mail servers and fixed leased lines. An increase in the volume of e-mail and internet traffic will not result in any incremental increase in the costs associated with such facilities.[8] Employees faced with charges of e-mail or Internet abuse have argued that because there are no direct cost implications for the employer their personal use of such facilities can be justified. However it is generally accepted that there are a number of substantial indirect costs associated with personal e-mail and internet usage, including decreased productivity and bandwidth wastage.

The question is often asked why many employees feel entitled to use their work e-mail facilities for their own personal use. "PC" stands for *personal* computer and many employees feel a sense of proprietorship over their workstations, even though it has been bought and paid for by their employer.[9] Attitudes towards computers are very often formed in the home before they are formed in the workplace.

A.2.4 Different types of electronic communications

It is important to note that different types of communication are transmitted over an employer's information system at any given time. Employers who provide e-mail and Internet use to their employees are primarily seeking to enhance

[8] L Michaelson, "E-mail and internet usage in the workplace"

[9] The issue of ownership of the computer facilities on which an employee works has been used by the US courts to grant a greater degree of latitude to employers who wish to monitor their employees' online activities.

productivity and the overall efficiency of the way they do business. It is therefore fair to assume that the majority of traffic on the employer's system will be for legitimate business or related purposes. **(Pure business communications)**

Although it is slightly unrealistic and would not make prudent business sense, an employer can place a complete ban on the personal use of e-mail and the Internet by his employees. However, it is more commonplace for employers to allow a limited amount of personal use. The sheer speed and ease of e-mail allows an employee to have the equivalent of a real-time conversation with friends and family without leaving their desk. Employees are also able to use the Internet to conduct a number of their personal affairs quickly and effectively, such as Internet banking. There are certain obvious advantages for an employer whose employees are organised and happy. **(Pure personal communications)**

In a number of the reported instances of e-mail abuse, the relevant messages contain material generated by unknown persons and which are merely forwarded by the employee to other members on their own mailing list. These e-mails, which include chain letters, jokes and picture parodies, are neither business related nor are they purely personal. **(Non-business communications)**

Finally, there are those business related communications that also include certain personal information pertaining to an employee or third party. E-mail correspondence between an employee and his HR manager regarding a medical condition would be a prime example. Employees, in building good relationships with clients and staff from other organisations, may also include certain personal information in their correspondence with such parties and visa versa. **(Partly personal partly business communications)**

It is important when seeking to regulate the use of e-mail and Internet facilities, that the nature of the communications transmitted over the employer's information system is considered carefully.

A.2.5 Legitimate reasons for monitoring e-mail and Internet usage

Although the sharp increase in monitoring activities may be disconcerting for many employees, there are a number of legitimate reasons for employers to carry them out. I have already mentioned some of the risks associated with e-mail usage by employees and employers obviously need to take steps to avoid any loss that can arise from abuse. Losses may include direct financial, reputation or physical loss, or indirect loss associated with vicarious liability.

There are also other reasons for such activities that go beyond risk management. With the introduction of the **Electronic Communications and Transactions Act**[10] last year, "data messages" (including e-mail) have now been given the same legal weight as paper-based communications. E-mails may now be used as evidence in litigation or to prove the conclusion of a contract. Sound document management practices will need to be implemented by a business that conducts much of its business electronically. Introducing automated monitoring systems will ensure that important e-mails are accessible and retained in a secure manner.

As the trend of globalisation continues to influence our economy, many South African businesses will also have subsidiaries in other countries or will themselves be a branch of an international company. Although still a relatively new concept in South Africa, data protection is taken very seriously in other jurisdictions, especially Europe. Businesses seeking to participate in this market will need to ensure that they have an "adequate" standard for protecting personal information. Keeping information secure and free from corruption by viruses or human intervention is an important principle of data protection and electronic monitoring systems will be indispensable in this regard.

---

[10] Act 25 of 2002 ("ECT Act")

A.2.6 Illegitimate reasons

The International Labour Organisation (ILO) has recognised that there may be no other social situation where such a large amount of personal information can be gathered from an individual than in the employment arena.[11] With the advent of more sophisticated monitoring methods, employers are now able to collect even more information about their employees. The organisation has also identified the threat that, once employers have sufficient information on their employees, they will use it to influence and even manipulate the employee's behaviour.

Once collected, employee information can be used for a number of purposes including, as evidence in disciplinary action, for performance evaluations, or to be sold to external third parties such as market researchers, banks or other financial institutions.

A.2.7 The technology used[12]

There are a number of different methods of automated or electronic monitoring systems that are used by employers to monitor e-mail and Internet use in the workplace. Affordable technology, such as packet sniffers, filtering software or desktop monitoring tools are now available to employers on a large scale.

Employers don't even need to invest in additional software to track their employees' computer use. Every computer leaves audit trails in the form of log files that provide evidence of what activities have been conducted on a particular work station. System administrators can use log files to determine what web sites have been visited or to monitor e-mail traffic simply by gaining access to the employee's computer. It is also important to note that information can be

[11] Preamble to the ILO's Code of Practice
[12] see K. Bonsor's article "How Workplace Surveillance Works", found at http://computer.howstuffworks.com/workplace-surveillance.htm

accessed even after it has been deleted. Many employees believe that by deleting their e-mails, they erase the trail.

In the wake of the recent identity theft debacle involving ABSA, the public have become more aware of "spy ware" technology such as key loggers. However it is not fully appreciated that many of these surveillance methods are also being used by employers to great effect. Although the extent of such use has not been measured in South Africa, it would be fair to say a great number of employees would be "un-pleasantly" surprised.

If employees were made more aware of the technology and how it works, I believe the rate of abuse would fall drastically. It is also crucial that employees are educated in the risks and costs associated with e-mail and Internet abuse. The importance of educating and training should therefore be highlighted even before any legal safeguards are considered.

A.3 THE RIGHTS OF EMPLOYEES THREATENED BY WORKPLACE MONITORING

A.3.1 The employee's right to privacy

Monitoring is invasive and will usually result in a factual infringement of an employee's right to privacy. The focus of this paper will be on how far such factual infringements can go before they become unlawful. In examining the present legal framework in South Africa for regulating the monitoring of e-mail and Internet usage in the workplace, a great deal of emphasis will be placed on the employee's constitutional and common law right to privacy, particularly their right not to have the privacy of their communications infringed.

A.3.2 The employee's right to enjoy fair labour practices

Monitoring in the workplace may also have certain labour law implications. Section 23 of the Constitution provides that "*everyone has the right to fair labour practices*". Effect has been given to this constitutional right in the **Labour Relations Act**[13] and electronic monitoring may constitute an unfair labour practice in a number of instances.

Employers may be obliged by existing collective agreements to consult with workplace forums or unions before introducing and/or implementing any monitoring activities into the workplace. Although these labour aspects will not be dealt with in this discussion, they need to be taken into account by employers when monitoring their employee's e-mail and Internet usage.

[13] Act 66 of 1995

B. THE RIGHT TO PRIVACY IN THE SOUTH AFRICAN WORKPLACE

B.1 THE CONSTITUTIONAL RIGHT TO PRIVACY IN THE WORKPLACE

B.1.1 Section 14 - the right to privacy

Section 14 of the Constitution recognises the right to privacy as an independent fundamental human right. The section has two parts; the first guarantees a general right to privacy and the second protects against specific infringements of privacy, including the right not to have the privacy of one's communications infringed.[14] Section 14(d) is directly relevant to the issue of monitoring employee e-mail and Internet use.

Defining the scope and substance of the right to privacy is not always easy and will depend on the particular context in which it is applied. It becomes even more problematic when the right is not adequately dealt with in a constitutional text or is described in abstract terms, as is the case in the US. The inclusion of section 14(d) in our Constitution is to be welcomed and will make the right to privacy a lot easier to interpret and apply when discussing workplace monitoring.

In **Bernstein and Others v Bester NO and Others**[15], it was held that the scope of a person's constitutional right to privacy extends only to aspects of his life or to conduct in regard to which he has a legitimate expectation of privacy. A

---

[14] s 14 reads:
"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; or
d) the privacy of their communications infringed."
[15] 1996 (4) BCLR 449 (CC)

legitimate expectation means that one must have a subjective expectation that society recognises as objectively reasonable.

Ackermann J's comments on the relative nature of the right to privacy is particularly relevant to the protection afforded it in the employment arena. He stated at 789 that:

"*A very high level of protection is given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions and there is a final untouchable sphere of human freedom that is beyond interference from any public authority.*"

He goes on to say that:

"*In the context of privacy, this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment which is shielded from erosion by conflicting rights of the community*"

"*..... But this most intimate core is narrowly construed. This inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual's activities then acquire a social dimension and the right to privacy in this context becomes subject to limitation.*" [16]

The **Bernstein** judgment confirms that an individual's right to privacy is not absolute and will be limited when the individual leaves their "inner sanctum". The judgment also implies that an employee cannot expect a great deal of privacy when he or she leaves their home to enter the doors of the workplace. Similar arguments have been made in other jurisdictions against an individual's right to privacy extending beyond their home and family life.

---

[16] ibid at 788-789

However, the right to establish and maintain relations with other human beings has been recognised as an integral part of the right to privacy. In **Investigating Directorate: Serious Economic Offences and Others v Hyandai Motor Distributors (Pty) Ltd and Others v Smit NO and Others**[17], Langa DP pointed out that:

"The right (to privacy) however does not relate solely to the individual within his or her intimate space. Ackermann J did not state in the above passage that when we move beyond this established "intimate core", we no longer retain a right to privacy in the social capacities in which we act. Thus, when people are in their offices (own emphasis), in their cars or on mobile telephones, they still retain the right to be left alone by the State unless certain conditions are satisfied."

This approach corresponds with the stance taken by the European Court of Human Rights when interpreting the right to privacy contained in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[18]. In **Niemitz v Germany**, the court made it clear that the protection of "private life", as envisaged by Article 8, does not exclude the professional life of an employee and is not limited to life within the home. The Court stated that:

"Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears to be no reason in principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a

---

[17] 2000 (10) BCLR 1079 (CC)

[18] Article 8 states that:

1. Everyone has the right to respect for his private and family life, his home and correspondence.
2. There shall be no inference with the exercise of this right except such as is in accordance with law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others.

significant if not the greatest opportunity of developing relationships with the outside world."[19]

This interpretation was also confirmed in **Halford v The United Kingdom**[20] where the interception of worker's telephone calls was held to constitute an infringement of Article 8. The government's argument that telephone calls made from the workplace fell outside the protection of Article 8 was rejected by the court.

