

Electronic communication in the workplace: employer vs employee legal rights

Gerard Louis Barnardt

Thesis presented in partial fulfilment of the requirements for the degree of Master of
Laws at the University of Stellenbosch



Supervisor: Roux de Villiers

April 2004

I, the undersigned, hereby declare that the work contained in this thesis is my own original work and that I have not previously in its entirety or in part submitted it at any university for a degree.

SUMMARY

The monitoring of electronic communication is likely to face all employers sooner or later. The rapid advancement in technology aimed at helping to monitor electronic communication, makes it easier than ever before for employers to monitor the electronic communications of their employees.

There are important questions to consider when dealing with the topic of monitoring electronic communication. Examples include "may an employer legally monitor electronic communications?" and "how does monitoring affect the employee's right to privacy?"

This thesis is an attempt to answer these and other related questions by analysing, *inter alia*, South African legislation, the Constitution and case law, as well as comparing the law as it applies in the United Kingdom and the United States of America.

The analysis and conclusion offered in this thesis aim to provide theoretical consideration to academics and practical application for employers that are faced with the reality of monitoring electronic communications.

OPSOMMING

Alle werkgewers sal waarskynlik die een of ander tyd met die monitering van elektroniese kommunikasie gekonfronteer word. Die snelle voortuitgang in tegnologie wat daarop gemik is om te help met die monitering van elektroniese kommunikasie, maak dit vir werkgewers makliker as ooit tevore om sodanige kommunikasies van hulle werknemers te monitor.

Daar is egter belangrike vrae wat oorweeg moet word wanneer die onderwerp van monitering van elektroniese kommunikasie ter sprake kom. Voorbeelde hiervan is "mag 'n werknemer regtens elektroniese kommunikasies monitor?" en "hoe raak monitering die werknemer se reg tot privaatheid?"

Hierdie tesis is 'n poging om hierdie en ander verwante vrae te beantwoord deur die ontleding van, onder andere, Suid-Afrikaanse wetgewing, die Grondwet en die reg soos deur hofuitsprake ontwikkel, sowel as vergelyking van die reg soos wat dit van toepassing is in die Verenigde Koninkryk en die Verenigde State van Amerika.

Die ontleding en gevolgtrekking wat in hierdie tesis aangebied word, is gemik op die verskaffing van teoretiese oorweging aan akademië en praktiese toepassing vir werkgewers wat met die realiteit van die monitering van elektroniese kommunikasies gekonfronteer word.

Table of contents

Introduction	9
1 An introduction to electronic communication and monitoring	12
1 1 History of electronic communication	12
1 2 Definition and overview of electronic communication and monitoring	16
1 3 The rationale behind the monitoring of electronic communication	21
2 Employment relationship and electronic communication monitoring	25
2 1 Employment contract	25
2 2 Employment relationship	25
2 3 Breakdown of the employment relationship	26
2 4 Role of workplace forums	30
3 Constitutional and statutory implications	32
3 1 General	32
3 2 Privacy issues	32
3 3 Statutory issues	41
3 3 1 Interception and Monitoring Prohibition Act 127 of 1992	41
3 3 2 Electronic Communications and Transactions Act 25 of 2002	44
3 3 3 Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002	46
3 3 3 1 General prohibition	49
3 3 3 2 Exceptions	52
3 3 3 3 Business exception	55
3 3 3 4 Communicated-related information	58

3 3 3 5 The Interception Act and Privacy	61
4 International developments around electronic communication monitoring in the workplace and the South African comparison	69
4 1 United Kingdom (UK) perspective	69
4 1 1 Introduction	69
4 1 2 UK legislation	70
4 1 2 1 The Office of Telecommunications (OFTEL)	71
4 1 2 2 Human Rights Act of 1998	72
4 1 2 3 Regulation of Investigatory Powers Act of 2000	74
4 1 2 4 Data Protection Act of 1998	81
4 1 2 5 The DPA Code of Practice	84
4 1 3 Summary	89
4 2 United States (US) perspective	91
4 2 1 Introduction	91
4 2 2 US proponents of monitoring employee electronic communications	93
4 2 3 US opponents of monitoring employee electronic communications	97
4 2 4 US laws	98
4 2 5 US Constitutional rights	107
4 2 6 US common law	111
4 2 7 Summary	114
4 3 Comparison with South Africa	117
4 3 1 Vicarious liability	117

4 3 2 Interception in South Africa compared	119
4 3 2 1 Business exception	119
4 3 2 2 Consent	121
4 3 2 3 Access to stored information	122
4 3 2 4 Disclosure of intercepted information	123
4 3 2 5 Communication-related information	124
4 3 2 6 Infrastructure - set-up for interception	125
4 3 2 7 Liability	127
4 3 3 Expectation of privacy	127
4 3 4 Constitution	128
5 Practical suggestions for employers faced with implementing data security policies and monitoring processes	130
5 1 Where to from here?	130
5 2 Practical suggestions	130
5 2 1 General	131
5 2 2 Employee consent	131
5 2 3 Employer policy guidelines	132
5 2 4 Monitoring	134
5 2 5 Intellectual property	135

6 Conclusion	137
6 1 Interception Act	138
6 2 Improving the Interception Act	140
6 3 Constitution	142
Glossary of computer terms	144
Bibliography	154
Books	154
Magazines, journals and periodicals	156
Table of cases	158
Table of legislation and treaties	162
Online sources	165

Introduction

The potential for significant improvement in the workplace can be made a reality by the new technologies available today. Employers can utilise the tools created through such technologies to increase profit and business share. Unfortunately, these tools may also create a simultaneous risk of abuse by employees. New technologies enable employers to monitor certain aspects of their employees' performance at work, especially the use of modern electronic communication tools such as telephones and computer terminals, and in particular electronic mail, voice communications and the Internet. Until recently, such monitoring has virtually been unregulated.

Employees are raising legitimate concerns, since new improvements in technology allow employers to monitor the activities of their employees more closely than ever before. To make it worse, most employees are unaware in which circumstances or how often they are being monitored. Even though some employees are informed of monitoring activities executed by their employers it is usually after the fact.

Employers have a legitimate expectation that their employees are performing as per the requirements of their employment contract, while employees do not appreciate having their every action scrutinised, especially since they retain a Constitutional right not to have the privacy of their communications infringed. In essence, such disparities of interest form the basis for the conflict resulting from workplace monitoring.

Employers recite several legitimate reasons why they need access to an employee's electronic files and why it may be necessary to monitor email and Internet traffic of employees. These include potential liability (vicarious or otherwise) and/or damages resulting from employee activities such as defamatory statements, the infringement of intellectual property rights or unauthorised contracts concluded by employees through the use of electronic communications, the managing of bandwidth needs, measuring employee productivity and having access to employer information stored on an employee's computer. In addition, employers also have an interest in ensuring that employees do not divulge company trade secrets by way of their communications. And, finally, after the terrible tragedy of September 11th 2001, employers more than ever want to make sure that employees are not engaging in any type of criminal activity in the workplace.

With the growing advancement in technology and the use of electronic communication, in addition to the long hours that many employees work, the monitoring of electronic communication is likely to face all employers. As the use of email increases, the relevant legal issues in the workplace multiply as well. Not surprisingly, international litigation involving electronic communication has increased steadily over the past few years. Many of these cases emphasise the competing interests of the employer and the employee. Employers want to monitor email for productivity and liability reasons, while employees argue that the employer's monitoring of electronic communication violates their right to privacy.

Various software packages exist that can monitor a wide range of electronic communications. Such software can assist employers in the enforcement of policies and procedures aimed to avoid legal liability for damage suffered as a result of the unlawful or non-permissible manner in which employees use the electronic resources provided by the employer. Furthermore, it can also be used to help the employer in making sure that employees spend their time attending to the business of the employer and not on personal issues.

The question remains whether or not an employer may legally monitor electronic communications? If so, may this happen without employee consent and, if so, to what extent and under which conditions? How does this affect the employee's right to privacy? What alternatives to monitoring exist? Furthermore, since interception often takes place with a view to gather evidence, to what extent may an employer rely on such evidence in a court of law - particularly when such evidence was obtained unlawfully? Current case law provides little guidance for employers in answering these questions. In addition, a lot of confusion still surrounds the Regulation of Interception of Communications and Provision of Communication-Related Information Act (Interception Act) 70 of 2002 and how it applies to monitoring and what needs to be done in order to comply with it. Some of the provisions in the newly enacted Interception Act¹ are still open for interpretation, which further complicates compliance.

¹ 70 of 2002.

The aim of this thesis is an attempt to answer these and other related questions. In doing so this thesis will cover the following aspects:

- (a) The rationale behind the monitoring of electronic communication including the reasons cited by employers to justify monitoring.
- (b) The relationship between employer and employee with specific reference to the nature of the employment relationship and the ability of employers to discipline or end the employment relationship with an employee for contravening policies regarding electronic communication. In this regard the role of fairness in such a dismissal will be investigated.
- (c) The right to privacy of employees in the workplace and the susceptibility thereof to waiver by agreement in the employment contract.
- (d) The constitutional and statutory implications with regards to the monitoring of electronic communication in South Africa. Special attention will be given to the Interception Act² and its implication for employers and employees, and whether it could withstand constitutional scrutiny in terms of its infringement of the right to privacy. Furthermore, the law as it applies in the United Kingdom and United States of America will be analysed and compared to the position in South African.

The analysis and conclusion offered in this thesis aim to provide theoretical consideration to academics and practical application for employers (their attorneys and/or legal advisors) faced with implementing data security policies and monitoring processes. As such this thesis will provide for both theoretical and practical application in the fast-paced world of electronic communication and how it impacts on the rights of the employer as opposed to those of the employee.

1 An introduction to electronic communication and monitoring

1.1 History of electronic communication

To understand the future of electronic communications monitoring, it is imperative that we understand what is meant by it, and its past.

From the late 1970s to the mid-eighties, the 300-baud Teletype terminals connecting to conference systems dominated computer communication. Although expensive and slow they managed to bridge space and time as never before.

In 1977 the Apple-II computer was introduced and four years later the IBM PC Microcomputers began to have an impact on science and anthropology.³ However, the only impact that microcomputers had on electronic communication was to make connections to mainframes easier and cheaper. At that stage only the mainframe computers were connected to digital networks.

Although computer-to-computer electronic communication was far more difficult then than it is today, the benefit was already visible. The Internet did not exist, but there were dozens of ideas, and implementations, for computers to talk to each other. One of these, ARPA Net, was destined to grow into the Internet, but without lucrative military contracts, the man in the street could not connect to it and so it was reserved for those with huge budgets and the scientific elite.

³ Bernard & Evans *New Microcomputer Techniques for Anthropologists Human Organization* (1983) 182-185.

In the early 1980s getting started with electronic communication meant reliance on technophiles.⁴ At that time, "hacker" was a good word that meant someone who put theoretical computer science and programming together to make computers do something useful and exciting. The hackers had created a way around the impenetrability of the ARPA Net. These "historic" systems had one advantage: they were cheap at a time when hardware and CPUs were expensive.

The UNIX operating system was a great boom to networking, being at the forefront of hacking activities. At that stage email made use of the UUCP (Unix to Unix Copy) system that had been built into the UNIX operating system. This copy facility permitted the sending of an electronic message from one machine to a user on another machine, with the provision that the exact path the message was going to take from the sender's machine to the recipient's machine was known.

Some ways of sending email in the mid-eighties included sending email from one computer to another across a network, or sending email from computer to computer using dialled up intermittent connections.

In the mid-eighties several means of electronic communication were developing. CompuServe⁵ attracted many customers to its centralised service. CompuServe installed its own packet-switching network; being available to the public as a front end to their dial-in services only. This network competed with other front-end dial-in packet networks such as TYMNET and TELNET. These networks only allowed users in making a modem phone call to a computer that treated them as a terminal. The Internet, on the other hand, connects computers to each other. With the Internet the computers can interact without a user touching the keyboard.

4 Technophiles are the eager adopters of new technology, and technophobes are those who are upset by rapid change in technology (Westrum *Technologies and Society Belmont* (1991)). When dealing with computers the latter are still the majority in modern society according to Weil & Rosen *TechnoStress: Coping With Technology @Work @Home @Play* (1997).

5 The largest information utility of that era.

In comparison with these early communication systems, the Internet is a vast improvement. Connecting computers together to work as a "team" has a potential that has hardly been realised. Based on this principle, the World Wide Web has had a tremendous impact on the way people and businesses communicate, albeit with limited effect.

The limiting factor is social organisation. In the social evolution that is taking place on the Internet, the responsibility and social consciences of the actors are critical ingredients. Commercial interests are currently stimulating Internet programming. Sophisticated programmers are luring unsophisticated people into their "commercial webs" causing a decay of social conscience. The tremendous power of computer-to-computer communication has allowed people who lack a social conscience to invade privacy and disrupt information processing in ways that was never possible before.

One of the problems in the early years (that continue to be a problem at present) was that communicators were primarily interested in technology as opposed to the subject of the communication. Most of the earlier communication traffic dealt with computer technology. Using computers to communicate is similar to learning a new language, and the Internet is full of people interested in computer technology. Fortunately, a division of labour stimulated by the commercial applications of the Internet has set in. The computer "whiz kids" have been put to work in making computers easier to use for the rest of us. Some of the big breakthroughs have been the result of graphical user interfaces (GUIs) that transfer linguistic memory tasks to the visible computer screen. This occurred in Macintosh for terminal emulation and in the program Mosaic, later to become Netscape, for the World Wide Web (WWW).

As the Internet developed, a number of useful features were adapted to WWW hypertext.⁶ Human memory requirements and the complexity of technology could now be hidden behind colourful computer display screens. The "computer" disappeared and a new virtual reality emerged.

⁶ Hypertext is text that allows you to jump from a selected word or phrase to another document or elsewhere in the same document by the mere click of a button. Also see definition of "hyperlink" in the Electronic Communications and Transactions Act 25 of 2002.

In the South African context, the National Party of old had a self-preservationist obsession with "security legislation". The interception of telephonic communications was originally authorised in terms of s 118A of the Post Office Act.⁷ Technological advances made it increasingly possible for the unauthorised interception and monitoring of telecommunications to take place by both state and private parties. The government of the time, moving for the passage of the Interception and Monitoring Prohibition Bill in 1992⁸, argued that such legislation was necessary in order to protect the individual's common-law right to privacy. Two modifications were introduced by the Interception and Monitoring Prohibition Act 127 of 1992. First, the Act⁹ altered the government functionary who could authorise such interceptions.¹⁰ In addition, the Act¹¹ allowed for only a judge or designated retired judge of the supreme court to issue a direction to monitor communications.¹² This change was vital in order to split the powers of the executive and judiciary. Secondly, state focus shifted from state security to the combating of serious crime.¹³ At the time, it was argued that a

7 Act 44 of 1958. The 1972 Potgieter Commission, set up to investigate matters relating to the security of the state, recommended the insertion of s 118A into the Post Office Act 44 of 1958. This amendment was seen to accord with similar legislation and powers in Australia, West Germany and Britain. In 1981, the Rabie Commission of Inquiry into security legislation reviewed the provisions of s 118A and proposed certain further administrative, procedural and technical amendments.

8 Second Reading Debate 17 June 1992 Hansard Col 11522. Now the Interception and Monitoring Prohibition Act 127 of 1992.

9 127 of 1992.

10 Under s 118A and 118(2)(b) of the Post Office Act 44 of 1958, the Minister of Posts and Telegraphs or any minister who was a member of the State Security Council could authorise communications interception "in the interests of state security".

11 127 of 1992.

12 S 2(2) of the Interception and Monitoring Act 127 of 1992.

13 As defined in schedule 1 of the Criminal Procedure Act 51 of 1977.

limitation on the right to privacy for this objective is as legitimate as one being in the national interest.¹⁴

The expanding of communication tools beyond that of the traditional fixed line telephone brings with it the tools for monitoring those communications. Governments around the world, fuelled by dual needs to protect the privacy rights of individuals as well as monitor the activities of criminals using the communications networks, are toning their surveillance laws in accordance with technological developments and constitutional necessity.

1 2 Definition and overview of electronic communication and monitoring

Electronic communication has been defined in a number of different acts, statutes and policies of countries across the world. Although such definitions largely constitute means to suit specific purpose such as criminal offences, they are by their very nature wide in definition.¹⁵ Electronic communication is simply defined as "communication by computer" by the WordNet online dictionary.¹⁶

Essentially, communication by computer is not possible without a means of transmitting the content to another computer. One facet thereof is called "networking", be it an internal company network or outside of company walls by means of a telephone "line" (be it physical or mobile cordless) via Internet.

14 The intention to combat the source and planning of crime is clearly evident in the transcripts of the parliamentary debates. The House of Assembly was divided 104:34 in favour of the bill.

15 The definition of "electronic communication" appears in the US Federal Statute 18 USC § 2510(12) and is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system that affects interstate or foreign commerce, but does not include -

(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;
(B) any wire or oral communication;
(C) any communication made through a tone-only paging device; or
(D) any communication from a tracking device".