It would therefore appear that our law now recognises that an individual's constitutional right to privacy extends beyond the home into the workplace. However, this right is not absolute and can be limited by the rights or legitimate interests of others, including those of their employer.[21] I have already mentioned that an employer has a number of legitimate interests that are advanced through electronic monitoring. The question is therefore not whether an employee's right to privacy in the workplace can be infringed, but rather to what extent it can be limited.

B.1.2 Limitation of the constitutional right to privacy

Section 36 of the Constitution, i.e. the so-called limitation clause, is important in determining when inroads can be made into fundamental rights contained in the Bill of Rights. The test applied is whether the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors. The relevant factors will include:

a) <u>The nature of the right</u>

---

[19] 23 November 1992, Series A no. 251/B at para. 29
[20] 27 May 1997
[21] See Neethling **Persoonlikheidsreg** at 288ff

It is difficult to clarify with any degree of certainty what the nature of an employee's right to privacy will be in the workplace. It is clear from section 14(d) of the Constitution that it includes the right not to have the privacy of one's communications infringed. Much will depend on the individual circumstances of each case; the nature of the particular employment relationship and workplace; and the legitimate expectations of the employee.

Certain rights contained in the Constitution are also more fundamental than others. For example, the infringement of the right not to have the privacy of one's communications infringed will be more easily justified that an infringement of the employee's human dignity.

Employers also have constitutionally protected rights in respect of their own businesses which may justify an invasion of their employees' right to privacy. However it has been argued that an employee's personal rights will usually override the employer's economic rights.[22].

b) The importance of the purpose of the limitation

The legitimate reasons or purpose for electronic monitoring may also vary in importance. It has been accepted that electronic monitoring is an integral part of any modern IT security strategy and that the employer's interest in securing the efficient operation of their information system against viruses and hackers will override the employee's right to privacy.

c) The nature and extent of the limitation

I have already mentioned that monitoring may take various forms with varying intensity. Covert and continuous monitoring is particularly invasive and may not

[22] **Moonsamy v The Mailhouse**, 1999 20 ILJ 464 (CCMA) at 471

be justified in terms of the provisions of section 36, unless there are alternative grounds for allowing it to take place.

d) The relation between the limitation and its purpose

Any determination as to whether a limitation of the employee's right to privacy is justified will involve an impact assessment based on proportionality whereby the purpose of the activity is weighed against any adverse impact it may have on employees or third parties.

e) Any less restrictive means to achieve the purpose

There may also be a number of alternatives to monitoring that will satisfy the employer's legitimate interests without limiting the employee's right to privacy. For example, monitoring traffic data instead of content to identify the cause of bandwidth wastage will be less restrictive.

B.1.3 Application of the Constitution to disputes concerning electronic monitoring

B1.3.1 Horizontal Application

Traditionally, a bill of rights regulates the relationship between the state and its individual citizens (vertical application). However our Bill of Rights goes further in that it also recognises that private abuse of human rights may be carried out between natural and juristic persons.

Section 8(2) of the Constitution, which deals with the horizontal application of the Bill of Rights, states that:

"a provision of the Bill of Rights binds a natural or a juristic person if, and to the extent that, it is applicable, taking into account the nature of the right and the nature of any duty imposed by the right."

Although there will not be any direct constitutional recourse for an employee against a private employer, the Bill of Rights may still apply to any dispute between them in one of the following ways:

a) Where a right contained in the Bill of Rights has been given further effect to by the Legislature, the courts will interpret the provisions of the legislation generously to give effect to the constitutional right in question.[23]

   In the case of the interception of electronic communications, section 2 of RICA has been introduced to give effect to section 14(d) of the Constitution. When determining the lawfulness of any interception of an employee's e-mail, the court will first apply the provisions of RICA and, if necessary, interpret its provisions generously to give effect to section 14.

b) Where no further legislation has been introduced, the courts themselves must give effect to the right in question by applying and developing the common law in line with the Bill of Rights. This will also include highlighting the circumstances in which a fundamental right can be limited by applying the provisions of section 36 of the Constitution.[24]

   The Bill of Rights will therefore be useful in adding content to vague and open-ended common law concepts such as "reasonableness" or the "legal convictions of the community", which are particularly relevant when determining the scope of an employee's right to privacy in the workplace.

---

[23] De Waal *et al* at p57-58
[24] ibid

c) The Constitution will never override the ordinary law but rather demands furtherance of its values through the operation of the ordinary law. Section 39(2) states that:

"When interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and object of the Bill of Rights."

B.1.3.2 Vertical Application

The Constitution will apply directly to any dispute involving the State and a private individual. Where an employer is prosecuted under section 2 of RICA, he or she will be entitled to argue their defence on constitutional grounds. They may allege that the relevant provision of the Act is unconstitutional, or that the interception is justified on the grounds set out in section 36.

The Constitution may also apply directly to disputes between public employees and the State.

B.1.4 Can an employee's constitutional right to privacy be waived?

It has been argued that obtaining an employee's consent to be monitored will render such activities lawful despite the fact that they may constitute an invasion of the employee's right to privacy. The issue of whether an employee can agree in his or her employment contract to waive their constitutional right to privacy in the work place is a difficult one.

What is settled is that parties cannot waive the application of the Bill of Rights to any law that may govern any future dispute between them. An employee can therefore not prevent the provisions of section 14 and the spirit of the Bill of

Rights in general from being applied by a forum hearing a dispute concerning the interception or monitoring of an employee's e-mails.

Individuals may however waive their right to exercise a fundamental right, provided that they do so freely and clearly without being placed under duress or misapprehension.[25] It will be argued later that this will be problematic when applied to the employment relationship. Such a waiver may also influence the enquiry in terms of section 36, or the remedy awarded for the violation of the right.

The nature of the right in question is also important. An employee may waive his rights in terms of section 14(d), but cannot waive his right to human dignity. An employee may consent to his e-mails being monitored; however he will be held not to have consented to the monitoring takes place in a manner so invasive that it infringes his dignity.

B.2 THE COMMON LAW RIGHT TO PRIVACY IN THE WORKPLACE

B.2.1 Delictual liability for privacy infringements

The same considerations that led to the entrenchment of the right to privacy in the Bill of Rights have been recognised by our common law for a long time. Privacy was initially seen as part of a person's *dignitas* but has since asserted itself as an independent personality right in our common law. The jurisprudence of the courts on the standards of reasonableness and the legal convictions of the community will inform the scope and substance to be given to the common law right to privacy in any particular context, including the workplace.

---

[25] **Tettey v Minister of Home Affairs** 1999 (1) BCLR 68(D) at 74I-75A

An infringement of the right to privacy at common law will be actionable through the *actio iniuriarum.* To succeed with such an action, an employee must prove that a factual infringement of their right to privacy is wrongful and was conducted with the necessary intent on the part of the employer.

The question of wrongfulness is decided by way of the subjective-objective test mentioned above, i.e. the employee must have a subjective expectation of a right to privacy which is objectively reasonable. In determining whether an expectation of privacy is reasonable, the current modes of thought and values of the community (the *boni mores)* will be important. The courts may be influenced by the provisions of RICA, the ECT Act and PROATIA as well as by section 14 of the Constitution.

An employer who wrongfully infringes his employees' right to privacy must also do so intentionally. He must direct his will to violating the privacy of the employee in question while knowing that such violation would be wrongful. *Animus iniuriandi* is presumed as soon as wrongful infringement of privacy has been proved. It will therefore be up to the employer to convince the court that he did so unintentionally.[26]

B.2.2 Common law defences

There are a number of common law defences to the action for invasion of privacy that may be relevant to workplace monitoring. Such defences may include consent, necessity, public interest or performance of a statutory or official capacity. For our purposes, I will focus on consent and necessity:

a) Consent

[26] see Neethling **Persoonlikheidsreg** p268 -269

It has been accepted by our courts that a person may consent to an infringement of their common law right to privacy, provided that such consent is given freely and voluntarily. The giving of consent should also not be *contra bonos mores*. Consent is a unilateral act and can therefore be revoked at any time. It has been argued by certain commentators that consent is invalid if it is set as a condition of employment or for the continuance of an employment contract.[27] More will be said later on the issue of consent in the employment context.

b) Necessity

In order to protect, further or maintain a certain interest, it is often necessary for other individuals or organisations to infringe the privacy rights of another. The legitimate interests an employer has for conducting e-mail and Internet monitoring may constitute adequate grounds for a defence of necessity under the common law.

In order to avoid liability, the interest in question must be a legitimate one that is recognised by law as such. It is therefore necessary for the purpose of any monitoring activity to be identified and defined so that the court may determine whether that purpose can be served by other means.

Even where the privacy infringement advances the legitimate interests of another, it must still be carried out in a reasonable manner. In other words, the monitoring activity should not be carried out for longer than is necessary and should cease when the identified purpose has been served. Anything beyond the boundaries of what is deemed necessary will result in the activity once again being regarded as wrongful.

B.3 CONCLUSION

[27] see Neethling at 329-330

The right to privacy has long been recognised in our common law as an independent personality right and its importance has been confirmed by its inclusion as a fundamental right in the Bill of Rights. Defining the right in precise terms is problematic and much will depend on the context in which it is applied. For the purposes of this discussion and in the context of workplace monitoring, it has been held to include the right of an individual to pursue social relationships with others and the right not to have the privacy of one's communications infringed.

An employee's right to privacy is not absolute and can be limited by the rights and legitimate interests of their employer. Whether one is considering the element of wrongfulness under the common law, or determining the extent to which the constitutional right can be limited, the same test must be applied – does the employee have a subjective expectation of a right to privacy which is objectively reasonable?

An employee's subjective expectation of a right to privacy will be curtailed if he or she has consented to workplace monitoring in their employment contract. It is important to remember that such consent must be fully informed and freely given, which will not always be apparent in the employment context. It will be argued that consent alone is not sufficient to justify an employer monitoring his employees' e-mail and Internet usage.

In determining objective reasonableness, the legal convictions of the community or the *boni mores* will inform both the Constitution and the common law. A number of factors will be applied, including those listed in section 36 of the Constitution. In the absence of judicial precedent on the issue, further assistance can be obtained from other legislation, particularly RICA, and from comparative international law. What is important for employers is that the same considerations that are applied to this enquiry can also be used by them to shape best practice for monitoring e-mail and Internet use.

C. THE REGULATION OF INTERCEPTION OF COMMUNICATIONS ACT OF 2002 (RICA)

C.1 INTRODUCTION

The new "Interception" legislation was signed by the State President on 30 December 2002[28] and has sparked a great deal of debate amongst business, legal experts and privacy advocates. Although the majority of its provisions regulate the interception of communications by law enforcement agencies, the Act will also have an important effect on private employers.

The provisions of RICA dealing with "private interceptions" bear a number of similarities to the UK's **Regulation of Investigatory Powers Act 2000**[29] (read together with the **Telecommunications (Lawful Business Practice) (Interception of communications) Regulations**[30]) and the US **Electronic Communications Privacy Act of 1986.**[31] It will be useful, when interpreting RICA, to compare it to both these Acts.

It is also important to note the background to the new Act when interpreting its provisions. In the wake of the September 11 terrorist attacks in the United States, there has been a growing sense of paranoia among governments around the world that the Internet and e-mail will be used to great effect by criminals and terrorists to plan and orchestrate further crimes. Due to the rapid rate at which the technology develops, together with the proportionate decrease in the costs thereof, the main concern has been that law enforcement agencies will no longer

---

[28] The government has not yet brought the Act into operation pending the introduction of the Council of Europe's new Convention on Cybercrime. If the new Convention is ratified, the government must ensure that the provisions of RICA and other legislation are in line with the measures adopted therein.
[29] at www.hmso.gov.uk/acts/acts2000
[30] at www.hmso.gov.uk/si/si2000
[31] 18 USC, found at http://www.law.cornell.edu:80/uscode/18/ch119.html>

be able to effectively combat such crime and terrorism. As a result, most countries have now "beefed up" their legislation dealing with the investigative powers of law enforcement agencies, including their ability to intercept communications between citizens.[32]

In response to a call from the South African government for an amendment to be made to the 1992 Interception Act, the SALC conducted a preliminary investigation culminating in a discussion paper and a proposed draft bill.[33] It is apparent from the SALC's report and from the contents of the new Act itself that its main purpose is to provide better interception capabilities for law enforcement agencies. What is also important is that the SALC did not expressly deal with the issue of interception and monitoring for business related purposes.

The new Act also differs quite substantially from previous drafts. Changes include a much wider prohibition against interception without consent in section 2, the exceptions, and the introduction of hefty criminal penalties that may be imposed on transgressors. It is not apparent from the process leading up to the signing of the new Act when the legislature decided to implement these changes and the reasoning behind them. I would suggest that the Legislature has reviewed similar provisions in other jurisdictions and decided to incorporate them into the new Act.

C.2 THE AMBIT OF RICA

Section 2 of RICA states that:

"*Subject to this Act, no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at*

---

[32] Epic and Privacy International's **Privacy and Human Rights 2002, An International Survey of Privacy Laws and Developments** at p. 20
[33] Project 105

any place in the Republic, any communication in the course of its occurrence or transmission."

The Legislature has created a statutory offence (or offences) from the constitutional right contained in section 14(d) of the Bill of Rights. Persons found guilty of contravening section 2 will now attract heavy criminal penalties.[34] Certain experts have advised employers that the best way to avoid incurring criminal liability in terms of RICA is to obtain their employee's prior written consent before embarking on any monitoring activity (as per section 5 of the Act).

Many employers not only see this option as a costly administrative and logistical exercise, but also believe that they should not be hamstrung by the choices made by their employees in matters involving their managerial prerogative. [35] I do not believe that RICA will affect the legality of monitoring e-mail and Internet usage as much as has been initially reported. I have two reasons for stating this:

a) On a closer inspection of the wording of section 2, read together with the definition section contained in section 1, it is possible to limit the general prohibition against monitoring without consent in a number of respects; and

b) The "business exception" contained in section 6, together with some of the other exceptions included in the Act, will exclude most forms of electronic monitoring from falling foul of the Act.

C.2.1 Limitation of the general prohibition against interception (section 2)

C.2.1.1 has there been an interception?

[34] Fines of up to R 2 million and/or 10 years imprisonment
[35] The "cost to business" argument has been the cause of much debate in the US Congress regarding new proposed privacy legislation.

"Interception" is broadly defined in section 1 of the Act to include

"*any activity that allows for the 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.*"

The definition goes on to list certain activities that will be regarded as interception for the purposes of the Act, including:

(i) the *monitoring* of any communication by means of a monitoring device;
(ii) viewing, examination or inspection of the contents of any *indirect communication*; and/or
(iii) diverting any *indirect communication* from its intended destination to any other destination.

"Monitoring" includes listening to or recording communications. This definition appears to relate mainly to aural interceptions, (i.e. of telephone calls) and should not be confused with the use of the term in the general sense to denote any activity where the conduct or activities of employees are observed.

E-mails and browser enquiries sent from a modem will constitute indirect communications in terms of RICA. Any activity conducted by an employer whereby he or she views, examines or inspects the contents of any indirect communication will constitute an interception. In the case of e-mails, this would appear to imply that the mail must be opened before it can be deemed to have been intercepted.

The Act also refers to the diversion of indirect communications from their intended destination to any other destination. It has been argued that this would

include any firewall or other forms of filtering software found in most modern businesses using e-mail and Internet facilities. This cannot have been the intention of the Legislature and I will argue that automated monitoring systems will fall outside the ambit of the Act for a number of reasons.

C.2.1.2 Real time vs. stored communications

Section 2 prohibits the interception of any communication *during the course of its occurrence or transmission*. Section 1(2) states further that the time during which an indirect communication is being transmitted will include any time when the communication is temporarily stored to enable the intended recipient to collect it or otherwise have access to it at a later stage.

In determining when a communication is in the course of transmission, the provisions of the ECT Act relating to the origination and receipt of data messages may also be useful. Section 23 of the ECT Act states that:

"A data message
a) … must be regarded as having been sent by the originator when it enters an information system outside the control of the originator or, if the originator and addressee are in the same information system, when it is capable of being retrieved by the addressee.

b)… must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee."

I submit that a communication is in the course of transmission up to and including the moment it is collected, opened and read by the intended recipient. Accessing

a stored collection of e-mails received and opened, or a stored collection of sent items will not constitute an unlawful interception in terms of the Act.

The US's **Electronic Communications Privacy Act of 1986** (ECPA), which amended the Federal Wiretap Act to include electronic communications, sets out certain prohibitions against intercepting and accessing communications and provides certain privacy protections. ECPA is divided into Title I and Title II. Title I prohibits the interception and disclosure of wire, oral or electronic communications. Title II goes one step further and prohibits the accessing of stored electronic communications.

In the absence of similar specific provisions in RICA, I would submit that section 2 of RICA only refers to real time communications and does not include the interception of stored communications. (Subject to the provisions of section 1(2)) This is also the approach that has been taken by the UK's Information Commissioner.

C.2.1.3 Content vs. Traffic data

The definition of "interception" contained in section 1 refers to the contents of communications on no less than three occasions. The "contents" of a communication is defined as any information concerning the substance, purport or meaning of that communication. I do not believe that this would include information such as the subject header of an e-mail or the size and format of attachments.

It is submitted that RICA does not expressly prevent employers from monitoring traffic data. Monitoring such data will be less invasive and in some instances will even provide added protection to an employee, e.g. where the employer detects from a reading of the subject header of a message that it is marked personal or

refers to content that is of a personal nature. Such an interpretation of the Act would therefore be in line with section 14(d) of the Constitution.

It will also be argued later in this paper that employers should be able to satisfy a number of the lawful purposes for monitoring e-mail and internet usage even when they confine themselves to traffic data. Where the need to inspect the contents of certain mails is unavoidable, initially monitoring traffic data will ensure that such monitoring is properly defined and limited to the relevant employees involved.

The UK equivalent of RICA specifically defines and excludes traffic data from the prohibition against interception. Section 2(5) states that:

"References in this Act to the interception of a communication in the course of its transmission do not include references to:

(a) Any conduct that takes place in relation only to so much of the communication as consists in any traffic data comprised in or attached to a communication …. , or

(b) any such conduct, in connection with conduct falling within paragraph (a), as gives a person who is neither the sender nor the intended recipient only so much access to a communication as is necessary for the purposes of identifying traffic data so comprised or attached."

Section 2(9) of RIPA identifies traffic data to include:

a) data identifying the person, apparatus or location from which the communication is transmitted;

b) *data identifying apparatus through which, or by means of which, the communication is being transmitted; and*

c) *any data identifying the data comprised in or attached to a particular communication.*

C.2.1.4 Automated interception

The prohibition against interception in terms of RICA includes the use of interception devices to monitor e-mail and Internet usage. However, the Act in the definition section specifically excludes any instrument, device, equipment or apparatus that is used by the employer in the ordinary course of their business and which has been fitted to the system either by the employer himself or by his service provider.[36] It would therefore appear that much of the technology used by employers to ensure the security and proper operation of their systems will be permitted by the Act.

The definition of interception also only refers to such activities where the contents of the communication are *made available to another person* (own emphasis). Monitoring workplace communications by automated means may not involve any information being made available to another natural person, i.e. certain technology can be run independently from beginning to end to achieve the desired result without another person ever seeing the results. Although this may be seen as a rather narrow interpretation of the definition, it is again in line with section 14(d) of the Constitution as it would provide a certain degree of added privacy for employees.

This interpretation has also been relied upon by the UK's Information Commissioner in connection with a similar definition of interception in RIPA.[37]

---

[36] Section 1(1) – "interception device"
[37] The UK Code at p. 34 of the Supplementary Guidance

C.2.1.4 Intentional interception

Intent is a necessary element of the statutory offence introduced by section 2 of RICA. This is slightly confusing as there are a number of elements that make up an unlawful interception in terms of the Act and the element of intent may relate to a number of these elements. For example, when intercepting a communication, must the employer's intention be to access the contents thereof in order to incur liability? What would the situation be where an employer intercepts an e-mail in the belief that it is business related in terms of section6, but on opening it he realises that it is a personal communication? Should he be held to have contravened the Act?

The UK's Lawful Business Practice Regulations provides for such a situation and allows businesses to intercept communications in order to determine whether they are business related or personal. In the absence of such a provision in our Act, it is suggested that employers should specifically state upfront that any communications sent over their information system will be regarded by the employer to be of a purely business nature. This should serve to negate the element of intent.

C.2.2 THE EXCEPTIONS

RICA sets out a number of exceptions to the general prohibition, a few of which are directly relevant to employers wishing to monitor workplace communications. They are:

a) Interception by a party to the communication (section 4);
b) Interception with the prior written consent of one of the party's to the communication (section 5); and
c) Interception in the course of carrying on a business. (section 6)

C.2.2.1 The Business Exception

The exception contained in section 6, i.e. the so-called "business exception", is found in various forms in similar legislation in other jurisdictions including the US's Electronic Communications Privacy Act. It is also important to note that the wording of section 6 follows closely the wording of RIPA and section 3 of the UK's Lawful Business Practice Regulations.