16 See <http://www.dictionary.com> - WordNet ® 1.6, © 1997 Princeton University.

In essence, the Internet is a worldwide system of interconnected computers. One form of communication over the Internet is effectively a worldwide electronic mail system. In addition, the Internet grants access to a vast compository of information that can generally be accessed with ease by an Internet user. This compository is commonly known as the World Wide Web. The Internet allows users to quickly transmit a magnitude of data (be it text, visual images or sound files) worldwide with the touch of a button.

Unlike email on a local or internal company network, email sent on the Internet is not routed through a central control point and, in fact, it can take many and varying paths before reaching its recipient(s). In addition, email on the Internet is generally assumed to be unsecured and as such may potentially be viewed by intermediate computers between the sender and the recipient, unless the message is specially encrypted.¹⁷

The ease with which messages can be exchanged over the Internet, of course, bears a price. One example of a cyberspace blunder demonstrates the potential dangers that come with this rapidly growing technology. The Philadelphia Inquirer reported on May 8, 1999 that a FCC employee inadvertently transmitted a dirty joke via email entitled "Nuns in Heaven" to 6,000 journalists and government officials.¹⁸ Instead of forwarding this joke to a friend, the employee in question mistakenly forwarded the joke to each person on the agency's distribution list. This mistake, which resulted in embarrassment for the agency and disciplinary action for the employee, shows the ease with which sensitive and confidential information can inadvertently be distributed to thousands of computer users.

17 Having an account with a respectable ISP the security risk has largely been reduced since secured sessions by means of encrypted software are now offered.

18 Nicholson "Oops Wrong E-Mail Address List. A Dirty Joke Goes Global" *Philadelphia Inquirer* (1999-5-8).

Messages between individuals can be exchanged over the Internet on a particular topic of interest, by either forwarding it automatically to recipients who are on a mailing list or through a moderator that oversees the distribution of the messages. Many commercial on-line services provide their own "chat groups" where individuals can exchange communication covering likeminded topics. Such service providers include America OnLine, CompuServe, Microsoft Network, Prodigy, and AT&T Worldnet.

A second category of Internet communication is the search for and retrieval of information located on remote computers. The primary methods to locate and retrieve information on the Internet are as listed, namely: (a) searching the "World Wide Web" (WWW) by means of software search programs such as Yahoo or Alta Vista; (b) searching a remote computer by means of a browser; and (c) by retrieving certain information using file transfer protocol ("FTP"), which is a method of transferring computer files between computers.

The WWW is essentially a series of documents stored in different computers that display files containing text images, sounds, animation and/or moving video. These files generally contain "links" to other information or resources. An essential element of the WWW is that every linked computer has a "physical address", better known as an IP address. Many organisations now have "home pages" on the WWW. Home pages are mostly electronic documents that provide a series of links to other information. Each link automatically connects the user to that information and/or to another Internet site on another computer connected through the Internet.

The WWW runs on tens of thousands of individual computers that are "linked" to each other, through what is known as the Internet, and has no centralised control. No single organisation controls any membership on the Internet, nor is there any single centralised point from which individual Internet sites or services can be centrally blocked or excluded. The only semblance of control or organisation on the Internet is that all information on the Internet must be formatted to a TCP/IP format so that all users are able to read the material published thereon.

A survey conducted by Louise Harris and Associates, in February 1999, found that the most popular use of the Internet was email, with 63% of the respondents reporting that they send emails often.¹⁹ SurfWatch Software, a division of Spyglass, Inc. launched CheckNet in March 1998 to help companies determine employee use of Internet access. According to the results of a 1998 SurfWatch survey, 24% of the time spent online by those employees participating in the survey was not work-related.²⁰ A March 1999 study conducted by Worldtalk Corporation found that employees spend on average 30 minutes a day sifting through their deluge of email messages.²¹

Although sending and receiving email accounts for a significant percentage of the online time spent by workers, exploring the Internet also preoccupies parts of the workday. SurfWatch determined that the three categories accounting for the largest portions of non-work surfing were general news, sexually explicit material, and investment information.²²

NetPartners estimated that US businesses lost \$450 million in worker productivity when Congress released the Starr Report and President Clinton's video deposition over the Internet.²³ Such use of the employer's communications network comes at a price and necessitate companies to take action.

According to an article by ZDNET UK News the analyst firm IDC stated that "companies can lose up to £3m a year in wasted time and bandwidth from employees surfing the Net on office time".²⁴

19 See <http://www.nua.ie/surveys>.

20 "Over 24 Percent of Employee Time is Non-Work Related" *Business Week* (1998-8-11).

21 Brown "The Mess Made for Business Junk Mail" *Business Week* (1999-4-19).

22 *Business Week* (1998-8-11).

23 Jackson "Survey: Legal Liability of Web Access a Top Concern" *Computer News* (1999-1-11).

24 See <http://news.zdnet.co.uk/story/0,,s2073980,00.html>.

According to preliminary data made available by the American Management Association (AMA), as of the first quarter of 1999, nearly 30% of major US companies monitored employee emails, up from 20% in 1998 and 15% in 1996.²⁵ Content Technologies Incorporated, a company developing software for monitoring purposes, has seen its sales double every year from 1996 through 1998.

Through March of 1999, AMA found that 84% of the participating companies inform their employees of company communication monitoring policies.²⁶ The financial sector, including banking, fund managers, brokerage, and insurance companies are most likely to monitor their employees' communications, according to AMA.

In the UK things are not much different. According to the Society for IT Managers' annual survey of local authorities, 77% of the 124 organisations surveyed admitted to using some form of email and web monitoring. Of those who admitted to monitoring, 48% admitted to message filtering, while 78% said they blocked web sites. Meanwhile, 73% admitted to having data protection policies.²⁷

The enormous increase in electronic communications and surveillance potentially exposes employers to various forms of legal liability. Corporate decision-makers must thus decide what policies they wish to adopt concerning access to, use, and disclosure of electronic and voice mail sent and received by their employees through means of office communication systems. While varying significantly from company to company and jurisdiction to jurisdiction, the following issues should be considered:

- (a) employee privacy rights;
- (b) the disclosure of confidential information;
- (c) the rights of third parties in obtaining access to company records and the company's need to manage its resources;

25 Carleton "Somebody's Watching, Worker Beware, as Companies Crack Down on E-Mail Abuses" *The Capital Times* (1999-4-9).

26 See <http://www.nua.ie/surveys>.

27 See <http://www.socitm.gov.uk>.

(d) the right of unions to access employee records stored on a company computer system.

Many employers have failed to address these concerns by neglecting to establish an email policy, and recent legal developments underscore the folly of such inaction. Now more than ever, it is imperative for employers to have a company email policy in place. Still to date, a significant number of companies do not have email or Internet user policies in place. According to a study by International Data Corporation, as of the end of 1998, 60% of the companies surveyed did not have an employee email or Internet usage policy, while 25% said they had a general ban on personal use of those resources.²⁸

As technology becomes faster and cheaper, concerns about employee privacy continue to mount. The impressive advancements in computer communications have created new problems, and in some cases increased the severity of old ones. In today's digital age information is no longer the privilege of only a few but is there for the taking by those with the knowledge and moral inclination to make use of it.

1 3 The rationale behind the monitoring of electronic communication

Shortly after the September 11²⁹ terrorist attacks on the United States of America two brothers William and Christiaan Conradie, aged 26 and 35 respectively, were accused of disseminating a false CNN report alleging South African involvement in the suicide attacks in America. This was done by means of email and as a consequence William Conradie was dismissed for contravening his employer's ethical code and electronic communication policy.³⁰ Whether such email was intended as a joke, the consequences of the action certainly is all but a laughable matter. The two brothers faced charges of sabotage, framed under the Internal Security Act 74 of 1982, in

28 Kokmen "Firms E-mail Computer Policies, Employees' Personal Use a Concern" *Denver Post* (1999-3-22).

29 Triple bombings in the U.S. on Tuesday 11th of September 2001.

30 "Sanlam Fires One of the E-mail Hoax Brothers" *The Herald* (2001-9-28). See <http://www.eherald.co.za/herald/2001/09/28/news/e-mail.htm>.

addition to fraud charges as the "alleged email might also have affected the economy of the country, including the value of the Rand".³¹

It is important to recognise that employers cite some valid reason for employee monitoring, be it in part or as a whole. Examples such as the "Conradie hoax" *supra* may have some serious consequences, not only for the employees involved but also for the employer as a whole.

What follows is a list of the reasons that employers cite as to why they monitor employees:

- (a) The monitoring of employees' work may be justified on the basis of security, especially where workers handle sensitive personal data or financial transactions. Examples here include employees working in the banking industry or those working for Government departments dealing with sensitive personal information such as the revenue service personnel.
- (b) Some employees may be monitored as a means of assessing performance against imposed targets. This is especially true of call centres, data processing and data entry workplaces, where speed of operation is crucial to operational performance. Employers like to be able to reward diligent workers for their efforts. As such, employee monitoring allows employers to see the good things as well as the bad, and act accordingly. After all, "people who like to do a good job like to be measured - intelligently and justly, that is".³²
- (c) Employers also have an incentive to ensure that employees do not unwittingly or intentionally divulge company trade secrets or infringe intellectual property by way of their communications. As such they may require additional monitoring services to guard against the possibility of intentional or unintentional leaking of sensitive company information. If employees are making mistakes that they are unaware of, employers want to be able to correct such mistakes before it impacts

31 "Alleged Hoax E-mailers to Face Charge of Sabotage" *ANC Daily News Briefing* (2001-9-18). See <http://www.anc.org.za/anc/newsbrief/2001/news0918.txt>.

32 "Big Brother?" *The New York Times* (1987-5-10) 14.

on productivity. If employee performance can be monitored, employers can determine where improvements need to be made. And if improvement is indeed necessary, monitoring data is vital to determine the appropriate training. If employers are aware of the areas where employees are lacking in, they can concentrate training efforts on those areas alone, saving time and money in the process.

- (d) Furthermore, employers want to prevent or remedy any defamatory statements made by employees in electronic communications, and as such monitoring may be a way of achieving this.
- (e) Employers want to make sure that employees are not engaging in any type of criminal activity in the workplace. The very nature of criminal activity makes detection thereof difficult and as such employers feel the need to use any means necessary aimed at exposing such activities.
- (f) Companies invest vast sums of money in building intellectual property. Employees have an obligation to protect the employer's intellectual property rights and employers are necessitated to insure this happens.
- (g) Email could be used to conclude or vary a contract in the same way as a written letter. The Electronic Communications and Transactions Act (ECTA) 25 of 2002 makes it clear that agreements concluded by means of data messages are not without legal force and effect.^{33 34} Such capability gives rise to the danger of

33 S 22 of the Electronic Communications and Transactions Act 25 of 2002.

34 Also see the UK case *Hall v Cognos Ltd* 1998-2-17 Case no 1803325/97. H's right to reimbursement of expenses was subject to detailed company rules. Having missed the claim deadlines specified in those rules, H e-mailed a request for permission to enter a late claim. His request was referred to his line manager, S, who replied via email "Yes, it is OK". Relying upon that assurance, H submitted a late claim but the employers refused to pay it. A clause in H's contract of employment stated that "any amendment or modification of this [contract] will be in writing and signed by the parties or it will have no effect". In his claim for breach of contract, two issues arose: was email correspondence capable of constituting a document "in writing and signed by the parties" and did S have ostensible authority to agree to a variation of the terms relating to payment of expenses? On the first issue, the tribunal held that, once an email was printed out, it took a written form and was signed by the parties because

employees inadvertently forming contracts on behalf of their employer or varying contractual terms to which the employer then becomes bound. Employers need to ensure that employees are aware of the implications attached to email communication, and may wish to ensure that appropriate disclaimers are attached to email messages.

- (h) Most of the organisations with internal email systems provide the exchange of emails between their internal network and other external networks on the Internet. Such organisations want to ensure the availability and integrity of their networks. As a result they need to implement scanning software to protect against viruses and spam. In addition, companies are adding value to their business by providing Internet access to their employees. However, some employers are concerned that these facilities may be used for inappropriate or non-business purpose and resultant production lost.
- (i) Companies want to comply with the legal requirements for distributing company correspondence. With regard to email it should be noted that s 50(1)(c) of the Companies Act 61 of 1973 requires the name and registration number of a company to be mentioned "in legible characters in all notices and other official publications of the company" with regards to "all letters, delivery notices, invoices, receipts and letters of credit of the company". It is submitted that section 50(1)(c) also applies to email communication of a company.

Apart from the above reasons there might be others specific to a certain business. Employers have a legitimate interest in making sure that those in its employ use electronic communication within the boundaries created for its intended use. In addition, the very nature of the human race is such that trusting employees does not always resolve the issue and certain steps necessitate the enforcement of rules and regulations from a company perspective.

each message contained the printed Christian name of the sender. On the second issue, the tribunal was satisfied that H was entitled to rely on S's apparent authority to authorise a variation of the terms of his contract since, at all material times, S was H's line manager. The employers were therefore bound by the variation sanctioned by S's email.

2 Employment relationship and electronic communication monitoring

2 1 Employment contract

The employment contract serves as the basis for the employment relationship.³⁵ As a result, it is the starting point for the entire system of rules associated with labour law. The contract helps to determine the existence of an employment relationship and the nature thereof.

The relative importance of the employment contract has declined in recent years, while other sources of legal regulation, for example legislation, have increased in importance.³⁶ Legislative intervention has surpassed the employment contract as an instrument of creating rights and duties between the employer and employee. However, the employment contract is still important as forming the basis for the employment relationship and containing the basic rights and duties pertaining to it.³⁷

2 2 Employment relationship

The employment relationship is wider than the employment contract. As such, it is characterised by other considerations whereas the employment contract is largely limited to rights and duties. Furthermore, our courts have held that the employment relationship can continue even though the employment contract has come to an end.³⁸

35 See Basson et al *Essential Labour Law I* (1998) 21-24.

36 See Basson et al *Essential Labour Law I* (1998) 21-24.

37 See Basson et al *Essential Labour Law I* (1998) 21-24.

38 See the *NAAWU v Borg Warner SA (Pty) Ltd* 1994 ILJ 509 (A) case where the court held that even though the employment contracts of the employees in question had been terminated, they were still entitled to relief.

The employment relationship is not evenly balanced with the employer typically having a position of far superior negotiating strength as compared to the employee.³⁹ The relationship is characterised by the following two important aspects, namely:

- (a) the existence of a relationship of authority⁴⁰ between the employer and employee; and
- (b) the existence of different rights and duties, attributed to the parties on an individual and collective basis in relation to each other.⁴¹

2 3 Breakdown of the employment relationship

In general, an employer is entitled to dismiss an employee (a) by virtue of serious misconduct, incapacity or incompetence if it is just and fair to do so; (b) if his conduct constitutes a material breach of the employment contract; or (c) when it appears that the relationship of trust between the parties has broken down irretrievably.⁴²

Wrongful termination of the employment contract by an employer, constitutes a breach of contract and the employee is entitled to all the ordinary contractual remedies such as reinstatement (specific performance), cancellation of contract and compensation (damages).⁴³ Furthermore, if the dismissal was not fair in a substantive or procedural sense, it may also constitute an unfair dismissal as contemplated in the

39 See Davies & Friedland *Kahn-Freud's Labour and the Law* (1983) 18.

40 See Van Jaarsveld, Van Eck & Kruger *Kompendium van Suid-Afrikaanse Arbeidsreg* (1992) par 57.

41 Employers and employees have definite basic rights, which are enforceable against each other. These rights and duties normally flow from a contract of employment (the individual labour contract) that exists between the parties. Collective labour law is different, with the source of rights and duties stemming from legislation and collective agreements. In this respect international labour rights have an important influence on the South African model because of the recognition and implementation thereof by both legislative and judicial bodies.

42 Butterworths *The Law of South Africa Volume 13(1) Labour Law*.

43 *TAWU v Natal Co-operative Timber Ltd* 1992 ILJ 1154 (D); *Info DB Computers v Newby* 1996 ILJ 32 (W); *Toerien v Stellenbosch University* 1996 ILJ 56 (C); *Jeffrey v*

Labour Relations Act 66 of 1995.⁴⁴ Subsequently, an employee may be entitled to various remedies in terms of the Labour Relations Act 66 of 1995.⁴⁵ Likewise, if the contractual relationship is wrongfully or unfairly terminated by an employee, such termination may be unfair or could constitute a breach of contract, entitling an employer to the ordinary contractual remedies or the remedies provided for in the Labour Relations Act.⁴⁶

Several requirements must be complied with before a dismissal of an employee by his employer can be regarded as fair and reasonable:

- (a) the dismissal must qualify as a dismissal in terms of the Labour Relations Act;⁴⁷
- (b) only an employee as defined in the Labour Relations Act⁴⁸ is entitled to the protection afforded by the doctrine of unfair dismissals;⁴⁹
- (c) the reason(s) for the dismissal must be fair (substantive fairness);⁵⁰ and

Persetel (Pty) Ltd 1996 ILJ 388 (IC); *Sun Packagings (Pty) Ltd v Vreulink* 1996 ILJ 633 (A).