Since the new Act has been published, certain experts have warned that section 6 is badly drafted and should not be relied upon by employers intending to conduct interception and monitoring activities in their workplace. I disagree with this viewpoint and believe that employers can confidently rely on this exception to avoid liability when monitoring business related electronic communications.

What e-mails can be intercepted by the employer?

The wording of subsection 1 is pretty wide and should cover all e-mail communications that are related to the daily running of an employer's business, including all e-mail correspondence exchanged between the business and its employees, clients, suppliers and any other third parties with whom they have a business relationship.[38]

---

[38] Section 6(1) enables businesses to monitor the following e-mail communications:

a) E-mails by means of which a transaction is entered into in the course of that business;

b) Any other business-related e-mail; and

c) Any e-mail communication that takes place in the course of carrying on of that business.

***The wording of this section is exactly the same as section 2(b) of the UK's Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations.**

Lawful purpose for the interception of business related e-mails

In terms of subsection 2(b)(i), the interception must be for the purpose of monitoring e-mails sent and received in order to establish the existence of facts; or for investigating and detecting the unauthorised use of the employer's system; or to secure the efficient operation of the system. In other words, the employer's legitimate interest in obtaining evidence, maintaining the security of their information systems or regulating the use of such systems would justify the infringement of the privacy of their employee's communications.

The provisions of RICA in this regard depart slightly from the UK' Regulations in that the UK employers are also allowed to monitor and record communications for training purposes as well as to ensure compliance with other regulatory and self-regulatory duties. Both are further legitimate business reasons for conducting the monitoring and processing of employee's information and it is not clear why these additional provisions have been omitted from section 6 of RICA.

The UK also allows monitoring activities that are in the interests of national security and/or can be used to investigate and detect criminal activity. Despite the majority of the provisions of RICA being geared towards better interception capabilities for law enforcement, the Act does not allow for private businesses to assist in this regard.

Additional conditions that must be complied with

There are certain other conditions that an employer must abide by before embarking on any monitoring activity, even where it is business related. Employers must ensure that:

a) *The activity must be carried out by the system controller or by any other person with the express or implied authorisation of the system controller.*

In a business with juristic personality, the system controller will be the CEO or some official with similar status. In the case of smaller businesses conducted as a sole proprietorship or partnership, the system controller will be the business owner/s or some other employee who is authorised as such.

b) *The system controller must make all reasonable efforts to give advance warning to persons who intend to use the employer's system that their e-mails could be monitored.*
OR
He or she must ensure that the e-mails of such persons are intercepted with their express or implied consent.

It is not apparent from the Act what will be regarded as "all reasonable efforts". In respect of employees, the best way would be through an office communication policy.

The issue becomes slightly more problematic when dealing with external users of the system, particularly in the case of unsolicited electronic communications sent by an outside third party. It is impossible for an employer to give advance warning or to obtain the prior consent of such parties.

c) *The system in question must have been provided by the employer to be used wholly or partly in connection with their business.*

This would cover situations where employees are given laptops or other mobile devices that allow them to work from home. This practice is becoming more common in the new world of work where working hours are flexible and more and more employees are not bound to their offices.

C.2.2.2 Section 4 – interception by a party to the communication

Section 4 of RICA states that an electronic communication may be intercepted by the sender or intended recipient of such communication. In the definition of "a party", the Act also provides for a situation where the communication is intended for more than one recipient in certain instances. These provisions are important in the context of workplace monitoring for the following reasons:

a) A number of e-mails sent to a business may be intended for the business itself, even though the message may be channelled within the organisation to a particular employee to be dealt with. In such cases, the business itself is the intended recipient and is free to lawfully intercept such communications.

b) One can go even further and argue that where business related e-mails are sent to a particular employee, they are also intended for the employer. If the named recipient was absent from work, would it be expected that the communication would be dealt with by someone else within the organisation? In these situations, the employer may also be regarded as "one of the intended recipients".

By relying on the exception contained in section 4, it does not appear that employers will be obliged to give advanced warning or get prior consent. Such interceptions will also not need to be authorised by the system controller.

C.2.2.3 Section 5 - Prior written consent

As previously mentioned, it has been argued by some that employers can only be absolutely certain of avoiding liability in terms of RICA if they obtain their employee's prior written consent to the interception. While this may hold true as an absolute measure, it will also place a large cost and administrative burden on employers which may not strictly be necessary.

In terms of section 5 of RICA, an employer may intercept any indirect communication transmitted through their system provided that *one of the parties* (own emphasis) to the communication has given their prior written consent. The communication in question does not need to be business related.

Section 5 differs from section 6(2)(d) in that it specifically requires written (express) consent whereas the latter also includes implied consent. It would also appear that consent in terms of section 6 will be required from every person who intends to use the employer's system and not just from one party to the communication.

By only requiring the consent of one party to the communication, I would argue that section 5 may be unconstitutional. This is especially true in the employment context where employers will almost always choose to obtain consent from their employees. Personal or non-business related communications exchanged between an employee and an external third party may also include personal information belonging to the third party. The interception of such communications by an employer, albeit with his employees consent, will still constitute an invasion of the third party's constitutional rights in terms of section 14 of the Bill of Rights.

The threat of abuse increases further when one considers that employees may be coerced into furnishing their prior written consent. Although such coercion

may not be direct; the fear of losing employment, being passed over for promotion or losing out on some or other benefit may result in employees not putting up much of a fight.

The corresponding provision in RIPA states that there must be reasonable grounds for believing that both the sender and receiver have consented to the interception of their communication. Such consent therefore need not be written and can be implied from the surrounding circumstances.

In terms of ECPA, only one party has to consent, and such consent can be implied or express.

C.2.2.4 The employer as a service provider (section 10)

Section 10 of RICA provides that any person who is lawfully engaged in duties relating to the installation of any equipment, facility or device used in connection with a telecommunication service (includes internet service), or relating to the operation and maintenance of that system may intercept **indirect communications* in the ordinary course of the performance of those duties and where it is reasonably necessary to do so.

* The section refers to the interception of a "signal relating to an indirect communication". An example of such an interception would be a Telkom technician working on a faulty telephone line. It is not clear how this section would be interpreted in relation to e-mail and Internet services. I suspect that the section has not been drafted with the new technology in mind and is simply inherited from the earlier Interception Act.

In the definition section of RICA, a telecommunications service provider is defined to include an Internet service provider (ISP). The section goes on to define an Internet service provider as "*any person who provides access to, or*

any other service related to, the Internet to another person." Employers will often be the provider of such services in respect of their own networks and would thus fall within the definition of an ISP for the purposes of RICA.

Does this mean that an employer can also lawfully intercept electronic communications in terms of the provisions of section 10? In other words, could an employer rely on this exception where its IT Department intercepts incoming e-mails in order to divert them so as not to block a gateway? I would submit that it does.

In the UK Act, there is a similar exception although it is worded slightly differently.[39] The Information Commissioner, in her guidelines, has held that employers can be deemed to be a service provider in certain circumstances and would fall within the ambit of the "operations exception".

Section 3(3) of RIPA reads as follows:

"*Interception without consent is authorised by this section if –*

a) it is conduct by or on behalf of a person who provides a telecommunications service; and

b) it takes place for purposes connected with the provision or operation of that service or with the enforcement in relation to that service, of any enactment relating to the use of telecommunications services."

The "service provider" exception in ECPA exempts system providers from liability under Title I and Title II. The statutory definition of a service provider refers to "*..... any service which provides users thereof the ability to send or receive wire or electronic communications*". However, the US courts have held that where the

[39] Section 3(3) of RIPA

employer's e-mail system is separate from the Internet and the employer does not independently provide Internet services, he does not qualify as a "provider".

This issue may require further clarification by our courts.

C.2.3 CONCLUSION

Monitoring e-mail and Internet usage will normally involve some form of "interception" as the term is defined in RICA. However I have argued that many of the electronic monitoring activities carried out by employers will not fall within the ambit of the Act's general prohibition. Such activities may include the monitoring of traffic data, stored communications and the use of automated interception devices in certain circumstances. Those activities that do fall foul of section 2 may also be excluded by one or more of the exceptions contained in sections 4, 5, 6 and 10.

It would appear from a narrow interpretation of RICA that an employer will only be found criminally liable in the following circumstances:

a) Where the employer has intentionally intercepted a personal e-mail (or Internet communication) sent or received by an employee;
b) while the e-mail message is being transmitted;
c) without first obtaining the prior written consent of the sender or recipient;
d) where the intention is to access and read the contents of the personal communication; and
e) the purpose for such access is not related to the operation and maintenance of the employer's information system.

In practice, employers who carry out electronic monitoring or intend to implement such measures should ensure that the person or persons responsible for such monitoring (i.e. the system controller and their support staff) should be properly

trained and made aware of the different provisions of RICA. Although I believe that the scope of the Act can be curtailed, the draconian fines that have been introduced are sufficient to ensure that a certain degree of caution is exercised.

D. OTHER LEGISLATION

I have previously mentioned that the gathering or collection of information relating to e-mail and Internet usage, i.e. interception, is only one aspect of the monitoring activity. It may also involve the use, storage and disclosure of personal information belonging to employees and/or external third parties, therefore giving rise to other considerations of information privacy and data protection.

South Africa does not currently have any specific privacy or data protection legislation except for the limited protection offered by the Promotion of Access to Information Act and the voluntary approach adopted in Chapter 8 of the ECT Act. The SALC is however currently investigating the need for such legislation and an issue paper has been published in this regard.

D.1 THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT

D.1.1 Chapter 8

Chapter 8 of the ECT Act provides for a voluntary and self-regulatory approach to data protection. This approach is seen as an interim measure to introduce the relatively new notion of data protection into South African law pending the promulgation of specific legislation. The Act sets out a number of principles that may be followed in order to ensure better privacy protection for an individual's personal information. These principles are not unique to South Africa and are

based on international data protection standards that have been developed by the OECD[40], the European Union[41] and various private advocacy groups.

Employers in SA may choose to incorporate the provisions of Chapter 8 into their employment contracts. However, if they do so, they are required to subscribe to all the principles and not simply to certain ones. They will also be entitled to regulate their respective rights and obligations in respect of a breach of the principles themselves. The following principles are particularly relevant to the issue of workplace monitoring:

Prior written consent

The prior written consent of the employee must be obtained before the employer can collect, collate and process any of their personal information, unless the employer is permitted or required by law to do so. What constitutes lawful monitoring without consent will depend on the circumstances of each case. The provisions of the constitution, RICA, and comparative international law will be helpful in this regard.

Lawful purpose

The employer must disclose in writing the lawful purpose for the monitoring activity and any information collected must only be used for that purpose.