44 See s 187 and s 188 of the Labour Relations Act 66 of 1995.

45 According to s 185 of the Labour Relations Act 66 of 1995 "every employee has the right not to be unfairly dismissed".

46 66 of 1995.

47 See s 186 of the Labour Relations Act 66 of 1995.

48 66 of 1995.

49 The employment relationship is more extensive than the mere contractual relationship between the parties and would survive should the contractual relationship be terminated; see *NAAWU v Borg Warner SA (Pty) Ltd* 1994 ILJ 509 (A) where the court said: "It is therefore sufficient that the legislature clearly had in mind that once a particular relationship is established, the parties to it remain 'employee' and 'employer' as defined beyond the point of time at which the relationship would have terminated under the common law. Where it includes also former employees seeking re-employment or re-instatement, it has placed no limitation suggesting when – or why – a former employee no longer falls within the definition." Also see *NUM v East Rand Gold & Uranium Co Ltd* 1991 ILJ 1221 (A) where a distinction was made between a contractual and a legal relationship.

- (d) the way (procedure) in which it was done must also be fair (procedural fairness).⁵¹

Furthermore, the Labour Relations Act⁵² sets out a Code of Good Practice, which provides guidelines to be followed by an employer before dismissing an employee. However, it must be stressed that the guidelines are not hard and fast rules and an employer's non-compliance with a particular guideline will not necessarily make the dismissal unfair.⁵³

In light of the above employers should take special precaution against the summary dismissal of employees based on inapposite use of employer electronic communication systems. The principles of fairness (both substantive and procedural) must be followed before an employee is dismissed for misconduct and good reasons must be present.

The question arises as to when an employee can be dismissed for contravening the electronic communication policy of the employer? In considering this question it is important to look at the reason for dismissal. In this case it will be misconduct based on contravening the electronic communication policy of the employer. Since misconduct implies that the employee has done something wrong or transgressed a rule, the question should be asked whether a rule (in this case a rule contained in the electronic communication policy of the employer) is reasonable and whether it has been consistently applied?⁵⁴ If the answer is affirmative the next question is whether the employee was aware of the rule?⁵⁵ Finally, once it has been established that (a) a rule exists; (b) is reasonable and applied constantly; and (c) the employee was aware

50 See s 188(1)(a) of the Labour Relations Act 66 of 1995.

51 See s 188(1)(b) of the Labour Relations Act 66 of 1995.

52 66 of 1995.

53 See Basson et al *Essential Labour Law I* (1998) 109.

54 See schedule 8 item 7(b)(i) and (iii) of the Labour Relations Act 66 of 1995.

55 See schedule 8 item 7(b)(ii) of the Labour Relations Act 66 of 1995.

of it, then the only question remaining is what the appropriate sanction should be?⁵⁶ It should be noted that the Labour Relations Act⁵⁷ expects employers to use dismissal only as a last resort and should therefore only consider it for serious misconduct or repeated offences making a continued employment relationship intolerable.⁵⁸ As a result employers should decide whether acts of employees contravening their electronic communication policies are of such a serious nature as to justify dismissal. Examples of serious acts that may justify dismissal include criminal activities, or acts resulting in potential delictual liability for the employer. First offence actions consisting of merely wasting the employer's time should rather be corrected with disciplinary steps short of dismissal. This concept of corrective discipline is underscored by the Labour Relations Act.⁵⁹

In the CCMA matter *Cronje v Toyota Holdings*,⁶⁰ the commissioner found justification for an employer's decision in dismissing an employee who contravened its email policy by circulating racist material. Based on this decision, the circulation of inappropriate material by using the electronic communication system of the employer may be seen as a good enough reason to justify dismissal. However, the need for an employee to be warned before being dismissed is generally accepted and will be a factor in establishing the fairness of such a dismissal.⁶¹ The purpose of a warning is to impress upon the employee the seriousness of his actions as well as the possible future consequences that might ensue if he misbehaves. This approach regard the purpose of discipline as a means for employees to know and understand what standards are required of them in an effort to rectify unwanted behaviour.

56 See schedule 8 item 7(b)(iv) of the Labour Relations Act 66 of 1995.

57 66 of 1995.

58 See schedule 8 item 3(4) of the Labour Relations Act 66 of 1995.

59 See schedule 8 item 3(2) of the Labour Relations Act 66 of 1995.

60 *Cronje v Toyota Holdings* 2001 3 BALR 213 (CCMA).

61 See schedule 8 item 3 of the Labour Relations Act 66 of 1995.

2 4 Role of workplace forums

The system of workplace forums is an innovating aspect of labour law in South Africa. This system allows for employees to obtain joint consultative powers in the management of matters that concern them. Although the concept is relatively new⁶² in South Africa, it is well known internationally.⁶³

According to the ministerial task team⁶⁴ it was necessary to produce products of high quality and improve productivity levels in order for South Africa to compete successfully in international markets. In order to achieve this substantial restructuring was required. The system of adversarial labour relations was unsuitable for such restructuring, and other countries with similar systems not supplemented by employees' representation in the workplace, such as the United Kingdom, experienced labour unrest as a result. Workplace structures focussing on employee participation have been successful in other countries such as Japan and Germany.⁶⁵ Therefore the task team suggested that workplace forums could resolve the problems faced in the South Africa labour market.

"Workplace forums are designed to facilitate a shift at the workplace, from adversarial collective bargaining on all matters to joint problem-solving and participation on certain subjects. In creating a structure for ongoing dialogue between management and workers, statutory recognition is given to the realisation that unless workers and managers work together more effectively they will fail adequately to

62 Regarding the history of the concept, see Wiehahn Report; Nel & Van Rooyen *Worker Representation in Practice in SA* (1987); Du Plessis 'n *Arbeidsregtelike Studie met betrekking tot die Deelname van Werknemers in die Besluitnemingsprosesse in Nywerhede* (1984) Unpublished thesis University of South Africa.

63 See Daubler 1975 ILJ (UK) 218; Bullock "Committee of Inquiry on Industrial Democracy" 6706 *Report Command Paper*; Carby-Hall *Worker Participation in Europe* (1977); European Community Council Directive 94/45/EC of 22 September 1994 (institution of a European Workers Council).

64 See Explanatory Memorandum 1995 ILJ 310.

improve productivity and living standards. Workplace forums are designed to perform functions that collective bargaining cannot easily achieve - that is the joint solution of problems and the resolution of conflicts over production. Their purpose is not to undermine collective bargaining but to supplement it. They achieve this purpose by relieving collective bargaining of functions to which it is not well suited. The forum's focus is qualitative – that is, it is on non-wage matters, such as restructuring, the introduction of new technologies and work methods, changes in the organisation of work, physical conditions of work and health and safety, all issues best resolved at the level of the workplace. Workplace forums expand worker representation beyond the limits of collective bargaining by providing workers with an institutionalised voice in managerial decisions. Employers receive different benefits from the workplace forum: increased efficiency and performance."⁶⁶

It is important for employers to realise the importance of workplace forums. Employers are advised to include such forums when making decisions on the implementation of company policies (for example an electronic communication policy) that will have a direct effect on employees. As a result a company policy decision may be seen as a joint venture between an employer and his employee rather than a "one-sided" implementation based on employer authority.

65 See Zöllner & Loritz *Arbeitsrecht* 437; Hanau & Adomeit *Arbeitsrecht* 113. Also see Robinson *Worker Participation* 49.

66 See Government Gazette 16259 135.

3 Constitutional and statutory implications

3.1 General

The rights and duties of parties involved in the employer-employee relationship have to some extent been codified through constitutional and statutory enactments. Before the Constitution of the Republic of South Africa⁶⁷ fundamental rights and duties could only be determined by the application of general common law principles. Given the myriad of potential abuses and invasion of rights, coupled with impending technological developments, legislation that allows interception and monitoring of communications has to be stringently examined and even more stringently applied, if it is to enjoy an ongoing constitutionally valid status.

3.2 Privacy issues

The common law right to privacy, as an independent personality right included within the concept of *dignitas*, has always been recognised in South African law.⁶⁸ As such, the concept and scope of "privacy" has been widely defined and interpreted through the years, but at the very least it includes the right to be free from intrusions and interference by the state and individuals.⁶⁹ Furthermore, it includes the freedom from unauthorised disclosures of information about one's personal life.^{70 71} In addition, it

67 Constitution of the Republic of South Africa 108 of 1996.

68 See McQuoid-Mason *The Law of Privacy in South Africa* (1978) 9. The right to privacy is also featured in most international and regional human rights instruments. For example, art 12 of the Universal Declaration on Human Rights; art 17 of the International Covenant on Civil and Political Rights; art 8 of the European Convention on Human Rights.

69 Ackermann J in *Bernstein and others v Bester & others NNO* 1996 2 SA 751 (CC) provides an excellent analysis of this interpretation at par 65 note 89 citing Dionisopoulos & Ducat *The Right to Privacy* (1976).

70 See *Case v Minister of Safety and Security* 1996 3 SA 617 (CC). Although this case dealt with the right to privacy extending to the possession of pornographic material in one's home, this right of non-disclosure is seeing increasing manifestation in the area of sexual orientation, health and disclosure of medical records, particularly with regard to HIV/AIDS.

connotes that individuals should have control over not only the "inner sanctum"⁷² of their communications and the contents of them, but also who has access to the flow of information about them.⁷³ The common law right to privacy was also entrenched in the Constitution of the Republic of South Africa.⁷⁴ A specific incident of this general right includes the right not to have communications infringed.⁷⁵

The right to privacy is afforded protection both in relation to intrusion into a person's private life⁷⁶ by the state or by other individuals. The rights to privacy and human

71 In the *Mistry* case *supra*, the Constitutional court by mouth of Chaskalson JP raised the question whether "a person has a constitutional right to privacy in respect of information concerning himself or herself". Although the judge felt that the facts of the case did not compel him to explore this further, he did assume that a right to informational privacy is covered by the broad protection of privacy guaranteed by s 13 of the Constitution of the Republic of South Africa (Interim Constitution) 200 of 1993.

72 The importance of the right to privacy has been emphasised by the Constitutional Court in *Bernstein v Bester* 1996 4 BCLR 449 (CC) 484D 491G–H and in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 1 SA 545 (CC).

73 McQuoid-Mason *The Law of Privacy*. The final conclusions of the Nordic Conference on the Right to Respect for Privacy of 1967 included the following additional elements of the right to privacy: (a) the prohibition to use a person's name, identity or photograph without his or her consent; (b) the prohibition to spy on a person; and (c) respect for correspondence and the prohibition to disclose official information. See *Bernstein v Bester supra*.

74 S 14 of the Constitution of the RSA 108 of 1996.

75 See s 14(d) of the Constitution of the RSA 108 of 1996. In terms of the Interception and Monitoring Prohibition Amendment Act 77 of 1995, a judge is required to approve the tapping of a telephone or interception of mail. The judge must be convinced that an actual or impending serious offence cannot be investigated in any other way, or that the security of the state is threatened. See *S v Naidoo* 1998 1 BCLR 46 (D) where the right to privacy of the accused had been infringed in that the police intercepted telephone conversations contrary to the provisions of the Interception and Monitoring Prohibition Act 127 of 1992. Evidence relating to the contents of the telephone conversations was excluded because its admission would have rendered the trial unfair – the right against self-incrimination which strikes at one of the fundamental tenets of a fair trial, had been violated – and it would have been detrimental to the administration of justice.

76 *D v K* 1997 2 BCLR 209 (N), in which the Natal Provincial Division held that a blood test on a non-consenting adult constituted an assault and an invasion of personal

dignity are inextricably intertwined. The right to privacy has as its objective the preservation for each individual of "the choice of when and how much he will allow others to know about his personal affairs or interfere with his or her mind, or body, or private activities".⁷⁷

Privacy is a relative newcomer to the body of justiciable and fundamental rights. The right to privacy in the workplace is a contentious issue since the employee's right to privacy (as afforded by the Constitution⁷⁸) competes with the employer's right to manage and conduct a business in an efficient manner and with limitation of risk.

The Constitutional Court illustrated in the *National Coalition*⁷⁹ case that "privacy recognises that we all have a right to a sphere of private intimacy and autonomy which allows us to establish and nurture human relationships without interference from the outside community". Likewise, in the US case *Olmstead v United States*⁸⁰ the judge described privacy as the "right to be left alone - the most comprehensive of rights and the most valued by civilised men".

However, the right to privacy is not absolute. For example, society may want to limit such rights in the investigation and prosecution of crime. Such limitations must of course be in line with the constitution.⁸¹

privacy. Such an intrusion of personal privacy cannot be justified by the competing interests of securing evidence or ascertaining the truth in a civil action between private parties where the paternity of a minor is in dispute. The court held that less intrusive methods could be used effectively.

77 The Guide to American Law *VIII* (1984) 288.

78 108 of 1996.

79 *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 1 SA 6 (CC).

80 *Olmstead v United States* 1928 277 US 438 475-476 478.

81 S 36(1) of the Constitution of the RSA 108 of 1996 states that "The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that 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".

A comprehensive and rational social security system can bring about the potential scope for privacy violations.⁸² In *Bernstein v Bester*⁸³ the Constitutional Court remarked that "privacy is acknowledged in the truly personal realm, but as a person moves into communal relations such as business and social interaction, the scope of personal space shrinks accordingly".⁸⁴

The *Bernstein v Bester* case *supra* concerned the constitutionality of the "summons and examination" provisions contained in the Companies Act 61 of 1973 on the basis that the provisions violate a cluster of interrelated and overlapping constitutional rights, which include the right to privacy.⁸⁵ It was argued that the compulsory production of documents under these provisions constituted a "seizure" within the meaning of the right not to be subject to the "seizure of private possessions".⁸⁶ The principles contained in the *Bernstein v Bester* case *supra*, correspond with those espoused in Canadian and United States case law on surveillance and the right to privacy. Both jurisdictions prohibit the unlawful interception of communications on

82 Freedman *Social Security Law: General Principles* 515–517.

83 *Bernstein v Bester* 1996 4 BCLR 449 (CC) 484D 491G–H; 1996 2 SA 751 (CC).

84 This statement was revisited in *Investigating Directorate v Hyundai supra*. The court noted that the *Bernstein* judgement did not say that when people moved beyond the "intimate core" they "no longer retained a right to privacy in the social capacities in which [they acted]". They still retained a right to be left alone, whether they were in their offices, in their cars or on mobile telephones, "unless certain conditions were satisfied". In essence, the intensity of the right to privacy depends on how close it moves "to the intimate personal sphere of the life of human beings".

85 S 417 of the Companies Act *supra* provides for the summoning and examination of persons regarding the affairs of a company that is winding-up and unable to pay its debts. The clause under scrutiny provided that the person concerned had to answer any question notwithstanding the risk of self-incrimination and the fact that the answer may thereafter be used in evidence against him. S 418 of the Act created a criminal offence for a person examined under s 417 who failed to answer a question "fully or satisfactorily". S 417 and s 418 were also alleged to violate the constitutional rights to freedom and security of the person (s 11(1) of the Constitution *supra*) and the general right to personal privacy, which embraces the right not to be subject to seizure of private possessions or the violation of private communications (s 13 of the Constitution *supra*).

86 S 13 of the Constitution of the Republic of South Africa (Interim Constitution) 200 of 1993.

the grounds that it constitutes a search or seizure.⁸⁷ The prohibition's aim is to protect a reasonable expectation of privacy, which is violated when a third party intercepts a telephone conversation without the consent or knowledge of the parties.⁸⁸

Privacy rights pertaining to interception and monitoring of communications are receiving more attention in South African jurisprudence. The courts have generally dealt with these issues on a case-by-case basis. Two broad issues generally tend to be raised for consideration by the courts: (a) whether the alleged monitoring of communications constitutes a breach of the right to privacy; and (b) whether the manner in which the evidence was obtained affects its admissibility.

With regards to the first issue, violations of private communication have long been recognised as invasions of privacy in South African law. For example, in the case *S v A*⁸⁹ the court held that eavesdropping and electronic surveillance by private detectives during matrimonial disputes might result in a criminal invasion of privacy if the methods used are unreasonable. Furthermore, the case *S v Naidoo*⁹⁰ found that while surveillance may be necessary in order to facilitate effective police work, it may only be carried out pursuant to a judicial authority. Monitoring that occur without such authority is in violation of the constitutional right to privacy. Cases pursuant to *Naidoo supra* have shared the view that only an "overriding justification of public

87 The Fourth Amendment of the US Constitution governs not only the seizure of tangible items but extends as well to the recording of oral statements. See *Silverman v United States* 1961 US 365 505 511; *Katz v United States* 1967 389 US 347; *Oliver v United States* 1984 466 US 170; *United States v Mancini* 1993 US 8 F 3d 104 109.