---

[40] Organisation for Economic Cooperation and Development's "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" Paris, 1981 (OECD Guidelines)
[41] Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data (the EU Data Protection Directive)

Limited use

Such information may only be used for some other purpose if the employee has given the employer written permission to do so, or the employer is permitted or required to do so by law.

Retention

The employer must keep a record of the personal information and the purpose for which it was collected for as long as the information is used and for one year thereafter.

Non-disclosure

After personal information on an employee has been collected, the employer must ensure that it is not disclosed to another party unless permitted or required by law or with specific written authorisation from the employee. Where lawful disclosures are made to third parties, the employer must keep a record of the third party to whom the personal information was disclosed for as long as it is being used and for a period of one year thereafter.

Deletion

The employer must delete and destroy all employee information which has become obsolete.

It is expected that these principles will be retained in some form or another in any new legislation that is introduced. In the meantime, I would recommend that employers introduce these concepts into their working environment. Although South Africa is still catching up with the rest of world in this area, there is no

doubt that data protection will become increasingly important in the next few years.

D.1.2 Section 86 offences

Chapter 13 of the ECT Act, which deals with cyber crime, may also be relevant to the question of the legality of electronic monitoring. I will not discuss each of the offences listed in section 86, save to say that the provisions of section 86(1), (2), (3) and (4) may apply to many of the methods used by employers to monitor e-mail and Internet usage.

Unlike RICA, section 86 does not expressly refer to data that is in the course of transmission. An employer who accesses *stored communications* without authority or permission to do so may now also be held criminally liable. It is not expressly stated in section 86 or anywhere else in the ECT Act in which circumstances a person will be authorised to access or intercept data. The exceptions contained in RICA, although not exhaustive, will be important in this regard.

The penalties in respect of any contravention of section 86 are also very different to those imposed by RICA. An employer who contravenes the ECT Act will face a fine of R 5000.00 or no more than 12 months in prison. This inconsistency will need to be addressed by the Legislature before RICA is brought into operation.

D.2 THE PROMOTION OF ACCESS TO INFORMATION ACT

PROATIA gives effect to section 32 of the Bill of Rights and provides additional data protection to individuals after their information has been collected. Employees are generally entitled to access any of their personal information that

has been collected by their employers, including information collected from electronic monitoring.

Employees are also entitled to amend any information held on them that is incorrect and/or inaccurate. Non-compliance with PROATIA will again result in criminal liability for the employer. It will be recommended at the end of this paper that employers conducting automated e-mail and Internet monitoring should ensure that the systems used have the capability of providing fast and adequate access to information should it be requested by an employee.

E. JUDICIAL PRECEDENT

E.1. THE LACK OF CASE LAW IN SA

South African courts have not yet been called on to decide cases involving e-mail and Internet abuse in the workplace. I have already mentioned that, in the absence of specific legislation, there is a growing need to develop the common law in this area. Adding content to open-ended concepts such as reasonableness and the legal convictions of the community will provide further certainty to employers and employees on what is and is not permitted when it comes to electronic monitoring. With the introduction of RICA it is hoped that our courts will get their opportunity.

There have been a few arbitration awards published in connection with the monitoring of e-mail and Internet use. Although these awards do not have any binding effect, they are useful in highlighting some of the relevant issues.

E.2 BAMFORD AND OTHERS v ENERGIZER [42]

For Ms. Bamford and others, their dismissal for e-mail and Internet abuse came as somewhat of a shock. In response to their dismissal, the applicants instituted arbitration proceedings in the CCMA and questioned the fairness of their dismissal on a number of grounds. Of importance is the following:

a) There was not a complete ban on personal use of e-mail and internet facilities in the Energizer workplace and any limitations placed on such use were not made clear to employees.

b) The contents of the e-mails in question contained pornography, sexually and racially offensive material and a number of trademark offences. The employees argued that the material was not offensive or obscene according to their own moral standards and that the e-mails were only forwarded to fellow workers with similar standards.

c) The "tone" of the workplace was regarded as relevant to the dispute. In this regard, the arbitrator found that the culprits were "*middle class articulate young women who are not bereft of education*". He found further that "*it cannot lie in the mouth of well educated white collar workers to say that they are unaware that it was impermissible for them to traffic in what was socially unacceptable material*". [43]

[42] [2001] 12 BALR 1251 (P)
[43] ibid at 1268 B-H

(The importance of the context of a particular workplace and employment relationship to the question of monitoring was also highlighted in **Cronje v Toyota Holdings**[44], where the employer was concerned about racial jokes and images being distributed amongst a unionised shop floor.)

d) The e-mails were held not to be "personal" in any respect but rather could be referred to as "non-business" or "private" as they consisted entirely of material generated by other, unknown persons which was distributed for the consumption of any interested parties on the internet. The personal dignity or affairs of the employees had not been disturbed.

e) The e-mails in question were recovered from the employer's own e-mail system where they had been stored. The arbitrator held that, even in the case of genuine personal communications, it would be unrealistic to argue that employees are entitled to store intimate material on a company-owned storage facility without the employer being entitled to examine the contents thereof from time to time to see if such material must be kept.[45]

F. THE FUTURE

The South African Law Commission is currently investigating the need for specific privacy and data protection legislation to be introduced into our law.[46] A preliminary issue paper was published in August 2003 for the purpose of

[44] 2001 3 BALR 213 (CCMA)
[45] ibid at 1271 A-B
[46] Project 124

identifying the relevant issues and to invite further comment from interested parties.[47]

The issue of workplace privacy is briefly discussed under Chapter 4 of the issue paper which relates to data users.[48] The Commission recognises the changing face of the modern work environment, particularly the blurring of the lines between home life and work life brought about by the introduction of mobile teleworking and computing. There is therefore a growing need in the area of employment for increased privacy and data protection measures.

The Commission also recognises that employers may have legitimate reasons for collecting information about their employees, and that electronic monitoring may be appropriate in this regard. The paper suggests that the best approach to these issues is through a process of consultation and negotiation between companies and their workers. It also believes that good employers will apply common sense and maintain a relationship of trust with their employees when introducing any monitoring activity into the workplace.

The Commission identified the ILO Code as a useful guideline but felt that it was merely advisory and the principles introduced therein needed to be strengthened. They have called for comment on the need for further research on the issue in line with in-depth studies that have been conducted overseas.

---

[47] Issue Paper 24
[48] ibid p. 96 - 97

G. INTERNATIONAL LAW

Countries with more sophisticated data protection laws have now come to grips with their legislation in this area and are now looking to ensure that the generally accepted principles are applied in specific sectors, including employment. At the same time, the International Labour Organisation (ILO) has highlighted the need for better protection of personal information about employees in the information age.

As a result, there have been a number of new developments over the past year in the area of electronic monitoring in the workplace, including the introduction of three new codes of practice in the EU, United Kingdom and Hong Kong. These documents highlight some useful principles that can be applied to strike a balance between the legitimate interests of the employer and the privacy rights of their employees.

G.1 ILO CODE OF PRACTICE ON THE PROTECTION OF WORKER'S PERSONAL DATA (1997)[49]

G.1.1 Introduction

The International Labour Organisation (ILO) began examining the whole issue of privacy at work in the 1980s. In 1990/1 it issued three major reports under the 'Conditions of Work Digest' series and in 1996 it published its own code of practice on the 'protection of workers' personal data'. The ILO Code was drawn up by an international panel of experts in response to the underlying need for the

[49] found at http://www.union-network.org/uniibits.nsf

more general data protection principles to be given specific application and content in the field of employment.

The drafters tried to retain a greater degree of flexibility by providing that the Code has no binding force. Instead, it provides a basis for employers and workers to agree on specific provisions relating to the processing of personal data in the workplace.

The Code, in dealing with workplace monitoring, recognises that such practices take place and may be necessary. However, it goes on to set out a number of principles that should be followed by employers to ensure that the monitoring activity is fair and, above all else, safeguards the human dignity of employees who are monitored.

G.1.2 General provisions

The Code is primarily concerned with the practice of employers systematically gathering large amounts of personal data belonging to their workers. It recognises that this may have certain far reaching consequences, including the tendency of employers to use this information to influence and manipulate their worker's behaviour. The Code emphasises that employers should only process personal data that is directly relevant to the employment relationship and that such processing should be the exception rather than the norm. What an employer must or can be expected to know about their employees will depend on the context of a particular employment relationship.

By applying the generally accepted data protection principles that have developed from other international data protection documents, the Code sets out a number of guidelines employers should follow in the collection, use, storage, security and disclosure of personal data. Perhaps the most important principle stressed in the Code is that an employer cannot have free and unlimited use of

the personal data collected. There must be a clearly identified and limited purpose for the collection of information, which must be communicated to the employee.

In the case of workplace monitoring, section 5.4 of the Code states that information collected in connection with technical measures to ensure the security and proper operation of automated information systems should not be used to control worker's behaviour. Such measures will normally include continuous or universal monitoring. It is therefore important that such systematic collection of data is tempered by a strict limitation on the uses to which such information can be put.

It also provides further that decisions concerning a worker should not be based solely on the automated processing of that worker's personal data. In situations where large amounts of data are gathered, the risks of that information being false or misconstrued increases considerably. It is therefore important that personal data collected by electronic monitoring should not be the only factor in evaluating a worker's performance.

G.1.3 Workplace monitoring

Section 6 of the Code deals specifically with monitoring and sets out the following important principles:

a) Advanced warning and full disclosure should be given to workers who will be monitored. Specific information must be furnished about the reasons for such monitoring, the time schedule, the methods and techniques used and the data to be collected. It will not be sufficient to simply issue a general directive that monitoring will take place.

b) The employer must minimize the intrusion on the worker's privacy as much as possible.

c) Workers will not be able to waive their privacy rights.

d) Covert monitoring should only be allowed in limited circumstances, the best example of which would be the suspicion on reasonable grounds of a criminal activity or other serious wrongdoing. Such monitoring must be in conformity to national legislation.

e) Continuous monitoring as a technical measure to ensure the security and proper operation of the employer's information system is probably one of the few cases where such activities by the employer are generally acknowledged to be indispensable. Continuous monitoring should also only take place if required to protect the health and safety of persons or the protection of property.

In section 12.2 the Code also provides that worker's representatives, where applicable, should be informed and consulted about:

a) the introduction or modification of automated systems that process worker's personal data; and
b) when electronic monitoring is to be introduced.

The Code has been applied in a number of countries, however it has been criticised for being too vague and not directly relevant to individual employment situations.

G.2 EUROPEAN UNION: ARTICLE 29 WORKING PARTY'S WORKING DOCUMENT ON THE SURVEILLANCE OF ELECTRONIC COMMUNICATIONS IN THE WORKPLACE (MAY 2002)[50]

G.2.1 Introduction

This document was drafted in response to a growing need for the uniform interpretation of the provisions of the EU's "Data Protection" Directive among its member states as they relate to the issue of workplace privacy, particularly electronic surveillance and monitoring in the workplace. Due to the growing importance of these issues, the Working Party intends introducing a new draft directive on "Privacy in the Workplace" by 2005. [51]

The EU specifically separates itself from the position taken in the US by recognising that employees have a legitimate expectation of a certain degree of privacy at work which is not overridden simply because they use communication tools that belong to the employer. However, the Working Party also recognises that employers have a legitimate interest in protecting themselves, their workplace and their employees in certain circumstances.

The working document, which is largely based on the jurisprudence of the EU Court of Human Rights and other international texts, sets out the most important principles that must be applied when balancing the legitimate interests of the employer with the fundamental rights of the employee.

The document suggests that employers ask the following questions before implementing any electronic monitoring measure in their workplace:

---

[50] found at http://www.europa.eu.int/comm/internal_market/privacy/docs
[51] Baker McKenzie Global E-law Alert, 8 September 2003.

a) Is the monitoring activity **transparent** to the employees?
b) Is it **necessary**? Could traditional methods of supervision be used to achieve the same purpose?
c) Is the processing of personal data proposed **fair** to the employees?
d) Is it **proportionate** to the concerns that it tries to ally?

G.2.2 The data protection principles applied

The working document confirms that electronic monitoring and surveillance activities fall within the broader definition of "data processing" under Directive 95/46/EC. This means that such activities must have a legitimate purpose that is communicated to the employee. The document states that the best form of legitimisation is where the activity is necessary to pursue the legitimate interests of the employer, the clearest being their right to protect themselves against liability, including vicarious liability. The working party also believes that legitimisation through consent is limited in the context of employment.

The document goes on to state that any monitoring activity must comply with the data protection principles introduced by Directive 95/46/EC. These principles are as follows:

G.2.2.1 Necessity

Any form of monitoring must be absolutely necessary for the specified purpose before it is proceeded with. Traditional methods of supervision and / or less intrusive methods should be used where possible.

G.2.2.2 Finality

Data collected through any monitoring activity may not be further processed for any other alternative purposes.

G.2.2.3 Legitimacy

The data processing operation may only take place if it has a legitimate purpose, i.e. it must be for the purpose of the legitimate interest pursued by the employer. Unless specifically authorised by national law that provides adequate safeguards, monitoring activities aimed directly at processing sensitive data would not be legitimate under the Directive.

G.2.2.4 Transparency

Employers should be clear and open with their employees about their monitoring activities. This includes the obligation to provide sufficient information to the employee about the specific circumstances which would justify such exceptional measures, and about the breadth and scope of the monitoring activity.

Compliance with this principle would include the employee's right of access to personal data collected by the employer through their monitoring activity and where appropriate the right to request rectification, erasure or blocking thereof.

Employees should also be informed immediately about any misuse that has been detected or where any other workplace rule or standard has been contravened.

G.2.2.5 Proportionality

Monitoring must be adequate, relevant and not excessive with regard to achieving the employer's specified purpose. Blanket monitoring should not be allowed except for maintaining a secure information system or for some other crucial reason.

G.2.2.6 Accuracy and retention of data

Employers must ensure that all data collected via the monitoring activity is correct and accurate. A record should be kept of all data collected for a limited period of time, the length of which will depend on the circumstances.

G.2.2.7 Security

The employer is obliged to implement technological and organisational methods which will ensure that any personal data collected will be kept safe and secure, during the collection process and thereafter.

The Working Party identifies the important role played by system administrators in any monitoring activity and in connection with the retention and protection of data collected. Other staff members who come into contact with the collected data should also be aware of the importance of good management principles and upholding the privacy rights of their colleagues.

The document goes on to examine the practical application of these principles particularly as they relate to issues of e-mail monitoring and personal Internet usage.

G.2.3 E-mail monitoring

It has been generally accepted that the right to secrecy of correspondence contained in the EU Convention on the Protection of Human Rights and Fundamental Freedom applies to the workplace. The Working Party is also of the view that on and offline communications should be treated equally in this regard. In other words, an employee's e-mail should enjoy the same protections afforded to their letters, facsimiles and memoranda.

The point is also emphasised that where e-mail correspondence is between an employee and an outside party, the latter will usually not have given his or her consent. It will therefore be very difficult to justify the monitoring activity on the basis of consent from one party alone.

The Working Party suggests that employees should be allowed a separate mail facility for personal use or, alternatively, a web-based mail account. They believe that it will be difficult for an employer to argue that they have a legitimate interest in monitoring e-mails transmitted through such means. It is recommended that only in circumstances where security is threatened will an employer be entitled to monitor personal mailboxes.

The document also draws the distinction between content and traffic data and suggests that employers can satisfy a number of their legitimate concerns by monitoring traffic data only.

G.2.4 Internet usage

The Working Party does not believe that a blanket ban against personal Internet use is workable in today's society. They also believe in a policy of prevention rather than detection. By the efficient use of technology, unwanted sites can be blocked and automatic warnings can be employed to alert transgressors. Again it is possible to alleviate concerns by monitoring time spent or a list of sites generally visited by a department rather than the content of any site visited by one specific employee.

Employers should also take cognisance of the fact that employees may unwittingly access sites that they do not intend to. A full hearing should be granted to an employee before disciplinary action is taken for any Internet abuse.

G.3 APPROACH BY INDIVIDUAL MEMBERS STATES

It is not possible within the confines of this paper to deal with each member state's approach in detail. I will briefly discuss some of the more interesting approaches and then deal separately with new developments in the United Kingdom.

G.3.1 Germany

The regulation of e-mail and internet usage by employees without consent through special monitoring software is contrary to German law. There are certain exceptions to this rule, including where there is an express provision in the employment contract regarding the prohibition of private use, or where the employee's representatives have consented to the monitoring activity.

Where an employer has gained consent from his employees to monitoring their e-mails, he will only be entitled to monitor traffic data initially to determine whether the message is relevant to his business. The monitoring of content will be only permitted when the employer is able to show that his/her business interests prevail over the information privacy rights of the employee.

Surveillance without consent is also allowed if necessary to ensure the effective operation of an information system. (i.e. virus checks, memory capacity).

G.3.2 France

France enacted law on the secrecy of communications in 1991. In terms of this law, communications cannot be accessed without judicial warrant or unless the interception is conducted in "good faith". This term has been interpreted to mean that only the volume and size of mails as well as the format of attachments can be monitored. (i.e. traffic data)

The French Labour Code also provides that employee personal data cannot be collected without informing the employee first.

In the recent Nikon decision[52], the French court found that limited daily personal use of e-mail and the Internet should be allowed provided that it does not affect the professional life of the employee. They also suggested that messages should contain a description at to whether it is private or professional. If an e-mail is labelled private, the employer will be prohibited from gaining access to it even where there is a workplace rule against personal use.

The French Data Protection Authority recommends further negotiation between the parties to find workable solutions and the designation of a specific data protection official in the workplace.

G.3.3 Netherlands

The Dutch Working Conditions Act states that employees, worker's councils and/or trade unions must be informed of monitoring activities.

The Data Protection Act states that monitoring may take place with the employee's unambiguous consent, in the performance of a labour agreement, in the fulfilment of legal obligations or where a legitimate interest is being pursued by the employer.

G.3.4 Portugal

The Portuguese Constitution is quite advanced in that rather than having a general article on privacy, Article 35 deals specifically with data protection in relation to the use of computerised data.

---

[52] **SA Nikon France v Frederick Onof** Decision No.4164, 2 October 2001

Article 34 assures the secrecy of correspondence and also prevents intrusion by public authorities into private communications, including telecommunications. In a 1998 decision, the Portuguese Data Protection Authority held that the right to secrecy of correspondence includes both traffic data and content.

Article 18 specifically gives the Portuguese Constitution vertical and horizontal effect, so the privacy provisions will apply to private employment relationships.

G.3.5 Finland

On 1 October 2001, the Finns introduced a new act dealing with the protection of privacy in working life.[53] The Act applies to both the public and private sectors and includes job applicants. Section 9 of the Act deals with the monitoring and surveillance of workers and highlights an approach based on self-regulation. The Act does not set out to create rights and obligations but rather to encourage the establishment of policies relating to technical surveillance and use of information networks.

The law emphasises that the employer must not endanger the secrecy of private e-mails by their actions and any data collected must be from the viewpoint of the employment relationship. The Act also obliges employers to consult with their employees before implementing policies relating to e-mail surveillance. After the consultation process, the employer is also obliged to disclose the purpose for the surveillance, the methods used and the principles pertaining to acceptable use of e-mail and information networks in the workplace.

G.4 UNITED KINGDOM: THE EMPLOYMENT PRACTICES DATA PROTECTION CODE, PART 3: MONITORING AT WORK[54]

[53] **Data Protection in Working Life** Law 477/2001
[54] found at http://www.dataprotection.gov.uk/dpr/dpdocs

G.4.1 Background

The UK introduced the 1998 Data Protection Act in order to comply with the EU's Data Protection Directive. In order to deal with the impact of new Act on the employment relationship, the UK Information Commissioner set out to investigate the matter with a view to producing a code of good practice. The introduction of the four part code titled "Employment Practices Data Protection Code" has been staggered over the past two years. Part 3 of the Code which deals with monitoring in the workplace was introduced in June 2003. The other parts of the code deal with recruitment and selection, employment records and medical information respectively.

"Personal Information" is defined in the Code as information relating to a living person that identifies an individual whether by itself or together with other information held by the organisation. Such information is further distinguished from "sensitive data". In the employment context, sensitive data may include trade union membership, details of physical or mental health contained in employee's sick leave records and racial classification for equal opportunity and /or affirmative action policies.

The Code also gives "processing" a wide definition to cover a comprehensive range of activities including the initial obtaining of personal data, retention and use thereof, access and disclosure and final disposal.

The Code does not have any direct binding effect; however it can be used as evidence when a provision of the Data Protection Act has been contravened.

G.4.2 Monitoring

The Code states that monitoring may, to varying degrees, have an adverse impact on workers. It may also interfere with the relationship of mutual trust and confidence that should exist between employers and their employees. It is therefore important that any adverse effect must be justified by the benefits to the employer and/or others.

The Code suggests the use of an "impact assessment" to judge whether the monitoring activity is a proportionate response to the problem the employer is seeking to address. This would involve the following test:

(i) identify the purpose(s) behind the monitoring activity and the benefits it is likely to deliver;

(ii) identify any likely adverse impact the activity may have;

(iii) consider alternatives to monitoring or different ways it can be carried out;

(iv) take account of the obligations that arise from monitoring; and

(v) judge whether monitoring is justified.