88 The Canadian Criminal Code does, however, make provision for the electronic interception of private telephone conversations, under a warrant issued by a superior court judge, based on reasonable and probable grounds. When the Criminal Code's regime of judicial authorisation is complied with, the wiretap, although obviously still a search and seizure by definition, is rendered lawful and reasonable. See Hogg *Constitutional Law of Canada* 3ed II (1996) 45-70.

89 *S v A* 1971 2 SA 293 (T). In this case, private detectives were convicted on charges of *crimen injuria* for installing a "transmitter wireless microphone" under the complainant's dressing table at the request of an estranged spouse.

90 See *S v Naidoo supra*. Here the court had to consider the admissibility of evidence in criminal proceedings obtained via an unlawfully monitored conversation.

interest" could prevail against the unlawful manner in which information was obtained and the infringement on the right to privacy that ensues.⁹¹ The exact content given to the vague notion of "public interest" remains imprecise.⁹² In the *Protea Technology*⁹³ case it was stated that whether a constitutional right should prevail with unmitigated force would have to depend on the merits of the case and a discretion exercised with due regard to s 36(1) of the Constitution,⁹⁴ the limitations clause. This invariably involves a balancing act, in that the interest of uncovering the truth (which is always in the public interest) is measured against the interests of protecting the right to privacy.

In most cases, surveillance legislation fails to discriminate sufficiently between communications warranting interception and those not warranting it.

91 See *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 2 SA 451 (A).

92 In the *Financial Mail* case *supra*, two important ratios emerged: first, that there is a wide difference between what is interesting to the public and what is in the public interest and second, that there is a public interest of a high order in preserving confidentiality in regard to private affairs.

93 *Protea Technology Ltd v Wainer* 1997 9 BCLR 1225 (W).

In this case, the matter to be decided was whether clandestine tape recordings made of the respondent were admissible as evidence or whether the recordings had been made in contravention of s 2 of the Interception and Monitoring Prohibition Act 127 of 1992 or whether the recordings had been made in breach of the respondent's constitutional right to privacy. The court found that the respondent had been employed by the applicant in a position of trust. The telephone conversations were conducted from the applicant's business premises within business hours. Where the parties stood to each other in the relationship of employer and employee, telephone conversations of the employee relating to the employer's affairs were not private and were not protected under the constitution. The court held further that an employer could not listen to private conversations although it could expect the employee to account for his or her activities during the employer's time. However, as soon as the employee abandoned the private sphere for that of the affairs of his employer, he lost the benefit of privacy. The judge held further that "an employer's bona fide interest extends to the manner in which the employee carries out his duties and there is no invasion inherent in exposing such matters to the employer's ear (or eye)". The judge held further that "telephonic conversations of the employee relating to the employer's affairs are not private and are not protected under the constitution".

94 108 of 1996.

"There is thus an encroachment on other people's privacy and not only that of the person that one actually wants to bring to book."⁹⁵

Problems of this nature are not limited to censorship type legislation. It is common to legislation that encroaches, albeit justifiably, on a fundamental constitutional right, such as monitoring legislation. Even though the law may target individuals suspected of committing serious offences, or posing a threat to the national security, it reaches further. The reach of such legislation may potentially extend to include journalists, human-rights organisations, political dissidents and opposition, as well as innocent individuals living in close proximity to those being monitored.

In the Swiss case *Kopp*⁹⁶ the European Court of Human Rights found that the Swiss government's tapping of an employee's line in a law firm constituted a breach of art 8 of the EC Human Rights Treaty, which guaranteed the right to privacy.⁹⁷ The worst of the violations was noted as being the monitoring of the law firm's partners and employees, clients and third parties whom had no connection with the criminal proceedings. The court found that

"This exceeds the bounds of what is required to protect democratic institutions and amounts to a perverse inquisition."

95 P C de Jager, MP, made this point during the parliamentary debates on the Interception and Monitoring Bill. He noted that "what makes this Bill even more unacceptable is that it is not only the suspect's telephone conversations which may be monitored, but also those of his wife and daughter, even when she is talking to her fiancé".

96 *Kopp v Switzerland European Court of Human Rights* 1998 13/1997/797/1000. Also see the EC Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications (96/C 329/01).

97 The case involved the illegal wiretapping of a lawyer's office telephone on the grounds of national security. The law did not clearly state how, under what conditions and by whom a distinction was to be drawn between matters specifically connected with a lawyer's work under instructions from a party to proceedings and those relating to other activities. The court held that it was wholly unacceptable to assign the task of monitoring to an official of the Post Office's legal department, a member of the executive, without supervision by an independent judge.

Justice Brandeis enunciated this concern in the US case *Olmstead v United States*⁹⁸ when he said:

"Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded and all conversations between them upon any subject and although proper, confidential and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping."

It is submitted that what is said with regards to the tapping of telephone conversation applies equally to the monitoring of electronic communications.

If employees do in fact have some right to privacy in the workplace, what affect does the inequality of bargaining power between employer and employee have? For example, if employees were allowed to "negotiate" their right to privacy away in an employment contract then the right would be of little benefit. An employment contract might include provisions that determine how company resources may be utilised by employees and whether allowance will be made for personal use. Most often such contracts refer to a company policy, which might include detail on what will be allowed, and what not. The question arises whether such contractual provisions are seen as in conflict with basic conditions of employment.

The Basic Conditions of Employment Act (BCEA) 75 of 1997 forms part of any employment relationship and an employee may enforce the provisions contained therein as if it were part of the employment contract. However, since the BCEA⁹⁹ does not specifically deal with these issues it is submitted that the question is answered in the negative. By including a notification in the employment contract that electronic communication are subject to monitoring, for example, employers can in

98 See *Olmstead v United States supra*.

99 75 of 1997.

essence destroy any expectation of privacy that employees may have.¹⁰⁰ By implementing privacy-invasive policies and practises the right to privacy in the workplace are of little consequence as a result of the management prerogative.¹⁰¹ Ford called it a "perverse logic" whereby the expectation of privacy gets reduced as more workers are subjected to intrusive surveillance.¹⁰²

With regards to the second issue ie "whether the manner in which the evidence was obtained affects its admissibility", the *Fedics Group v Matus*¹⁰³ case illustrates the courts' view that steps must be taken to protect business assets. In this case the evidence (certain documents) were obtained in a manner, which infringed on the respondent's constitutional rights to dignity and privacy. After comparing the position in criminal and civil cases the court held that it has a discretion to allow such evidence in civil cases. Furthermore, the court held that this discretion needs to be considered with care and by taking into account all the circumstances of a particular case.

100 See the UK case *Halford v United Kingdom* 1997 73/1996/692/884 and US case *Smyth v Pillsbury Co* 1996 US. Also see *Protea Technology supra*, which shows that as soon as the employee abandoned the private sphere for that of the affairs of his employer, he loses the benefit of privacy.

101 Oliver "Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out" 2002 *Industrial Law Journal* 336.

102 Ford "Surveillance and Privacy at work" 1998 *London: Institute of Employment Rights* 50.

103 In the case *Fedics Group v Matus* 1997 9 BCLR 1199 (C) one of the issues to be decided was when and under what circumstances an employer would be entitled to search the office or part of the office of his employee. The judge examined various approaches in international case law and found that there were no absolute rules in regard to this area. The answers to the question whether an employee has the right or a legitimate expectation of privacy to his office as well as to the question when an employer will be justified to invade that right of privacy, depend on the circumstances of each case. In this particular case the judge held that the search of the respondent's office constituted a violation of her constitutional rights to dignity and privacy. He held further that it must also be accepted that the aforesaid question is not an easy one and that the advice obtained by the applicant from counsel that it was permitted to search the respondent's office was not unreasonable. The judge further noted that all the documents found during the search of the respondent's office were discoverable and as such could have been legitimately obtained by the applicants at some stage during the proceedings. The court held that in light of the above it would allow the admission into evidence of the documents found by the applicant during the search of the respondent's office.

3 3 Statutory issues

3 3 1 Interception and Monitoring Prohibition Act 127 of 1992

The Interception and Monitoring Prohibition Act (IMPA) 127 of 1992 was enacted "to prohibit the interception of certain communications and the monitoring of certain conversations or communications", in addition to addressing issues relating to the interception of postal articles.

IMPA¹⁰⁴ prohibits the interception of any communication over a telephone or other telecommunications line without the knowledge or permission of the sender.¹⁰⁵ In essence s 2(1)(a) of IMPA¹⁰⁶ means that the interception of a telephone conversation by a third party or the recipient without the knowledge or permission of the dispatcher to the communication, is illegal. The illegality of the interception would depend to a great extent on the meaning of the word "intercept".¹⁰⁷ It is my view that the recording of a conversation, to which one is a party, cannot be described as "interception" under s 2(1)(a).

104 127 of 1992.

105 S 2(1)(a) of the Interception and Monitoring Act 127 of 1992.

106 127 of 1992.

107 See the court's definition of "intercept" in the *Diablo Trade 28 (Pty) Ltd v Madiba Air (Pty) Ltd* 1999 3 All SA 305 (W) case. It appears that the court affixed words such as "seize", "stop" and "obstruct" to the meaning of "intercept" as contained in the Interception and Monitoring Prohibition Act 127 of 1992. The court found that a communication made directly over a telephone required no interception by the recipient in the course of its progress along the line. Also see the *Protea Technology* case *supra* where the court found "intercept" to bear the meaning of "to check" or "cut off the passage from one place to another".

Furthermore, IMPA¹⁰⁸ prohibits the intentional monitoring¹⁰⁹ of any conversation or communication so as to "gather confidential information concerning any person, body or organisation".¹¹⁰ ¹¹¹ S 2(1)(b) only prohibits the monitoring of a conversation or communication if the purpose is to gather confidential information. That necessarily implies that if the information or communication is not confidential, then it is not illegal to monitor a conversation, even if the purpose is to gather information.¹¹² But how do you know if communication is confidential before monitoring it? In the *Protea Technology* case *supra* the court found it will be necessary to consider why a communication was monitored in order to ascertain whether the purpose was to gather confidential information. Furthermore, the court said it might be necessary to examine the contents of a communication in order to establish that purpose.

108 127 of 1992.

109 The Interception and Monitoring Act 127 of 1992 defines "monitoring" as "includes the recording of conversations or communications by means of a monitoring device" and "monitoring device" as "any instrument, device or equipment which is used or can be used, whether by itself or in combination with any other instrument, device or equipment, to listen to or record any conversation or communication".

110 S 2(1)(b) of the Interception and Monitoring Act 127 of 1992.

111 In the *Protea Technology* case *supra* the court attempted to define "monitoring" by affixing phrases to it such as "to listen to and report on (radio broadcasts, especially from a foreign country)", "to eavesdrop on (a telephone conversation)", "to keep track of by means of an electronic device" and "to scrutinise or check systematically (with a view to collecting certain categories of data)". Furthermore, the court found it unnecessary to decide whether the legislator intended any other meaning besides "simple eavesdropping".

112 In the *Protea Technology* case *supra* the court found "confidential information" to mean "such information as the communicator does not intend to disclose to any person other than the person to whom he is speaking and any other person to whom the disclosure of such information is necessarily or impliedly intended to be restricted."

It must be noted that the courts have found that IMPA¹¹³ did not render the production of recordings made in contravention of its provisions inadmissible before a court trying a civil dispute.¹¹⁴ However, in *S v Naidoo supra* the court found such evidence inadmissible in criminal disputes.¹¹⁵

IMPA¹¹⁶ also provides for monitoring by means of a court order issued by a judge under s 3, provided that the judge is convinced that (a) "the offence that has been or is being or will probably be committed, is a serious offence that cannot be properly investigated in any other manner and of which the investigation in terms of this act is necessary"; or (b) "that the security of the Republic is threatened or that the gathering of information concerning a threat to the security of the Republic is necessary". This clearly relates to monitoring of suspected criminal activity and does not allow for monitoring in the general scope of business.

113 127 of 1992.

114 See *Protea Technology supra* and *Diablo v Madiba Air supra*.

115 See *S v Naidoo supra* where the right to privacy of the accused had been infringed in that the police intercepted telephone conversations contrary to the provisions of the Interception and Monitoring Prohibition Act *supra*. Evidence relating to the contents of the telephone conversations was excluded because its admission would have rendered the trial unfair – the right against self-incrimination which strikes at one of the fundamental tenets of a fair trial, had been violated – and it would have been detrimental to the administration of justice.

116 127 of 1992.

3 3 2 Electronic Communications and Transactions Act 25 of 2002

For the first time electronic communication (for example email) is legally recognised through the enactment of the Electronic Communications and Transactions Act (ECTA) 25 of 2002. In terms of the ECTA,¹¹⁷ information will not be without legal effect simply because it was embodied in an electronic message.¹¹⁸ In addition, the legal requirement that information must be in writing will be met by an electronic message if that message is usable for subsequent reference.¹¹⁹

An agreement concluded by means of electronic messages is given legal effect by the ECTA.¹²⁰ In addition, the ECTA¹²¹ provides for the protection of personal information obtained through electronic transactions.¹²² As such the ECTA¹²³ contains certain principles for electronically collecting personal information.¹²⁴ One such principle requires that a data controller must obtain the permission of a person when collecting or storing personal information about that person, unless otherwise required by law.¹²⁵ It should be noted that the principles contained in s 51 of the ECTA¹²⁶ are voluntary and a data controller can subscribe thereto by recording such fact in any

117 25 of 2002.

118 S 11(1) of the Electronic Communications and Transactions Act 25 of 2002.

119 S 12 of the Electronic Communications and Transactions Act 25 of 2002.

120 S 22(1) of the Electronic Communications and Transactions Act 25 of 2002.

121 25 of 2002.

122 S 86(2) of the Electronic Communications and Transactions Act 25 of 2002 prohibits the interfering with data "in a way which causes such data to be modified, destroyed or otherwise rendered ineffective". However, this does not prohibit the monitoring or interception of data where such data is not "modified, destroyed or otherwise rendered ineffective".

123 25 of 2002.

124 S 51 of the Electronic Communications and Transactions Act 25 of 2002.

125 S 51(1) of the Electronic Communications and Transactions Act 25 of 2002.

126 25 of 2002.

agreement¹²⁷ with a data subject.¹²⁸ Furthermore, s 50(2) of the ECTA¹²⁹ stipulates that a data controller must subscribe to the principles as a whole and will not be allowed to partially subscribe.

The ECTA¹³⁰ also makes provision for tackling "Cyber Crime". For this purpose the ECTA¹³¹ makes provision for the appointment of "cyber inspectors" who have wide powers to monitor Internet communications and the activities of cryptography and authentication service providers.¹³² In addition, the ECTA¹³³ makes it an offence, subject to the IMPA¹³⁴ to access or intercept data without being authorised¹³⁵ thereto.¹³⁶ Likewise, the unlawful production, selling, offer to sell, procures for use, etc of products designed to assist in the above activities are also prohibited.¹³⁷ In effect, this could be interpreted to mean that employers have to obtain consent from employees before accessing their electronic communications or be otherwise authorised to do so (for example by way of legislation such as the Regulation of

127 S 50(4) of the Electronic Communications and Transactions Act 25 of 2002 stipulates that "The rights and obligations of the parties in respect of the breach of the principles outlined in s 51 are governed by the terms of any agreement between them."

128 S 50(2) of the Electronic Communications and Transactions Act 25 of 2002.

129 25 of 2002.

130 25 of 2002.

131 25 of 2002.

132 S 81 of the Electronic Communications and Transactions Act 25 of 2002.

133 25 of 2002.

134 127 of 1992.

135 S 86(4) of the Electronic Communications and Transactions Act 25 of 2002 renders it an offence to utilise "any device or computer program...in order to unlawfully overcome security measures designed to protect such data of access thereto".

136 S 86 of the Electronic Communications and Transactions Act 25 of 2002.

137 See s 86(3) of the Electronic Communications and Transactions Act 25 of 2002 for a complete list of unlawful acts.

Interception of Communications and Provision of Communication-Related Information Act 70 of 2002). It could however also be argued that an employer should, in principle, always be authorised to access any information on its own computer systems, and therefore this section by itself may not prevent monitoring by the employer.¹³⁸

3 3 3 Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

IMPA¹³⁹ was enacted "to prohibit the interception of certain communications and the monitoring of certain conversations or communications", in addition to addressing aspects of the interception of postal articles. The Regulation of Interception of Communications and Provision of Communication-Related Information Act (Interception Act) 70 of 2002 was assented to during December 2002. Apart from provisions being made to validate the directions previously granted and also to confirm the designations of judges under IMPA,¹⁴⁰ the Interception Act¹⁴¹ repeals IMPA¹⁴² in its entirety.¹⁴³ However, at the time of writing no commencement date has yet been established for the Interception Act¹⁴⁴ and IMPA¹⁴⁵ is still the governing legislation.

138 It should be noted that s 86 of the Electronic Communications and Transactions Act 25 of 2002 does not prevent authorised access to electronic communication.

139 127 of 1992.

140 127 of 1992.

141 70 of 2002.

142 127 of 1992.

143 See s 62(1)-(3) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

144 70 of 2002.

145 127 of 1992.

The Interception Act¹⁴⁶ aims, *inter alia*, to set out the basis on which employers can lawfully monitor employees' communications. Accordingly, the Interception Act¹⁴⁷ provides some guidance in determining whether or not an employer acts lawfully when dealing with employee electronic communications, including the monitoring of email and the websites that its employees browse, as well as recording the telephone conversations of employees.

With regards to the Interception Act¹⁴⁸ it should be noted that "intercept" or "interception" is defined in the act as

"the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of a communication available to a person other than the sender or recipient or intended recipient of that communication, and includes the:

- (a) monitoring of any such communication by means of a monitoring device;
- (b) viewing, examination or inspection of the contents of any indirect communication; and
- (c) diversion of any indirect communication from its intended destination to any other destination".¹⁴⁹

146 70 of 2002.

147 70 of 2002.

148 70 of 2002.

149 See definition of "intercept" in the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

The question whether "filtering" amounts to interception is important in determining whether such action is prohibited in terms of the Interception Act.¹⁵⁰ The reason for filtering is of importance when answering this question. The definition of "interception" requires that such reason need to be for the purpose of making "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".

Filtering email messages for the purposes of getting rid of spam is done in order to guard against the cluttering of email inboxes by unsolicited email, and not to make such communication available to somebody other than the "sender or recipient or intended recipient of that communication". It is therefor submitted that "filtering" email for the purpose of getting rid of spam will be excluded from the definition of "interception" under the Interception Act¹⁵¹ and is not prohibited in terms of the Act. Similarly, it is submitted that filtering email for purposes of virus control or the automatic blocking of email containing obscene text will not be prohibited by the Act, since the reason for such filtering is not to make such communication available to somebody other than the "sender or recipient or intended recipient of that communication". However, communications that are filtered for the purpose of "spot checking" in order for employers to ascertain whether employees are transgressing communication policies will fall within the ambit of the "interception" definition, since the reasoning behind such action amounts to making "communication available to a person other than the sender or recipient or intended recipient of that communication".

150 70 of 2002.

151 70 of 2002.

3 3 3 1 General prohibition

The Interception Act¹⁵² contains a general prohibition against the interception of certain communications. As such, s 2 of the Interception Act¹⁵³ states that

"[N]o person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission."

The general prohibition contained in s 2 includes both direct (such as discussions that are face to face) and indirect (such as email, paper memo's, postal mail etc.) communications.

In order to understand what is meant by the words "in the course of its occurrence or transmission" as contained in s 2 the following analysis is supplied. The Interception Act¹⁵⁴ gives us a clue on the interpretation of the phrase in s 1(2), which states that:

"[T]he time during which an indirect communication is being transmitted by means of a telecommunication system includes any time when the telecommunication system by means of which such indirect communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it."

Email messages are stored on an email server, be it a company server, an Internet service provider or free email service provider such as Yahoo. Strictly speaking, if one considers this definition it is clear that as long as the message is stored, for collection or otherwise, on an email server, such message is deemed to be "in the process of being transmitted". It is therefor submitted that viewing or accessing any communication stored on an email server satisfies the "in the course of its occurrence

152 70 of 2002.

153 70 of 2002.

154 70 of 2002.

or transmission" requirement and will amount to a prohibited interception, subject to exceptions, by the Interception Act.¹⁵⁵

When will a communication be deemed "delivered" and as such regarded as falling outside the "course of transmission"? This is an important question since communication classified as falling outside the "course of transmission" will not be prohibited from being intercepted under the Interception Act.¹⁵⁶ As long as communication is stored on a telecommunication system (for example an email server) it will fall within the ambit of in the "course of transmission" provision contained in s 2. It is submitted that this will also include email messages that were received, read and then dropped in a "history" or "archived" folder, provided such folders are stored on the email server. However, if such folders were stored on the hard-drive of an employee's computer it will be communication outside the "course of transmission", since the hard drive is not used to transmit such email.¹⁵⁷

In the labour law matter, *Jacqueline Bamford v Energizer*,¹⁵⁸ it was shown that employers tend to access information kept on the computers of employees in order to obtain the necessary evidence during disciplinary hearings. It seems that employers do not collect the necessary evidence as it travels across the Internet or a corporate Intranet, but rather after its arrival. This is particularly true for smaller organisations that use external service providers. In light of the interpretation of the phrase "in the course of its occurrence or transmission" the Interception Act¹⁵⁹ will not prohibit such action provided that the evidence is deemed "delivered". If not, employers should seek to rely on one of the exceptions contained in the Act.

155 70 of 2002.

156 70 of 2002.

157 See definition of "telecommunication system" in the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

158 *Jacqueline Bamford and Four Others v Energizer (SA) Limited* (CCMA) 2001-6-22.

159 70 of 2002.

In light of the *Bamford* matter *supra* the question arises whether employees have a legitimate expectation of privacy in the workplace and in particular as it concerns their communications as stored on the hard drive of their computers. In the *Protea Technology* case *supra* the Constitutional Court said that as soon as the employee abandoned the private sphere for that of the affairs of his employer, he lost the benefit of privacy. Furthermore, the judge held that telephonic conversations of the employee relating to the employer's affairs are not private and as such not protected under the constitution. In the light of the court's view it would appear that employees don't have a legitimate right of privacy in the workplace as far as using the computer and telecommunication systems of the employer, and dealing with his affairs. There may be times when employees are using their personal computer equipment to attend to the business of the employer. It's submitted that even though an employee may be using his personal computer equipment when dealing with the affairs of the employer, an employee will not have a legitimate right to privacy when dealing with the affairs of the employer.^{160 161}

160 See the *Protea Technology* case *supra* where the judge held that "an employer's bona fide interest extends to the manner in which the employee carries out his duties and there is no invasion inherent in exposing such matters to the employer's ear (or eye)".

161 The *Protea Technology* decision *supra* is in contrast to the CCMA arbitration *Moonsamy v The Mailhouse* 1999 20 ILJ 464 (CCMA) in which the commissioner was dealing with the fairness of a dismissal. The commissioner was required to determine whether the employer had been entitled, in a disciplinary hearing, to use evidence which it had obtained from a recording device fitted to the employee's office telephone at the employer's premises. The commissioner found that the recordings were an invasion of the employee's constitutional right to privacy and that the employer's action in recording the calls, without prior authorisation or the consent of the employee, was not reasonable or justifiable. As a result the commissioner found the evidence to be inadmissible. However, the commissioner did point out that an alternative would be for the employer to obtain the consent of the employee at the inception of the employment relationship or through a consensual amendment to an existing employment agreement. Furthermore, the commissioner went on by saying "Whilst it appears that consent can operate as a defence to an *injuria*, the consent, which would in most cases form an express or implied term and condition of employment, would have to be such that the employee has a full appreciation of the nature and extent of the act to which he or she is voluntarily consenting."

However, a legitimate expectation of privacy may arise in respect of private communications if the employer allows it. Since such an expectation has to be both subjective and objectively reasonable the employer can remove it by giving adequate notice to the employee.¹⁶² This is of particular importance regarding material contained on the hard drive of an employee, which should be accessible by the employer including any private materials of the employee, provided such notice was given in advance.

In general, an employer that intercepts the electronic communication of its employee in contravention of the Interception Act¹⁶³ is committing an offence.¹⁶⁴ Furthermore, the penalty for being found guilty of such an offence is punishable by a fine of up to R2,000,000 or up to ten years imprisonment.¹⁶⁵

3 3 3 2 Exceptions

The general prohibition against intercepting communication does not apply in an unqualified manner. The Interception Act¹⁶⁶ recognises certain instances where the interception of communications may lawfully take place. Those relevant to this dissertation are as follows:

- (a) The authorised person who executes an interception direction or assists with the execution thereof may intercept any communication, to which such interception direction relates.¹⁶⁷

162 See the *Bernstein v Bester* case *supra*.

163 70 of 2002.

164 See s 49 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

165 See s 51(b)(i) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

166 70 of 2002.

167 See s 3(a) and (b) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

(b) Any communication may be intercepted by one of the parties to that communication, provided that such communication is not intercepted for the purpose of committing an offence.^{168 169} For this purpose, it should be noted that a party to a direct communication is "any person participating in such direct communication or to whom such direct communication is directed, or in whose immediate presence such direct communication occurs and is audible to the person concerned, regardless of whether or not the direct communication is specifically directed to him or her", whereas a party to an indirect communication is the sender or (intended) recipient(s) of such communication, or "if it is intended by the sender of an indirect communication that such indirect communication be received by more than one person, any of those recipients; or any other person who, at the time of the occurrence of the indirect communication, is in the immediate presence of the sender or the recipient or intended recipient of that indirect communication".¹⁷⁰ From this definition it can be deduced that employers can legally intercept the communications of employees provided they are a party thereto.

168 See s 4(1) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

169 A tape recording (made at the instigation of a suspect) of a conversation between a suspect and accused was also not inadmissible under the provisions of the Interception and Monitoring Prohibition Act 127 of 1992. Obtaining such evidence does not infringe on the accused's right of privacy. See *S v Kidson* 1999 1 SACR 338 (W) and *Diablo v Madiba Air* case *supra*.

170 See definition of "party to the communication" in the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

- (c) Any person may intercept any communication if one of the parties to the communication has given their prior consent to such interception in writing,¹⁷¹ provided that such communication is not intercepted for the purpose of committing an offence.¹⁷² It is submitted that in terms of this section employers may legally intercept employee communications by satisfying the consent requirement above, provided that prior written permission is obtained.¹⁷³ For this purpose, it should be noted that a party to a direct communication is any participant or any person, to whom the direct communication is directed, whereas a party to an indirect communication is the sender or (intended) recipient(s) of such communication.¹⁷⁴
- (d) Any person may intercept any indirect communication in the course of the carrying on of any business provided that certain requirements are met.¹⁷⁵ This exception is particularly useful given the fact that employers are not required to be a party to or have the written permission of their employees to intercept employee communications.

171 The requirement that consent has to be in writing will be met if it is in the "form of a data message" and "accessible in a manner usable for subsequent reference" - see s 12 of the Electronic Communications and Transactions Act 25 of 2002. It is submitted that a user "clicking" on a confirmation button after being prompted by an electronic notice will meet this requirement.

172 See s 5(1) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

173 On the question of whether implied consent will suffice, it is answered in the negative since s 5(1) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 requires consent to be in writing.

174 The phrase "party to the communication" pertaining to consent is defined in the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 as "any person participating in such direct communication or to whom such direct communication is directed" in the case of a direct communication, and "the sender or the recipient or intended recipient of such indirect communication; or if it is intended by the sender of an indirect communication that such indirect communication be received by more than one person, any of those recipients" in the case of an indirect communication.

175 See s 6(1) and (2) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

3 3 3 3 Business exception

The "business exception" contained in the Interception Act¹⁷⁶ makes it possible for employers to intercept the communication of their employees without having to first obtain their written permission. The Interception Act¹⁷⁷ lists certain requirements that must be met before such interception is regarded as lawful.¹⁷⁸ In terms of s 6(1) of the Act, indirect communications in the course of transmission over a telecommunications system, may be intercepted if (a) it relates to a transaction being entered into in the course of the business; or (b) it otherwise relates to the business; or (c) it otherwise takes place in the course of that business. S 6(2) provides a further condition, in that the interception of indirect communications in terms of s 6(1) is only permitted:

- (a) if the system controller¹⁷⁹ gives his consent thereto or if it is done with his implied consent;¹⁸⁰
- (b) if the communication is intercepted for a legitimate purpose, which is limited to (i) establishing the existence of facts; (ii) investigating or detecting the unauthorised use of the employer's telecommunication system; or (iii) securing the effective operation of the employer's telecommunications system or as an inherent part of, the effective operation of such system; or "monitoring indirect communications made to a confidential voice-telephony counselling or support service which is

176 70 of 2002.

177 70 of 2002.

178 See s 6 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

179 The phrase "system controller", with regards to a private body, is defined in the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 as "in the case of a (i) natural person, that natural person or any person duly authorised by that natural person; (ii) partnership, any partner of the partnership or any person duly authorised by the partnership; or (iii) juristic person, the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or person who is acting as such or any person duly authorised by such acting person".

180 See s 6(2)(a) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that users thereof may remain anonymous if they so choose";¹⁸¹

- (c) if the use of the telecommunication system concerned is provided for wholly or partly in connection with that business;¹⁸² and
- (d) if the system controller has made all reasonable efforts to inform individuals in advance, that indirect communications transmitted by means of a telecommunications system may be intercepted, or if such indirect communication is intercepted with the express or implied consent of the person who uses such system.¹⁸³

Any employer may therefore lawfully monitor, examine and otherwise intercept telephone conversations, electronic communications (such as email messages etc), faxes and other forms of indirect communication of their employees "in the course of the carrying on of its business", provided it has satisfied the other conditions.¹⁸⁴ Of note is that the Interception Act¹⁸⁵ only allows for the interception of "indirect" communications under the business exception, and then only as far as the transmission was executed over a telecommunication system.¹⁸⁶ Therefore, direct

181 See s 6(2)(b) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

182 See s 6(2)(c) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

183 See s 6(2)(d) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

184 See s 6(1) and (2) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

185 70 of 2002.

186 The Telecommunications Act 103 of 1996 defines a telecommunication system as "any system or series of telecommunication facilities or radio, optical or other electromagnetic apparatus or any similar technical system used for the purpose of telecommunication, whether or not such telecommunication is subject to re-arrangement, composition or other processes by any means in the course of their transmission or emission or reception".

communications (such as discussions that are face to face) are excluded from the ambit of this provision. Furthermore, indirect communications (such as paper memo's, postal mail etc) not transmitted over a telecommunications system could not be lawfully intercepted under s 6 of the Interception Act.¹⁸⁷ However, they are not prohibited from being intercepted in terms of the other provisions of the Act.¹⁸⁸

The Interception Act¹⁸⁹ repeatedly refers to the phrase "in the course of the carrying on of that business".¹⁹⁰ Lack of clarity does exist as to what is meant by the legislature when reference is made to "in the course of the carrying on of any business".¹⁹¹ What is unclear is whether the business exception will be interpreted strictly and whether it will be wide enough in ambit to include borderline cases.¹⁹² It is submitted that in cases of uncertainty it is preferable for an employer to respect its employee's right to privacy and obtain the necessary consent to intercept the electronic communications of such employee.

187 70 of 2002.

188 S 2 of the Interception Act prohibits, subject to other provisions in the Act, the interception of "any communication in the course of its occurrence or transmission". The definition of "communication" in this case includes indirect communications.

189 70 of 2002.

190 See s 6 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

191 See chapter 1 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 which defines "business" as "any business activity conducted by any person, including activities of any private or public body". From this definition it can be deduced that the business exception will apply equally to private and public bodies (such as state departments). The ambit is thus wide enough to include all employers.

192 For example, may electronic communication (such as an email message) be intercepted under the business exception when an employee uses an employer's system during a personal crisis?

3 3 3 4 Communicated-related information

What is meant by communication-related information? The Interception Act¹⁹³ defines communicated-related information as

"[A]ny information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identifies the origin, destination, termination, duration, and equipment used in respect, of each indirect communication generated or received by a customer or user of any equipment, facility or service provided by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system;"

From this definition it can be deduced that such information does not relate to the contents of indirect communications (such as email) but rather to information associated with it such as origin, destination etc.

S 12 of the Interception Act¹⁹⁴ contains a general prohibition against supplying communication-related information to anyone besides the customer of a service provider, provided that the information relates to that customer.¹⁹⁵ Exceptions to this general prohibition apply. As such, the Interception Act¹⁹⁶ allows for communication-related information to be supplied under a real-time or archived communication-related direction.¹⁹⁷ Furthermore, the Interception Act¹⁹⁸ also allows for telecommunication service providers to supply communication-related information to

193 70 of 2002.

194 70 of 2002.

195 See s 12 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

196 70 of 2002.

197 See s 13 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

198 70 of 2002.

a third party as per specific written authorisation of the customer, provided that such information is only provided to the person specified by the customer.¹⁹⁹

An interesting question is whether third parties are entitled to communication-related information that is held by a telecommunications service provider. For example, can a commissioner presiding in a Commission for Conciliation, Mediation and Arbitration (CCMA) proceeding request that communication-related information pertaining to the dispute be supplied to him? S 42 of the Interception Act²⁰⁰ provides that information may not be disclosed except under certain conditions; for example information required as evidence in any "court of law."²⁰¹ The CCMA is not a court of law and information requested by a commissioner, presiding in a CCMA case, is not included in any of the exceptions.²⁰² However s 42 of the Interception Act²⁰³ does allow for disclosure if the information is "required in terms of any law". Neither of the terms "law" or "court of law" is defined. In terms of the Labour Relations Act,²⁰⁴ a commissioner of the CCMA who attempts to resolve a dispute, may subpoena for questioning any person who may be able to give information or whose presence at the conciliation or arbitration proceedings may help to resolve the dispute.²⁰⁵ Although "information" is not defined in the Labour Relations Act,²⁰⁶ it is submitted that the ambit of the word is such that "communication-related information" will be included provided it pertains to the dispute. Furthermore, the commissioner may also subpoena

199 See s 14 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

200 70 of 2002.