G.4.3 Consent

The Code confirms that there are limitations to how far consent can be relied on in the employment context to justify the processing of personal data. Consent must be "freely given" in terms of the Data Protection Act and, once given, it may be withdrawn. Employers will, in most cases, not be able to obtain the consent of external parties, but if the monitoring activity can be justified on other grounds consent is not necessary.

G.4.4 Core principles relating to monitoring

The Code states from the outset that it will usually be intrusive for an employer to monitor their employees. By applying the current jurisprudence of the European Court for Human Rights, the code also confirms that employees have a legitimate expectation of a certain degree of privacy in their workplaces.

If employers wish to conduct any monitoring in their workplace, they must be clear about the purpose and satisfied that the particular monitoring activity is justified by the real, and not apparent, benefits that will be delivered.

Workers should be aware of the nature, extent and reasons for any monitoring, unless covert monitoring is justified. Such awareness will influence the worker's expectations when it comes to determining the scope of their right to privacy.

If monitoring is to be used to enforce an organisation's rules and standards, the employer must make sure that the rule and standard is clearly set out in a policy or is in some other way brought to their employees' attention.

If information gathered from the monitoring activity might have an adverse impact on the employee, they must be presented with the information and allowed the opportunity to make representations before any action is taken against them.

G.5 HONG KONG: A DRAFT CODE OF PRACTICE ON MONITORING AND PERSONAL DATA PRIVACY AT WORK (March 2002)[55]

G.5.1 General

The Code was compiled by the Office of the Hong Kong Privacy Commissioner for Personal Data in 2002 in response to the alarming results of a number of surveys conducted in 2000 and 2001.[56] Due to the legacy of English law that has been left in Hong Kong, their Code is very similar to the UK Code even though they were released at different times. The Code does not have any binding effect and is merely a guideline to employers on how to conduct electronic monitoring fairly.

G.5.2 Two important principles

Two principles are identified by the Code to ensure that monitoring of employee's electronic communications is conducted in a fair manner:

G.5.2.1 Proportionality

The Code states that any intrusion on an employee's privacy should be in proportion to the benefits derived from the monitoring by a reasonable employer. Such benefits are related to the risks monitoring is intended to reduce. It states

[55] found at http://www.pco.org.hk

[56] It was found that 64% of Hong Kong businesses used at least one of five forms of electronic surveillance in their workplace; while only 22% had relevant written policies.

that the level of monitoring should be no greater than is reasonably required to contain or guard against the risk. The risks identified by the Code include:

a) financial loss
b) damage to reputation and goodwill
c) unauthorised disclosure of confidential information, including loss of trade secrets
d) exposure to vicarious liability
e) productivity / loss of working time

G.5.2.2 Transparency

This basically equates to proper communication with employees. Again the Code provides that specific information regarding the nature of, and justification for, the monitoring activity must be given to the employees before the activity begins. Employees will then be able to assess the risks associated with their actions and choose an appropriate level of behaviour. The Code makes the valid point that without transparency, choice cannot be fully informed.

The employer must also clearly specify the purposes served by monitoring, and the data that is to be collected.

G.5.3 Other recommendations

The Hong Kong Code also suggests that the adverse impact of any monitoring activity be measured before it is adopted by the employer. This should include any adverse effects the monitoring will have on third parties outside the employment relationship.

The Code also suggests that:

a) Monitoring be restricted to traffic data rather than content as much as possible.

b) Continuous monitoring should only be adopted if it is the only means of ensuring security of assets, safety of persons, integrity of business transactions or monitoring exchanges of a sensitive nature between employees and others.

c) Universal monitoring should only be adopted where there is *prima facie* evidence of wrongdoing which cannot be attributed to a particular group or individual employee. All monitoring should be targeted and of a limited duration.

d) Covert monitoring should be limited to situations where specific criminal activity or serious wrongdoing has been identified, and notifying employees of the monitoring would prejudice the successful gathering of evidence. It is however important that the monitoring is again for a limited length of time and proper safeguards are implemented.

The Code specifically recommends that a written employee monitoring policy be adopted to cover the business interests served, the methods employed, the location and times of the activity, the criteria for accessing records and the retention period for information gathered. It also recommends that persons administering the monitoring and collection of personal data must possess the requisite integrity, prudence and competence.

G.6 USA

G.6.1 Background

The US has been widely criticized for not paying sufficient attention to privacy protection. These concerns have become even more relevant in light of new security legislation that has been passed in the US in the wake of the September 11 terrorist attacks. In the case of workplace privacy issues, the US adopts a self-regulatory approach and has allowed companies a greater degree of latitude to monitor e-mail and Internet usage.

Two interesting 2001 surveys in the US have highlighted the enormity of electronic monitoring in the US:

a) According to a report from the American Management Association[57], nearly 80% of employers engage in electronic monitoring of work-related communications and activities, including monitoring e-mails or Internet usage, videotaping the workplace and recording telephone calls; and

b) The Privacy Foundation reports that 40 million out of the 140 million workers in the US regularly use e-mail and the Internet at their jobs.[58]

G.6.2 The reasonable expectation of privacy test

It has been accepted in the US that employees do not have an unlimited right to privacy in the workplace. The US courts apply the general privacy test normally applied in non-electronic privacy disputes by asking whether the employee's subjective expectation of a right to privacy was reasonable.

In **Bohach v City of Reno**,[59] the court rejected the invasion of privacy claims of two police officers who had sent messages to each other on the department's internal messaging system. The messages were assessed and used in an internal affairs investigation several months later. The plaintiff's argued that the

[57] Found at http://www.amanet.org/research/pdfs/ems_short2001.pdf
[58] see fn 4
[59] 932 F.Supp.1232 (D.Nev. 1996)

retrieval of the months-old messages was a violation of their right to privacy (under ECPA).

The court held that the messages were essentially e-mails and pointed to a department order informing employees that their messages would be logged on the network. The employees could therefore not have a reasonable expectation of privacy.

Because most disputes are usually settled at state level, the standards of reasonableness and decisions taken may differ between states. In **Smyth v Pillsbury Co.**[60] the court refused to find in favour of an employee who had been fired for sending inappropriate and unprofessional e-mails, even though the company had consistently assured its employees that their e-mail was confidential. The court held that the plaintiff employee had no reasonable expectation of privacy because he had voluntarily communicated the messages over the company's computer system.

The court went on to say that, even if the plaintiff did have such an expectation, it was outweighed by the company's legitimate interest in preventing inappropriate or unprofessional e-mails being sent over it's system.

The counter-argument that has been raised in some cases is that even though the messages are sent over the company's computer system, the messages themselves are protected by the employee's personal password. The courts have refused to accept that furnishing an employee with a private password entitles the employee to a reasonable expectation of privacy.

---

[60] 914 Supp. 97 (E.D.) Pa 1996

The California court in **Bourke v Nissan Motor Corp.**[61] held that although protected by a password, the employee still knew that the message could be accessed by third parties. This view was also upheld in a Texas court in the case of **McLaren v Microsoft Corp.**[62]

The US courts have based their findings in these matters on the employers ownership of the computer facilities.[63] However, they have always upheld the principle that a company may not monitor its employee's e-mails without first informing them that their use of company equipment is subject to such monitoring.

G.6.3 The future

There has been a great deal of lobbying in the US for stricter privacy protection particularly in the area of information security. New privacy legislation has been passed through Congress and should come into operation shortly.[64] Although the new act does not expressly deal with workplace privacy and the issue of electronic monitoring, it perhaps signifies a new mindset being adopted in the US.

---

[61] Cal. Court of Appeal, 2nd Dist, 26 July 1993, found at http://www.tomwbell.com/netlaw/Ch05/Bourke.html>

[62] (1999)WL 339015(Tex. App)

[63] cf. to Singapore where it is expressly provided in the relevant property laws that employers own workplace e-mail, telephone and computer content. Monitoring employee communications is permissible and invasion of privacy cannot be raised as a defence to dismissal.

[64] The Online Personal Privacy Act

H. GOOD PRACTICE RECOMMENDATIONS

It has been shown through an examination of the existing legal framework in South Africa and from comparative international law that there are a number of objective principles that can be applied to the regulation of electronic monitoring in the workplace. In addition to assisting our law in determining when an infringement of the employee's right to privacy will be justified, these principles also offer useful guidance to employers on how to implement electronic monitoring in a manner that is lawful and fair. In this section of the paper, I will suggest how the more important principles can be given practical application in the workplace.

Before continuing, it should be noted that it is important to retain a measure of flexibility. Each employment relationship and workplace will be unique and have their own dynamic and should be regulated on an individual basis. Research has suggested that the size of an organisation is directly related to the scale and extent of workplace monitoring, with e-mail and internet monitoring being far more prevalent in larger organisations.[65] However, I believe that these general recommendations will be useful to any organisation, regardless of its size.

H.1 General Recommendations

a) The business owner, CEO or any other official identified as the system controller should be adequately briefed in the provisions of RICA, other applicable legislation and the generally accepted international standards for data protection. Other responsible person or persons, who have knowledge of the issues and are of sufficient character and integrity, should be appointed by the system controller to administer

[65] see fn 54

electronic monitoring and to oversee overall data protection in the workplace if he or she is not able to perform this function themselves.

b) All employees who play a role in workplace monitoring should be adequately trained and should know their own responsibilities when it comes to processing personal information belonging to others.

c) An employer's monitoring policies should be seen as an integral part of their overall procedures. Such policies must be constantly reviewed and upgraded to stay in line with new technologies being introduced into the workplace.

d) Employers should consult and negotiate with employees, workplace forums or trade union representatives before implementing electronic monitoring procedures. Common sense and trust should prevail. If there are legitimate reasons and proper safeguards for monitoring e-mail and Internet usage, and it is carried out in a dignified manner, employees should have no complaints.

H.2 Necessity

a) Before introducing electronic monitoring, employers should clearly identify the purposes behind the activity in question. The purpose of the monitoring activity is the reference point for determining what is necessary, reasonable and fair.

b) Where possible, electronic monitoring should be limited to that which is necessary to ensure the security and efficient operation of the employer's information system. Protecting a business against viruses

c) and malicious code, which may result in crippling financial and information losses, is clearly a necessity for any modern business.

d) The monitoring activity should also be limited in its duration, extent and targeted personnel to ensure that it remains reasonably necessary to achieve the purpose identified.

e) Information obtained through electronic monitoring should not be used for any alternative purposes that have not been previously identified, unless it can be shown that it is in the employee's interest or is information that a reasonable employer could not possibly ignore.