201 See s 42 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

202 In the *Carephone (Pty) Ltd v Marcus* 1998 10 BCLR 1326 (LAC) case, Froneman J found that the CCMA performs functions of a judicial nature, but is "not a court of law".

203 70 of 2002.

204 66 of 1995.

205 See s 142(1)(a) and (d) of the Labour Relations Act 66 of 1995.

206 66 of 1995.

any person who is believed to have in his possession or control any book, document or object relevant to the resolution of the dispute, to appear before the commissioner, to be questioned or to produce such a book, document or object.²⁰⁷ The right of the commissioner to subpoena is granted in terms of s 142(1)(a) and (b) of the Labour Relations Act.²⁰⁸ As a result, it can be argued that the commissioner's right to subpoena satisfies the exception "required in terms of law" for purposes of s 42 of the Interception Act.²⁰⁹

In the case of a disciplinary enquiry it will depend on whether the employer is a customer of a telecommunications service provider or whether it supplies a telecommunications service for its own use. It seems that although the employer will have access to communication-related information as a "customer" of the telecommunications service provider, the employee (as a third party) can be precluded from access under s 42 of the Interception Act,²¹⁰ on the ground that none of the exceptions apply to disciplinary enquiries. The employer, as a customer of the telecommunications service provider, may however authorise the telecommunications service provider to supply communication-related information to the employee.²¹¹

In the case where an employer is the supplier of a telecommunications service rather than a "customer" of a service provider, it can be argued that the employee will be precluded from having access to communication-related information under the general prohibition contained in s 42 of the Interception Act.²¹² However, it can also be argued that the employee may be regarded as a "customer" of the employer in a

207 See s 142(1)(b) of the Labour Relations Act 66 of 1995.

208 66 of 1995.

209 70 of 2002.

210 70 of 2002.

211 See s 14 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

212 See s 42 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, which contains a general prohibition against disclosing information. S 42(3)(c) specifically includes communication-related information when referring to "information".

situation whereby the employer is a provider of a telecommunications service to the employee.²¹³ As a result the employee will then be able to access communication-related information pertaining to it, as a "customer" of the employer.²¹⁴ Since an internal disciplinary hearing will not involve a disclosure by the employer to a third party, the employer should also be able to use the communication-related information freely at such hearing.

3 3 3 5 The Interception Act and Privacy

What is the impact of the Interception Act²¹⁵ on the right to privacy entrenched in the Bill of Rights of the Constitution?²¹⁶ If there is an impact, does it mean that the Interception Act²¹⁷ is unconstitutional? In answering these questions a balancing act ensues, in that the interest of an employer in running a business is measured against the interests of protecting the employee's right to privacy.

S 36 of the Constitution²¹⁸ essentially requires a two-stage approach when deciding on the limitation of a right contained in the Bill of Rights. The first question is whether a right in the Bill of Rights was infringed and secondly if a right was indeed infringed, whether the infringement is nevertheless permissible in terms of the criteria for a legitimate limitation of the right laid down in s 36.²¹⁹

213 The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 defines "customer" as "any person to whom a telecommunication service provider provides a telecommunication service" and "telecommunication service provider" as "any person who provides a telecommunication service...and includes any person who provides a...private telecommunication network".

214 See s 12 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

215 70 of 2002.

216 108 of 1996.

217 70 of 2002.

218 108 of 1996.

219 *S v Makwanyane* 1995 6 BCLR 665 (CC).

There can be no doubt that the Interception Act²²⁰ impacts on the right to privacy of individuals.²²¹ The mere fact that it allows the interception of communication as provided for in s 2 means an infringement of the "right to privacy" and more particular the right not to have the privacy of communications infringed.²²² However, as previously discussed, the right to privacy is not absolute under the constitution.²²³

The question then becomes whether the right to privacy entrenched in the Constitution²²⁴ may be limited in terms of the limitations clause.²²⁵ S 36(1) of the Constitution²²⁶ provides that a law may legitimately limit a right in the Bill of Rights if it is a law of general application that is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. The qualification "law of general application" contained in s 36(1) of the Constitution²²⁷ means that the legislature may not in a law provide for the limitation of the rights of a specific person or a single or unique set of circumstances.²²⁸ The Interception Act²²⁹ does not limit its

220 70 of 2002.

221 The Interception Act recognises certain instances where the interception of communications may lawfully take place which infringes on the right not to have the privacy of communications infringed - see s 2-6 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

222 See s 14(d) of the Constitution of the RSA 108 of 1996.

223 See s 36(1) of the Constitution of the RSA 108 of 1996.

224 108 of 1996.

225 S 36(1) of the Constitution of the RSA 108 of 1996 states that "The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that 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".

226 108 of 1996.

227 108 of 1996.

228 See *President of the RSA v Hugo* 1997 6 BCLR 708 (CC) where Mokgoro J said that "a law for the purpose of a law of general application includes rules of legislation" and "a rule must be accessible, precise and of general application" and furthermore that "a law should apply generally and should not target specific

application to any one person but aims to regulate the interception of communications in general. Therefore, it is submitted that it can be seen as a "law of general application".

In order for a law to pass the "reasonable and justifiable" test, it must serve an acceptable purpose and there must be sufficient proportionality between the harm done by the law (infringement of the right to privacy of communications in the case of the Interception Act)²³⁰ and the benefits it is designed to achieve (purpose of the Act).²³¹ In considering the purpose and proportionality of a law the Constitution²³² prescribes certain factors to be considered. It should be noted that these factors are not an exhaustive list and are simply indicators as to whether a limitation is reasonable and justifiable. The factors are:

(a) the nature of the right²³³ -

This is essentially a proportionality enquiry, meaning a weighing up of the harm done by a law that infringes a fundamental right against the benefit(s) that the law seeks to achieve. In order to do this one has to look at the reason for the law or purpose of the law. It must be kept in mind that some rights contained in the Bill of Rights weigh more heavily than others do. For example the right to life is perceived as the most fundamental of all human rights.²³⁴ When applying this test to the Interception Act²³⁵

individuals". Also see De Waal, Currie & Erasmus *The Bill of Rights Handbook* (1998) which states "To qualify as a law of general application a rule must apply generally in the sense of not being unequal or arbitrary."

229 70 of 2002.

230 70 of 2002.

231 See preamble of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

232 108 of 1996.

233 See s 36(1)(a) of Constitution of the RSA 108 of 1996.

234 Du Plessis & Corder *Understanding SA's Transitional Bill of Rights* (1994). The right to life is entrenched in s 11 of the Constitution of the RSA 108 of 1996.

235 70 of 2002.

it can be deduced that one purpose of the Interception Act²³⁶ is to regulate the interception of communication for various reasons, which may include protecting business interests of employers that utilises telecommunication systems, and the prevention of criminal activities through such systems. It is submitted that the Interception Act²³⁷ can be seen to have a legitimate purpose and will in all probability pass this test.

(b) importance of purpose of limitation²³⁸ -

This factor requires the limitation of the right to serve some purpose. Justifiably requires that the purpose be one that is worthwhile and important in a constitutional democracy. It must be noted that a limitation of a right that serves a purpose but does not contribute to an open and democratic society based on human dignity, equality and freedom cannot be justifiable. The question is thus whether the Interception Act²³⁹ is worthwhile and important in a constitutional democracy. Our constitution is based on freedom of trade, which includes the right to conduct business. In order to achieve that, certain regulations need to be put in place. The Interception Act²⁴⁰ contributes to an open and democratic society by helping employers to safeguard their telecommunications systems in running a business. Therefore it is submitted that the Interception Act²⁴¹ has a purpose as well as contributing to an open and democratic society.

236 70 of 2002.

237 70 of 2002.

238 See s 36(1)(b) of Constitution of the RSA 108 of 1996.

239 70 of 2002.

240 70 of 2002.

241 70 of 2002.

(c) nature and extent of limitation²⁴² -

This factor requires a court to assess the way the limitation effects the fundamental right concerned. Is the limitation a serious or relatively minor infringement of the fundamental right? The more substantial the inroads into a fundamental right, the more persuasive the grounds of justification must be.²⁴³ In order to determine whether the limitation does more damage to the right than is reasonable for achieving its purpose, one first requires an assessment of how extensive the infringement is. The Interception Act²⁴⁴ does not permit the unjustified interception of communications. In fact, s 2 of the Interception Act²⁴⁵ contains a general provision against the interception of communications. Certain exceptions exist, such as the "business exception",²⁴⁶ but these are limited and subject to specific conditions. Even though the infringement imposed by the Interception Act²⁴⁷ on the right "not to have the privacy of communications infringed" is extensive in the sense that employers will be able to monitor nearly all employee communications, it should be noted that employees are expected to attend to the business affairs of the employer when at work and as soon as they abandon the private sphere outside of work for that of the business affairs of the employer, the benefit of privacy is lost.²⁴⁸ In view of the court's approach in the *Protea Technology* case *supra* that employee privacy is lost when the private sphere is abandoned for that of the employer, it appears that the courts are not affording employees much privacy at work, resulting in less likelihood of an infringement.

242 See s 36(1)(c) of Constitution of the RSA 108 of 1996.

243 *S v Bhulwana* 1995 1 SA 509 (C); *S v Gwadiso* 1995 12 BCLR 1579 (CC).

244 70 of 2002.

245 70 of 2002.

246 See s 6 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

247 70 of 2002.

248 See *Protea Technology supra*.

(d) relation between the limitation and its purpose²⁴⁹ -

To serve as a legitimate limitation of a right, a law that infringes must be reasonable and justifiable. There must be good reasons for the infringement and the law must tend to serve the purpose for which it was designed. If the law is likely to have only a marginal impact in achieving its purpose there cannot be adequate justification for its infringement on a fundamental right. The question is thus whether the Interception Act²⁵⁰ has a marginal impact on its purpose. This remains to be seen since the Act was acceded to during December 2002 and at the time of writing has not yet taken effect. However, the purpose of the Interception Act²⁵¹ and the regulations imposed by it gives the sense that it will have more than just a marginal impact on its purpose, since it aims to provide legislative guidance on electronic communication issues faced by most businesses during a time when employers are not aware of the implications created by interception and monitoring activities. It should be noted that with the advancement of technology in today's digital age businesses cannot survive without it, but at the same time they are exposed to electronic "attacks" through the use of telecommunication systems. Their survival is dependent on taking the relevant precautions, of which interception of electronic communication in terms of the Interception Act²⁵² is but one. The Interception Act²⁵³ allows employers a certain amount of "freedom" by means of the legitimate monitoring and interception of electronic communications that pass through the telecommunications system and which may pose a threat to them.

249 See s 36(1)(d) of Constitution of the RSA 108 of 1996.

250 70 of 2002.

251 70 of 2002.

252 70 of 2002.

253 70 of 2002.

(e) less restrictive means to achieve purpose²⁵⁴ -

This factor obliges those limiting the right, and courts reviewing its constitutionality, to have due regard to alternative ways in which the purpose can be achieved. Taking into account alternatives does not mean that any other alternative, which would limit the right less severely, should have been used, unless such alternative will achieve at least similar results. In principle, the state itself may decide which method will be the most effective to achieve the purpose. A court will thus give the state a margin of discretion.²⁵⁵ Taking into account the court's view in *S v Makwanyane*, where it was said that the role of the court is not to second-guess the wisdom of legislative policy decisions, it is doubtful whether a court will interfere with the legislator in deciding that another alternative will be more "appropriate" than the Interception Act.²⁵⁶ Some alternative ways in achieving the purpose may include providing employees with "private" telecommunication equipment with which to conduct private affairs, or providing employees with privacy timeslots during which time access is granted to the internet or private email for personal use. Similarly, employers may be able to fund the granting of personal email and Internet accounts of employees. A range of alternative measures may exist; all of which may be reasonable and justifiable in an open and democratic society. As long as the state employs any one of the methods falling within this range, the courts will not interfere with the decision to limit rights.

Applying the above analysis it is submitted that even though the Interception Act²⁵⁷ infringes on the right not to have the privacy of one's communications infringed, it should in general withstand constitutional scrutiny in terms of the limitations clause contained in s 36 of the Constitution.²⁵⁸ ²⁵⁹ However, certain sections of the

254 See s 36(1)(e) of Constitution of the RSA 108 of 1996.

255 In *S v Makwanyane supra* it was said that it is not the role of the court to second-guess the wisdom of policy choices made by legislators.

256 70 of 2002.

257 70 of 2002.

258 108 of 1996.

259 A similar finding was made in respect of the Interception and Monitoring Prohibition Act 127 of 1992 in the case of *S v Naidoo supra*.

Interception Act²⁶⁰ are still unclear and controversial. For example, the Interception Act²⁶¹ fails to discriminate sufficiently between communications warranting interception and those not warranting it. As such, the Interception Act²⁶² does not differentiate between indirect communications that are received from third parties which may have no relation to the employer and those originating from employees which stand in a working relationship with the employer. The reach of the Interception Act²⁶³ may potentially extend to include the communications of innocent individuals living in close proximity to those being monitored. These individuals will normally not be aware of company monitoring policies and could not have given consent to the interception or monitoring of their electronic communications. A court may very well find that such an infringement will not withstand constitutional scrutiny under the limitation clause (s 36).²⁶⁴

260 70 of 2002.

261 70 of 2002.

262 70 of 2002.

263 70 of 2002.

264 In *S v Naidoo supra* McCall J held that "Clearly, neither the accused nor Mrs Rajnarain and her daughter consented to the monitoring. In both of the conversations there was evidence of an awareness of the necessity to be careful about talking over the telephone. That awareness could not, in my opinion, constitute consent to the violation, or a waiver, of the accused's expectation of a right of privacy." Also see *Kopp* and *Olmstead* cases *supra*. Although these cases dealt with telephone tapping it is submitted that they will equally apply when dealing with electronic communications. After all, electronic communication is the mere putting unto paper of voice communication. It should be kept in mind that the constitutional law of foreign jurisdictions may be consulted especially in areas where conventional wisdom on constitutional matters has not established itself in South Africa - see *Mistry* case *supra*.

4 International developments around electronic communication monitoring in the workplace and the South African comparison

4 1 United Kingdom (UK) perspective

4 1 1 Introduction

The Internet has become more than a productivity tool for UK companies - it is now also considered a distraction for employees. Dataquest, a division of Gartner Group, estimated that more than 13.6 million workers in the UK are Internet-enabled. According to a press release issued by Websense International²⁶⁵ on 13 November 2002, Internet misuse is costing UK businesses "more than £15 billion annually in lost productivity".²⁶⁶ Websense has further shown that 44% of UK employees who are Internet enabled are spending an average of three hours per week "surfing" personal sites at work.

However, there is a flip side to the story. If managed correctly, electronic communication is an incredibly powerful and useful business tool. Due to a tightening labour market, employers will find it increasingly difficult to retain and motivate high quality employees in a changing workplace environment. By giving employees managed access to electronic communication, employers can provide access to banking, travel, shopping facilities at appropriate times and block out offensive content at all times, in order to help create a more pleasant working environment. With that being said, companies need to strike an effective balance between personal and work-related use of electronic communication.

265 Websense International is a software company that develops employee Internet management solutions allowing companies to manage their employee Internet use.

266 See <http://www.websense.com/company/news/pr/02/emea/131102b-uk.cfm>.

4 1 2 UK legislation

The Regulation of Investigatory Powers Act (RIPA) of 2000²⁶⁷ formalised the legal position pertaining to workplace monitoring of communications in the UK. RIPA²⁶⁸ came into force in October 2000 and established a new legal framework to govern the interception of email, Internet and telephone communications in the UK.

Before the introduction of RIPA²⁶⁹ there was no legislation governing interception of communications over private networks. However, licensing arrangements for private telephone systems did provide some degree of protection against covert monitoring. It was a condition of the license grant that the licensee make "every reasonable effort" to inform all parties to a telephone conversation that it may or would be recorded. However, no remedial provisions were made if the licensee breached the terms of the license, and the broader legal issues relating to privacy were not addressed either.

267 See <http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm>.

268 Regulation of Investigatory Powers Act of 2000.

269 Regulation of Investigatory Powers Act of 2000.

4 1 2 1 The Office of Telecommunications (OFTEL)

In addition to licensing conditions, the Office of Telecommunications (OFTEL)²⁷⁰ published guidelines in 1999 covering the responsibilities of businesses in relation to recording phone calls for business purposes.²⁷¹ The guidelines were issued in response to a successful claim brought in 1997 by Alison Halford²⁷² in the European Court of Human Rights for breach of article 8 of the European Convention on Human Rights.²⁷³

The OFTEL guidelines are intended to apply to any organisation that runs its own switchboard, call centre or other type of private voice network. As a result, the majority of employers fall within the scope of the guidelines. The guidelines focus on the reasonable expectation of privacy in the workplace that employees are entitled to. This right to respect for privacy is entrenched in the European Convention on Human Rights.²⁷⁴ The guidelines state that there must be some way in which employees can make or receive personal calls at work that will not be recorded or monitored. This may be achieved by providing access to pay phones that are not in any way subject to recording or monitoring or, alternatively, to provide for some paid but unrecorded, unmonitored telephone lines at work that employees may use for private calls. Furthermore, the OFTEL guidelines emphasise the need for employers to inform their

270 The Office of Telecommunications (OFTEL) is the regulator for the UK telecommunications industry. OFTEL was set up under the UK Telecommunications Act of 1984.

271 See <http://www.iproof.biz/legalInfo.asp>.

272 Alison Halford is the former Deputy Chief Constable of Merseyside police. She brought a claim against Merseyside police for tapping her telephone. Her employer was trying to obtain evidence regarding a sex discrimination claim that she was pursuing against the police authority. She had not been given any prior warning that her telephone calls might be intercepted. As a result, the court found that she had a reasonable expectation of privacy for her calls. She was successful in establishing that, by its conduct, the police authority had unlawfully breached her right to respect for privacy and family life.

273 Article 8 sets out an individual's right to respect for privacy and family life. See http://www.hrcr.org/docs/Eur_Convention/euroconv2.html.

274 Now incorporated into UK law by the Human Rights Act of 1998.

employees that recording or monitoring may take place on official work phones. Once an employee has been informed that monitoring or recording may occur it will assume implied consent to the monitoring/recording and removes the employee's expectation of privacy. Employers may inform employees by issuing staff notices, global emails or by a stipulation contained in the contract of employment.

The guidelines recommend that employers must consider confining recording and monitoring of telephone lines to those situations in which recording/monitoring is absolutely necessary and is proportionate to the problem that the employer is trying to address. For example, if the problem is misuse of office phones for personal calls a less intrusive means than recording or monitoring the call would be to obtain an itemised account of all calls made.

4 1 2 2 Human Rights Act of 1998

The UK courts have not comprehensively addressed legal concerns pertaining to the appropriate extent permissible in auditing and monitoring of company computer systems. Nonetheless, some measure of protection of an employee's privacy in relation to telephone calls and emails is provided by the Human Rights Act of 1998, which served to incorporate the European Convention for the Protection of Human Rights into UK national law. Article 8(1) of the Convention provides that

"Everyone has the right to respect for his private and family life, his home and his correspondence."

In the case of *Halford v United Kingdom*,²⁷⁵ the European Court of Human Rights considered the application of article 8(1) in the context of a case involving surveillance by an employer of an employee's office telephone. The court found that, since the employer had not given any prior warning that telephone calls were liable to interception, the employee had a reasonable expectation of privacy when making such calls. The court concluded that the telephone calls were covered by article 8 and that the interception of those calls was an unlawful breach of said article. It is submitted

²⁷⁵ *Halford v United Kingdom* 1997 73/1996/692/884.

that the same reasoning could be used in relation to the interception of other forms of electronic communications, including email and the Internet.

It would appear from the *Halford* decision *supra* that if an employee does not have a reasonable expectation of privacy, then an employer may be free to intercept communications of such employee. If an employer reminds employees - by means of a computer use policy - that computer resources are owned by the company and that any use thereof may be monitored when the employer deems it necessary, then an employee will arguably not retain any expectation of privacy when making use of such resources.

However, it is possible that the use of passwords or security levels restricting electronic communication may give an employee a legitimate belief that such communications will be strictly private. Similarly, the capacity to delete files or messages may encourage a reasonable expectation of privacy on the part of employees if they are unaware that deleted and purged files may actually remain backed up on the computer systems of the employer. Such expectations may be removed or modified by the actions of the employer. The wording of an appropriate computer usage policy will therefore be crucial in setting the parameters for any expectation of privacy.

As noted above, the Human Rights Act of 1998 incorporates the European Convention on Human Rights. Article 8 of the Convention sets out an individual's right to "respect for privacy and family life". In principle, monitoring and recording employees' communications may amount to a breach of such rights. The Human Rights Act of 1998 has limited effect in the UK, as it is only directly enforceable against employers in the public sector. However, it is not irrelevant to employers in the private sector because an Employment Tribunal may take a breach of an employee's human rights into account when considering claims for unfair dismissal and/or discrimination. Where an employer has, in its pre-dismissal procedure, breached an employee's human rights, this may result in an otherwise fair dismissal being declared as unfair.

4 1 2 3 Regulation of Investigatory Powers Act of 2000

RIPA²⁷⁶ governs interception of communications over both public and private networks. RIPA²⁷⁷ is intended to ensure UK compliance with the European Telecoms Data Protection Directive whilst also ensuring that the powers are used in accordance with human rights. RIPA²⁷⁸ established a criminal offence of unlawful interception pertaining to communications on a public telecommunication system and a civil tort of unlawful interception on a private telecommunication system.

S 1 of RIPA²⁷⁹ provides that it is unlawful for a person, without lawful authority, to intentionally intercept a communication in the course of its transmission by way of a public or private telecommunication system. However, s 3 provides that it will not be unlawful to intercept such a communication if the interceptor reasonably believes that both parties to the communication consented to the interception. Consent from *both* parties is therefore a vital ingredient in making interception lawful. This creates a problem for employers intercepting electronic communication, as they will have to obtain consent from the sender and the receiver of an email message before they are allowed to intercept it.

The question may be asked why RIPA²⁸⁰ is relevant in an employer/employee context? Employers see a need for the monitoring of employee electronic communication. Misuse of electronic communication systems may result in claims for breach of contract, misrepresentation, breach of copyright, on-line defamation or harassment. Keeping these legal consequences in mind, employers need to be aware of the limitation of their monitoring powers. Employers may be liable, as operators of the system, for unlawful interception of communications by employees using the employer's internal private telecommunications network or to and from an external

276 Regulation of Investigatory Powers Act of 2000.

277 Regulation of Investigatory Powers Act of 2000.

278 Regulation of Investigatory Powers Act of 2000.

279 Regulation of Investigatory Powers Act of 2000.

280 Regulation of Investigatory Powers Act of 2000.

public telecommunication network. To fall in the ambit of RIPA²⁸¹ a private telecommunication system must be attached to a public network. If an employer intercepts its employees' communications unlawfully, the sender or recipient of the communication may be able to obtain an injunction against the employer or sue for damages if he/she is able to establish financial loss as a result. In addition, an employer need to be aware of the possibility of a potential constructive dismissal claim, if an employee can show that the implied term of trust and confidence, which is implicit in all employment contracts, has been breached by the employer's actions.

281 Regulation of Investigatory Powers Act of 2000.

The owner of a private telecommunications system may lawfully monitor it within certain limits.²⁸² An employer will be excluded from criminal liability when intercepting the electronic communication on a private telecommunication system provided that (a) he has the right to control the use or operation of the system; or (b) he has the express or implied consent from the operator of the system to conduct interception.²⁸³ The only means by which a private sector employer is lawfully able to intercept the communications of its employees are:

- (a) if the employee and the third party with whom the employee is communicating have consented to such monitoring (or the employer has reasonable grounds to believe that they have consented); or
- (b) the employer acts within the scope of Regulations published under RIPA²⁸⁴ which authorise interception of communications for certain purposes.²⁸⁵

The Regulations authorise a business to monitor or record all communications transmitted over its telecommunications system (including both telephone and email) without the employee's consent for a number of different purposes. The Regulations are quite lenient with regards to the purposes for which employers may monitor or record.

282 See s 1(6) of the Regulation of Investigatory Powers Act of 2000.

283 It appears from s 1(3) of the Regulation of Investigatory Powers Act of 2000 that such conduct will also exclude civil liability.

284 Regulation of Investigatory Powers Act of 2000.

285 These Regulations, which are called the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, were signed into law during October 2000. Their purpose is to provide for circumstances where, in a business context, it will be lawful to intercept communications made over a private network. However, the Regulations must be read alongside the requirements of data protection legislation, which is more restrictive about what employers may and may not do.

The Regulations authorise monitoring or recording without consent for the following purposes:²⁸⁶

- (a) establishing the existence of facts relevant to the business;
- (b) ascertaining compliance with regulatory or self regulatory practices or procedures relevant to the business;
- (c) ascertaining or demonstrating standards which are achieved or ought to be achieved by those using the system;
- (d) preventing or detecting crime;
- (e) investigating or detecting unauthorised use of the business' telecommunications system;
- (f) ensuring the effective operation of the system.

However, in all cases the interception and monitoring of electronic communications must be shown to be for a reason that is relevant to the employer's business. "Relevance" in this context is widely defined and includes "any communication relating to the business, which takes place in the course of carrying on that business".²⁸⁷ If, therefore, a private communication breaches a clear company policy on the use of telecommunications, for example, by transmitting trade secrets or pornography, then such communication would be "relevant" to the business and would accordingly be subject to the right to monitor under the Regulations.

286 S 3(1) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699.

287 S 2(b) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699.

The Regulations also authorise businesses to monitor (but not record) communications transmitted over their systems without the employee's consent for the following purposes:²⁸⁸

- (a) checking whether or not communications are relevant to the business; and
- (b) monitoring calls to confidential counselling or support helplines run free of charge.

The Regulations also authorise public authorities to monitor or record in the interests of national security.²⁸⁹

The powers under the Regulations are fairly wide. However, monitoring or recording should be limited to those circumstances where it is necessary and relevant to the employer's business. Monitoring or recording directed at communications, which are obviously private, or which is carried out for non-business or malicious reasons will not come within the scope of the authorisation given by the Regulations. This is consistent with the fact that the Regulations needs interpretation, taking into account an individual's right to respect for privacy under the Human Rights Act of 1998.

In all of the above circumstances, the Regulations require businesses to "make all reasonable efforts" to inform users of the telecommunications system that interception may occur.²⁹⁰

The Department of Trade and Industry (DTI) has issued guidance notes for businesses to explain the Regulations and, in particular, to give examples as to what amounts to lawful interception of communications without consent (in the form of monitoring or recording) for the purposes set out above. These guidelines do not have any legal

288 S 3(1)(b) and (c) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699.

289 S 3(1)(a)(ii) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699.

290 S 3(2)(c) The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699.

effect but may be taken into account by a court in determining whether the Regulations have been breached.

What follows is a list of DTI examples of lawful practice:

- (a) Interception to establish the existence of facts relevant to the business -

Example: keeping records of transactions and other communications in cases where it is necessary or desirable to know the specific facts of the conversation or communication that take place. Recording a telephone conversation in which the parties enter into a contract (for example, buying insurance or other goods or services) in case there is a future dispute as to the terms of that contract is covered herein.

- (b) Interception to ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the business -

Example: monitoring to check that the business is complying with regulatory or self-regulatory rules or guidelines. In the financial services sector, the Financial Services Authority (FSA) can impose rules of conduct that businesses within the financial services sector must comply with. Similarly, in the legal sector, the Law Society imposes rules of conduct that all law firms must comply with.

- (c) Interception to ascertain or demonstrate standards which are or ought to be achieved by persons using the telecommunication system -

Example: monitoring for the purposes of quality control or staff training. This will be relevant to the call centre industry.

- (d) Interception to prevent or detect crime -

Example: monitoring or recording of communications in order to detect fraud or corruption.

- (e) Interception to investigate or detect the unauthorised use of the businesses' telecommunication systems -

Example: monitoring to ensure that employees do not breach employer rules regarding use of the system. For example, if employers have Internet or email policies in place, which limit the level or type of personal use of the systems, monitoring or recording of the systems could take place to ensure that these policies were being complied with.

- (f) Interception to ensure the effective operation of the system -

Example: monitoring in order to check for viruses or such other threats to the employer computer system.

Examples in the DTI guidance of where businesses are allowed to monitor but not record without consent are:

- (a) Interception for the purpose of determining whether or not communications are relevant to the business -

Example: checking email in-boxes of employees absent due to sickness or holiday to ensure that business communications are dealt with.

- (b) Interception of communications to a confidential anonymous counselling or support helpline -

Example: monitoring of incoming calls to confidential helplines in order to enable the employer to protect or support the helpline staff.

Whilst interception of employees' communications in the above circumstances without consent would be lawful, the employer is required to make all reasonable efforts to inform every person who may use their telecommunications system (including informing callers from outside the employer's organisation) that interception of communications may take place. In addition, if interception is for a purpose other than those set out above (an example might be monitoring or recording for marketing purposes), the interception will be lawful only if consent to it is

obtained. In these circumstances not only would the employee have to consent but also the person with whom they are communicating by telephone or email. Such a person will often be someone outside the organisation.

Clearly, RIPA²⁹¹ places an emphasis on the requirement that employers should inform every person using its telecommunication system that interception of electronic communication might occur. Where consent to interception is required, the employer will be acting lawfully, so long as reasonable grounds exist in his belief that the consent has been obtained. Best practice then is to incorporate a provision in the employment contract under which employees consent to electronic communication and telephones being monitored or recorded.

4 1 2 4 Data Protection Act of 1998

While the Regulations²⁹² authorise the monitoring and/or recording of a wide range of communications (including electronic communication), the important question remains what happens to the information once it has been recorded? RIPA²⁹³ and its Regulations are not the only legislation that UK employers need to be concerned with when monitoring or recording employees' electronic communications. Once monitoring and/or recording activities are conducted as per the Regulations, the Data Protection Act (DPA) of 1998²⁹⁴ then sets out what may and may not be done with the information obtained.

The relevant data protection principles contained in the DPA²⁹⁵ require individuals to be advised beforehand of the purpose for which "personal data" about them will be used and the persons to whom it will be disclosed.

291 Regulation of Investigatory Powers Act of 2000.

292 The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699.

293 Regulation of Investigatory Powers Act of 2000.

294 See <http://www.hmso.gov.uk/acts/acts1998/19980029.htm>.

295 Data Protection Act of 1998.

Information obtained through monitoring or recording activities will be regarded as "personal data" if it contains information by which an employee can be identified.²⁹⁶ For example, information that identifies an employee by their email address would be seen as personal data. The processing of such information is governed by the DPA.²⁹⁷

The DPA²⁹⁸ defines "processing" as follows:

"Obtaining, recording or holding the information or data or carrying out any operations or set of operations on the information or data."

From the above definition it can be seen that the ambit of "processing" is wide and anything that the employer does with personal data will therefore almost certainly amount to "processing" under the DPA.²⁹⁹ Processing of information also includes destroying it. The processing of information under the DPA³⁰⁰ is subject to the data protection principles as set out below.³⁰¹

The data protection principles require that personal data must be:

- (a) processed fairly and lawfully;
- (b) obtained only for one or more specified and lawful purposes;
- (c) adequate, relevant and not excessive in relation to the purpose for which it is processed;
- (d) accurate;
- (e) not be kept for longer than is necessary for a specific purpose;

296 See chapter 1 of the Data Protection Act of 1998.

297 Data Protection Act of 1998.

298 Data Protection Act of 1998.

299 Data Protection Act of 1998.

300 Data Protection Act of 1998.

- (f) processed in accordance with the rights of data subjects (ie employees);
- (g) secure;
- (h) not transferred to a country or territory outside the EEA unless that country or territory has an adequate level of protection for the rights and freedoms of data subjects.

In general, compliance with the relevant data protection principles means that employees must be advised beforehand of the purposes for which personal data about them will be processed.³⁰² In the absence of employee consent, it is necessary for the employer to show that the collection and use of personal information is necessary for:

- (a) the performance of the employment contract; or
- (b) is in the vital interests of the employee; or
- (c) fall within one of the statutory exemptions (the most likely of which is that processing is necessary in order to detect or prevent crime).

In order to ensure compliance with the DPA,³⁰³ employers should make sure that they have an email, internet and telephone policy, which clearly sets out the circumstances in which monitoring and recording of employees' communications will take place. It should also contain those instances under which employees' explicit consent to processing for specified purposes is obtained. Failure to comply with the DPA³⁰⁴ may result in legal action being taken. These include criminal prosecutions, penalties³⁰⁵ and compensation awarded to employees (including compensation for distress). When

301 See part I, schedule I of the Data Protection Act of 1998.

302 See part II, schedule I of the Data Protection Act of 1998.

303 Data Protection Act of 1998.

304 Data Protection Act of 1998.

305 See chapter 60 and 61 of the Data Protection Act of 1998.

interpreting the DPA³⁰⁶ one must also take into account the Human Rights Act of 1998. Article 8 of the Human Rights Act, which relates to the right to respect for private and family life, is of particular importance.³⁰⁷ It is likely that this provision will impact on the future interpretation of the DPA³⁰⁸ with regards to the surveillance and monitoring of employee communications.

4 1 2 5 The DPA Code of Practice

A draft Code of Practice on the use of personal data in employer/employee relationships, which specifically addresses the question of email and telephone monitoring was issued by the Information Commissioner (IC)³⁰⁹. Unfortunately the draft Code did not sit well with Regulations issued under RIPA.³¹⁰ The reason for this was that, in contrast to the Regulations, it took a very restrictive view of monitoring in the workplace. The Code was therefore revised after calls were made for public submissions.³¹¹ The revised Code continues to be restrictive in its approach to monitoring. It states that monitoring should only take place where there is a genuine business need, where the methods used are proportionate to the employer's legitimate aims and where there is no undue invasion into the employees' privacy. It should be noted that the legal requirement on employers is to comply with the DPA³¹² itself.