H.3 Proportionality

a) After the purpose for the activity and the benefits to be derived therefrom have been identified, employers should conduct an impact assessment test to determine whether the activity will have any adverse impact on employees or any other persons.

b) If certain adverse impacts are identified, the employer should weigh up whether the likely benefits achieved by the monitoring activity will justify any adverse impact.

c) The employer should determine whether there are alternatives to electronic monitoring that will achieve the same purpose. Traditional methods of supervision, training and management counselling are some of the ways in which employers may be able to avoid introducing electronic monitoring.

d) Where electronic monitoring is unavoidable, employers should ensure that the scope, methods and duration of the activity are limited as much as possible. A few examples would include:

(i) Monitoring traffic data rather than the contents of electronic communications will achieve a number of the purposes identified by employers. Where it is necessary to inspect content, initially monitoring traffic data will narrow the scope of such monitoring. For example, restricting the examination of content to only those messages that have been sent to rival organisations when investigating a trade secret leakage.

(ii) Conducting spot checks or once-off monitoring rather than continuous monitoring may be appropriate to confirm suspicions of specific misconduct or misuse.

(iii) Accessing stored e-mails may be less invasive than intercepting real time communications.

(iv) Automated systems may often achieve the desired purpose without another person, including a colleague, from having sight of an employee's communications.

NOTE: Where automated monitoring takes place for a specific purpose, such as virus protection, it may also result in extraneous information on an employee or third party being indirectly gathered. If the monitoring function remains automated, such additional information will not be seen by management or other staff members.

H.4 Transparency

a) Unless covert monitoring is justified, advanced warning and full disclosure should be given to employees about the monitoring of their e-mail and Internet usage at work. Covert monitoring will be justified if notice to employees would be likely to prejudice the prevention or detection of a crime or similar workplace misconduct, or the apprehension and prosecution of offenders. The Hong Kong Code provides a useful test by asking whether the misconduct in question would warrant police involvement. If so, the covert monitoring may be justified.

b) The best way to provide information to employees and ensure transparency about an employer's intended or current monitoring activities is to establish, document and communicate a policy in this regard. The use of a clearly worded electronic communications policy, that has been read and signed by all employees, will assist employers on a number of levels. Assumed understanding amongst employees and employers is dangerous and can lead to unpleasant and costly disputes.

c) It is however important to note that employees base their expectations of privacy not only on the employer's stated policy but also on its practice. Employers should ensure that the principles, rules and standards contained in a policy should be adhered to and implemented on a uniform basis.

d) The capabilities of information systems can also be used to inform and remind employees of their obligations. For example, formatting a click wrap agreement to appear before an employee accesses the Internet

or e-mail facilities at work; or using "pop-ups" to warn employees who have accessed an unauthorised website.

e) As previously mentioned in this paper, it will be difficult for employers to notify external third parties, especially those who are the senders of communications. Reasonable steps that an employer can take to inform outsiders may include providing such information in a footer or attachment to all outgoing e-mails, or to formally request employees to advise friends and family accordingly.

f) The more invasive the monitoring activity is, the more information must be given to the employee.

g) Full disclosure must be given regarding the nature, method, duration and time schedule for the monitoring activity; as well as the type of information that will be collected, the purpose and likely benefits to be achieved and any other information relevant to the activity. A blanket statement that monitoring may take place is not sufficient.

h) Where the monitoring activity is used to enforce an employer's rules and standards for the use of e-mail and internet facilities, they must ensure that these rules and standards are clearly identified, preferably in the same communication policy.

i) Where words such as "offensive' or "unacceptable content" are used in such policies, the employer must define in greater detail what is meant by these concepts and give examples thereof.

j) The policy should also outline how it will be enforced and what the penalties are for non-compliance. Employees can then make the appropriate decision regarding their further conduct.

k) Employees should also be informed of the extent to which information about Internet access and e-mail use is retained and for how long. Educating employees on when a message will be deleted completely from the system or where there may still be an "audit trail" will also ensure that their expectations of privacy remain realistic.

H.5 Enforcement and disciplinary action

a) The ILO has stated in strong terms that information collected by way of electronic monitoring should not be the sole basis on which an employer makes decisions. This is especially so in matters involving discipline and dismissal. The reasoning behind this warning is that information collected by automated means can be inaccurate due to a system malfunctioning or being deliberately falsified for ulterior motives. When combined with other facts, the information may also become misleading.

b) Where adverse information is collected, employees should be allowed immediate access to such information and given the opportunity to make representations to their employer before any action is taken against them.

c) As can be noted from the Energizer arbitration award, the normal defence raised by employees when faced with dismissal for e-mail or Internet abuse, is that they were not aware that such use was prohibited. In successfully countering such a defence, an employer must show that there is an established rule or standard against such use and that this rule or standard has been contravened. Clearly formulating a policy which sets out the parameters for acceptable or prohibited use and ensuring that it is known to all

employees will assist employers should subsequent disciplinary action be necessary.

H.6 Personal Use

a) Opening an employee's personal e-mails will only be justified in exceptional circumstances. Even where an employer has expressly prohibited personal use of e-mail and internet facilities at work, they would still be precluded from opening any personal correspondence detected on the system. However an employer should still be entitled to implement automated monitoring that rejects or returns unacceptable messages even if they are personal in nature.

b) Where an employer allows a certain degree of private use, employees should be encouraged to mark their personal e-mails as such in the subject header. They should also inform third parties to do the same.

c) Personal e-mail accounts or web-based hotmail accounts would also allow for a more realistic balance. Unacceptably large volumes of personal use could be easily detected and regulated. There does not appear to be any reason why employers would be required to access content in respect of these private accounts. The employer's domain name would not be associated with any "questionable" e-mails and they would be more likely to avoid any issues of vicarious liability.

d) It is highly unlikely that intercepting and monitoring e-mails containing sensitive personal information will ever be justified. Alternative secure lines of communication should be provided for

employees who need to transmit sensitive data such as medical information or trade union correspondence.

H.7 Retention, access and disclosure

a) Employers must ensure that they uphold their employee's access rights to information collected via electronic monitoring, including the employee's right to correct or modify any inaccurate or misleading information. Automated systems must allow for quick and accurate access to enable employers to comply with any requests from their employees.

b) Information collected and stored by the employer should be adequately secured and retained in the proper format. Ironically, such security measures may include a further need for electronic monitoring.

c) The ECT Act sets out a number of general provisions regarding the retention, storage and accessibility of data messages which may be applicable. If an employer adopts the Chapter 8 framework for data protection, they will be obliged to retain all information collected for a period of one year.

d) Disclosure of information collected from electronic monitoring to another employee may be inappropriate, even where viewing such information is within that employee's function in the business. This may become more problematic in smaller businesses where employees will know one another well and usually have some degree of a personal relationship.

e) Information collected via electronic monitoring should not be disclosed to any external third party unless the employee has consented thereto (in terms of Chapter 8 of the ECT Act such consent must be in writing and a record of the persons to whom the information has been disclosed must be kept for a period of one year). An obvious exception is where such information is relevant to the commission of a criminal offence and should be reported to the necessary authorities.

H.8 Consent

a) Many of the international documents have confirmed my submission that consent alone is not sufficient to justify electronic monitoring in the workplace. If a direct consequence of not consenting is dismissal, being passed over for promotion or denial of a significant benefit, consent cannot be regarded as being freely given.

b) Consent is also a unilateral act and can be withdrawn at any time. Employers therefore should not rely on employee consent unless there are other grounds for justifying their monitoring activities.

c) Obtaining an employee's consent will affect their subjective expectations and therefore the extent to which their right to privacy will be protected. Prior written consent will also ensure that employers do not fall foul of RICA.

H.9 Non-legal considerations

Apart from the legal considerations that must be applied, employers should also evaluate whether implementing electronic monitoring will have other adverse effects. The most important social consideration for an employer will be whether the relationship of trust between an employer and their employees will deteriorate as a result of electronic monitoring. Instead of effectively policing productivity, monitoring an employee's e-mail may result in discontent and a lack of motivation on the part of the employee.

Finally, as South Africa catches up with the rest of the developed world on recognising the importance of information privacy, it will be important that an understanding, awareness and respect for this notion is fostered throughout the country. By implementing a best practice model in their workplace, employers will encourage employees to take their own responsibility for this issue more seriously, thus creating a corporate culture that is based on respect for data protection and information privacy. In the wake of the King 2 report, this must be seen as one of the cornerstones of good corporate governance.

BIBLIOGRAPHY

BOOKS

- Neethling J, **Persoonlikheidsreg,** Butterworths, 1998
- De Waal J, Currie I and Erasmus G, **The Bill of Rights Handbook**, Third Edition, Juta & Co. Ltd, 2000

TABLE OF CASES (SA)

- Bamford and Others v Energizer [2001] 12 BALR 1251 (P)
- Bernstein and Others v Bester NO and Others 1996 (4) BCLR 449 (CC)
- Cronje v Toyota Holdings [2001] 3 BALR 213 (CCMA)
- Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others v Smit and Others 2000 (10) BCLR 1079 (CC)
- Moonsamy v The Mailhouse 1999 20 ILJ 464 (CCMA)
- Tettey v Minister of Home Affairs 1999 (1) BCLR 68 (D)

TABLE OF CASES (FOREIGN)

- Bonhach v City of Reno
- Bourke v Nissan Motor Corp.
- Halford v The United Kingdom
- McLaren v Microsoft Corp.
- Niemitz v Germany
- SA Nikon France v Frederick Onof
- Smyth v Pilsbury

TABLE OF STATUTES (SA)

- Constitution of the Republic of South Africa Act 108 of 1996
- Electronic Communications and Transactions Act 25 of 2002
- Labour Relations Act 66 of 1995

- Promotion of Access to Information Act of 2000
- Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002

TABLE OF STATUTES (FOREIGN)

- Electronic Communications Privacy Act 1986 (US)
- Regulation of Investigatory Powers Act 2000 (UK)
- Data Protection in Working Life Law 477/2001 (FINLAND)

INTERNATIONAL DOCUMENTS

- A Draft Code of Practice on Monitoring and Personal Data Privacy at Work (HONG KONG)
- European Convention for the Protection of Human Rights and Fundamental Freedoms
- European Union's Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data
- European Union Article 29 Working Party's Working Document on the Surveillance of Electronic Communications in the Workplace
- ILO's Code of Practice on the Protection of Worker's Personal Data
- OECD's Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data (1981)
- Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments
- Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments
- The Employment Practices Data Protection Code: Part 3 – Monitoring at Work (including Supplementary Guidance) (UK)

NATIONAL DOCUMENTS

- South African Law Commission's Discussion Paper (Project 105)

- South African law Commission's Issues Paper (Project 124)