306 Data Protection Act of 1998.

307 The reference to family life includes work life.

308 Data Protection Act of 1998.

309 The Information Commissioner enforces and oversees the Data Protection Act of 1998 and the Freedom of Information Act of 2000. The Commissioner is an UK independent supervisory authority reporting directly to the UK Parliament and has an international role as well as a national one. In the UK the Commissioner has a range of duties including the promotion of good information handling and the encouragement of codes of practice for data controllers, that is, anyone who decides how and why personal data, (information about identifiable, living individuals) are processed.

310 Regulation of Investigatory Powers Act of 2000.

311 See <http://www.informationcommissioner.gov.uk>.

312 Data Protection Act of 1998.

The benchmarks in the Code are however designed to bring about compliance with the DPA.³¹³ They develop and apply the DPA³¹⁴ in the context of employment practices. They are the Information Commissioner's recommendations as to how the legal requirements of the DPA³¹⁵ can be met. Employers may have alternative ways of meeting these requirements but if they do nothing they risk breaking the law.³¹⁶

The key principle in the Code is that employers should only do what is necessary and proportionate when monitoring or recording communications of employees in order to meet a specific aim that the employer is trying to achieve. As a result, "fishing expeditions" by the employer will not be acceptable. The first thing an employer needs to establish is the need to monitor or record employee communication. For example, the employer became aware that a problem of misuse of electronic communication exists.

Even where a genuine need to monitor has been identified, the Code makes it clear that the methods used by employers to monitor should be proportionate and not unduly intrusive into an individual's privacy. For example, if monitoring email traffic could identify misuse, it will not be acceptable for the employer to go one step further and open email messages of its employees. Similarly, monitoring in order to detect viruses would not justify employers reading the content of incoming email messages. In addition to an employee's right to respect for his privacy, the Code also refers to an employee's right to expect a degree of trust from his employer and to be given reasonable freedom in determining his own actions without constantly being monitored. In this sense the Code is more restrictive than the Regulations published under RIPA,³¹⁷ which allows for the interception of all email.

313 Data Protection Act of 1998.

314 Data Protection Act of 1998.

315 Data Protection Act of 1998.

316 See the Employment Practices Data Protection Code.

317 Regulation of Investigatory Powers Act of 2000.

The Code contains a number of benchmarks that can be used for measuring monitored activities. The benchmarks are designed to bring about compliance with the DPA³¹⁸ and failure to comply with the benchmarks therefore suggests failure to comply with the DPA.³¹⁹

The benchmarks are divided into:

- (a) those that apply to all monitoring activities; and
- (b) those that apply in relation to each of email, internet and telephone monitoring.

The Code includes the following general benchmarks, which relates to all monitoring activities:

- (a) identify who can authorise monitoring and make sure they are aware of their responsibilities under the DPA;³²⁰
- (b) establish a specific business risk for which the monitoring is taking place;
- (c) assess the impact of monitoring on the privacy, relationship of trust and other legitimate rights of staff and make an assessment of the effectiveness of monitoring in reducing the risk identified and document that assessment;
- (d) do not introduce monitoring in which any adverse impact to employees is out of proportion to the benefits for the employer;
- (e) if comparable benefits can reasonably be achieved by another method with less adverse impact, adopt the alternative method;
- (f) consider consulting trade unions or other representatives about the need for monitoring;

318 Data Protection Act of 1998.

319 Data Protection Act of 1998.

320 Data Protection Act of 1998.

- (g) target any monitoring on those areas where it is actually necessary and proportionate to achieve the business purpose as the monitoring of all staff will not be justified if the purpose of the monitoring is to address a risk that is posed by only a few;
- (h) keep those who have access to personal information obtained through monitoring to a minimum;
- (i) make all staff aware that monitoring is taking place and of the purpose for which personal information is collected unless in exceptional circumstances including:
 - (i) the monitoring is to check whether employees are complying with the employer's rules and standards of conduct; and
 - (ii) it is carried out for the purpose of preventing or detecting crime or the apprehension or prosecution of offenders; and
 - (iii) informing staff would be likely to prejudice this purpose; and
 - (iv) the standards set out in the Code for covert monitoring are complied with (essentially, that specific criminal activity has been identified, that covert monitoring is necessary to obtain evidence of that activity, that notifying employees would prejudice the evidence, and that the covert monitoring is carried out for no longer than necessary to obtain the evidence required);
- (j) do not use personal information collected through monitoring for purposes other than those for which the monitoring was introduced and staff were told about (the exception is where the information is such that no reasonable employer could ignore it - ie it reveals criminal activity or gross misconduct or it is otherwise clearly in the worker's interest to use it for other purposes);
- (k) remember that information collected through monitoring can be misleading, misinterpreted or even deliberately falsified as well as being inaccurate because of equipment malfunction (if the information is to be used in a way that might have an adverse impact on employees, present them with the information and give them an opportunity to challenge or explain it before it is used).

The Code makes the following recommendations in relation to the benchmarks that should apply to employers monitoring their employees' communications:

- (a) Establish a policy on the use of electronic communications, which clearly sets out the circumstances in which employees may or may not use the employer's electronic communication facilities.
- (b) Limit the scope of monitoring to what is strictly required to reduce the intended risk.

The Code suggests that the first step in monitoring email messages to determine whether the system is being abused would be to carry out "traffic" monitoring rather than monitoring the content of emails. The content should only be monitored when traffic- or subject monitoring of email messages is not sufficient on its own. Any monitoring or recording should be strictly limited and have a specific target. Cognisance should be taken of employee and third party privacy and autonomy. In addition, wherever possible, the Code recommends that monitoring should be restricted to email messages sent to specific employees and those messages that an employee has kept rather than including deleted ones as well.

When monitoring the content of incoming email messages, to scan for computer viruses for example, an automated monitoring and detection process should be used. The information obtained should only be used for a specific purpose such as virus detection. Employers finding it necessary to check the email folders of employees in their absence - if they are on holiday for example and the employer wants to ensure that the business responds properly to its customers - should make their employees aware that such activity will take place. Information obtained through such activity should only be used for this purpose unless it reveals criminal offences or gross misconduct.

The Code states that email messages that are clearly personal should not be opened. The Code also recommends that employers provide a means by which employees can purge email messages not required.

The Code indicates that the main reasons given by employers for monitoring Internet access by employees are to prevent time wasting and to prevent the downloading of pornography. The Code recommends that monitoring of Internet access should be designed to prevent rather than detect misuse. This can be done through the blocking of access to inappropriate sites or the use of web-filtering software. The Code also recommends that employees be given clear limits on the circumstances in which they may use the Internet. For this purpose the Code suggests that a simple ban on access to pornography will not be enough. In addition, employees should not be monitored in terms of the sites visited or content viewed if the purpose of the monitoring can be achieved by simply recording the amount of time spent on the internet.

Information that is obtained by the employer from the monitoring process should be disregarded unless it reveals a significant risk to the employer. The Code further states that employers should be mindful that websites could be visited unwittingly due to unintended responses of search engines, unclear hypertext links, and misleading banner advertising or mistyping.

If employees are allowed to use the employer's system to access the Internet for personal reasons, no record of the sites visited or viewed content should be kept as far as possible. If this is not possible, then employees should be informed of what information is retained by the employer and for how long.

4 1 3 Summary

The DPA³²¹ is still a relatively new piece of legislation and very little case law, especially in the context of the employment relationship, has emerged. The draft Code of Practice was due to be finalised in 2001, but due to the responses that it provoked when it was put out to consultation, further work on it was required. Despite the controversy, the essential tenets of the draft Code weren't altered much in the finalised version. The Information Commissioner's message is clear, in that monitoring should only occur where there is a real business need and - adopting the language applicable to breaches of human rights - where the methods used to carry it out are proportionate

321 Data Protection Act of 1998.

to the legitimate aims of the employer and are not unduly intrusive into an individual's privacy.

It is clear that the monitoring of communications and activities of employees in the workplace in the UK must, however, be balanced with requirements under the Human Rights Act of 1998 and Article 8 of the European Convention on Human Rights. In this sense, employers must have regard for the private lives of their employees.

4 2 United States (US) perspective

4 2 1 Introduction

According to Fader (1998)³²²

"American laws don't protect worker privacy very well. We differ from Europe and most industrialised nations. They limit the employee data companies to collect, store, and disseminate. We have no such laws."

Even though the US Government offers less statutory protection, the amount of employer monitoring is by no means less than compared to that in the UK. It is interesting to note that according to the American Civil Liberties Union (ACLU), the number of workers subject to electronic surveillance in the US has grown from eight million in 1990 to 20 million in 1996.³²³ More recently, it was reported that

"More than 78 percent of large US firms monitor employee communications on the job, twice as many as reported doing so in 1997."³²⁴

These and similar studies show that as with the UK, the US faces similar issues relating to electronic employee monitoring.

322 Fader "Want Some Privacy? Stay at Home" *Chicago Tribune* (1998-5-28) 1-3.

323 Hubbartt *The New Battle Over Workplace Privacy* (1998) 212.

324 Sullivan "U.S. Lawmakers Introduce Workplace Privacy Measure" *Reuters* (2000-7-21).

With the increased monitoring activity, employees are becoming increasingly concerned about their workplace privacy, since employers are monitoring employees more closely than ever before. At the same time, certain state efforts³²⁵ to prevent employee electronic monitoring are not succeeding. According to PC World three "Snoopware Bills" related to computer surveillance, were introduced in the United States Congress during July 2000. The one related to controlling employer surveillance, Notification of Employee Monitoring Act (H.R. 4908), died quietly in subcommittee hearings in November of the same year.³²⁶ The question arises as to what legal impact such "Big Brother" activity mentalities might have on employees? And even if the courts are allowing it and employers have some valid reasons for monitoring, should they be allowed to monitor their employees? There is little doubt that this particular debate should rage on for quite some time.

In an attempt to answer these questions, I will firstly look at proponents and opponents for and against employee electronic communication monitoring. What follows thereafter is an outline of the US legal implications when answering the above questions.

325 For example, the California State Assembly passed a bill, SB 147, in a 43-22 vote that would have prevented employers from monitoring employee email in many contexts. The bill would have extended some privacy protections afforded to employee telephone usage to emails. However, California governor Gray Davis vetoed the bill on October 5th 2001. While SB 147 was vetoed, Davis did just sign into law SB 168, which is designed to help prevent "identity theft". SB 168 requires companies to stop printing Social Security numbers on employee identification and health plan cards, as well as on other forms of identification. SB 168 also prospectively prohibits the printing of Social Security numbers on bank statements and other documents transmitted by mail, and it allows consumers to halt the access of others to their credit reports. Several pieces of federal legislation providing similar protections for Social Security numbers have been introduced by members of congress during 2001, but at this juncture it is difficult to predict whether any will be made into law.

326 Borck "Full, Open Disclosure of E-resource Policies Yields Better Feelings in Your Employees" *InfoWorld* (2000-11-20) 80.

4 2 2 US proponents of monitoring employee electronic communications

The proponents' argument for electronic communication monitoring comes down to economics. Companies value profitability, economic development, and power over privacy, justice, freedom of speech, participatory freedom, and employee health.

The government works in co-operation with big business and industry through which increased productivity and competitiveness leads to economic growth. Apparently, at this time, they see no social injustice. According to Hubbart

"Government becomes involved in social issues when there is an apparent need to correct a social wrong. When employer abuses of employee privacy rights come to light, the government is pressured to do something to protect 'employee rights'. However, government laws, regulations, and subsequent court decisions often complicate matters. If employers can exercise their right to manage employee relations in a reasonable and non-discriminatory manner, then there will be less pressure for government intervention."³²⁷

Mr. Lewis, executive director for the Centre for Public Integrity, states three lawmakers who support monitoring activity and have been instrumental in stopping legislation that improves consumer and workforce privacy. These are republican Marge Roukema, who has received \$250,000 in campaign contributions from banks and financial-services companies, republican Peter Hoekstra, who said,

"What level of privacy can an employee expect when on company time, using official phones, or using company computers or cash registers?"

and 98-year old US senator Strom Thurmond, who states "businesses are finding it essential to use electronic monitoring as a means of staying competitive in the 1990s and into the next century, and employees' privacy must be balanced against the need of businesses to maintain quality services in a competitive market". Even congressmen Paul Simon, Bob Barr, Charles Canady, and Charles Schumer, who have

327 Hubbartt *The New Battle Over Workplace Privacy* 212.

submitted bills to improve consumer and workforce privacy through advance notification requirements, have not suggested elimination of electronic monitoring.³²⁸

The US Government's position is based on the need to ensure economic stability and the precedence that US citizens have previously given up certain individual rights to accommodate the greater needs of the US workforce as a whole. As an example, US citizens submit to video surveillance while shopping in stores and when filling up the car with petrol, while baggage scans and personal searches are conducted at airports.

The National Association of Manufacturers (NAM) is one of the strongest supporters of electronic monitoring. They also oppose legislation that increases privacy for consumers and employees. NAM is an association representing 12,500 US companies, whose vice president, Barry Fineran, testified that "random and periodic silent monitoring is a very important management tool", and that "spying on workers helped produce productivity gains that enabled US companies to keep pace with foreign competitors".³²⁹

Insurance companies would stand to lose vast amounts of money if something were not done to deter the theft of goods or intellectual property insured by them. At the same time security companies profit by providing electronic monitoring capability to the industry. These companies value their own profitability and ability in providing a industry service, more than protecting an individual's need for privacy or other individual rights. Vincent Ruffolo, president of Security Companies Organized for Legislative Action, stated:

"An employer would be put in the absurd position of having to advise suspected thieves when they are being monitored."³³⁰

The American Insurance Society, the Risk and Insurance Management Society, and other groups lobbied against legislation (to provide more privacy). They managed to get an amendment to the bill that allowed employers to conduct off-site covert

328 Borck *InfoWorld* (2000-11-20) 80.

329 Lewis "American Workers Beware: Big Brother is Watching" *USA Today* (2000-2-19).

surveillance of employees, which the insurers argued was necessary to prevent workers' compensation fraud.³³¹

The US is a capitalist society that supports the entitlement of profit making and employer rights to running a business based thereon. Even though employers are said to value their employees or customers, their business decisions are based on what is best for the bottom line of the business and little else. They value profitability, legal requirements (the work environment must meet many legal requirements, at both federal and state levels) and liability concerns. Once those conditions have been met, they might also take into consideration those aspects that help them hire and retain employees. In support of the above claims the following is cited:

- (a) Proponents argue that monitoring is an indispensable tool that organisations can use to increase productivity, improve quality and service, heighten safety, and reduce costs.³³²
- (b) In a study at a major North American insurance firm, 80% of the monitored employees surveyed said that production quantity was the most important factor in their employee evaluations. Conversely, 99% of the unmonitored employees said that quality (customer service and teamwork) was the most important.³³³
- (c) There is little evidence that companies are taking any additional steps to further the cause of employee privacy except when it appears that those steps will aid in the protection of corporate profitability. As a rule, companies rely on the adherence to the law as their shield against employee privacy problems. They

330 Lewis *USA Today* (2000-2-19).

331 Lewis *USA Today* (2000-2-19).

332 Schminke *Managerial Ethics: Moral Management of People and Processes* (1998).

333 Vaught, Taylor & Vaught "The Attitudes of Managers Regarding the Electronic Monitoring of Employee Behavior: Procedural and Ethical Considerations" 2000 *American Business Review* 107-114.

conduct business solely to maximise their own profitability, even at the expense of personal information privacy.³³⁴

- (d) Todd Purifoy, at Navistar International Corporation, is responsible for enforcing the company's Email policy. His biggest concerns are file sizes; worms and viruses that impact system performance or that might even shut down the company systems. According to Todd, violations are usually "innocent vacation snapshots" or the proliferation of executable files like "Elf Bowling" that went around just before Christmas 1998.³³⁵

Companies are not only buying technology for monitoring when there is just cause. They even invest in software that gives them the capability to monitor a wide scope of activity even though they do not currently need it. For example, the Heritage Foundation uses Watchguard, which can track all Internet traffic and according to Michael Spillar, VP of technology:

"Internally we use SMS (Security Management System) from Microsoft to assist and monitor employees. But we do not monitor employees unless we have a reason to."³³⁶

It is difficult to find data that identifies exactly what employees value with regards to electronic monitoring while in the workplace. At a minimum, they must value the income their job provides, which allows them to afford housing, clothing and food ie basic human requirements. According to Vaught

"Most managers would prefer that any electronic monitoring (telephone, computer, video) be conducted on a case-by-case basis as problems arise in the workplace."³³⁷

334 Smith "Managing Privacy: Information Technology and Corporate America" 1994 *Chapel Hill: The University of North Carolina Press* 176-177.

335 York "Invasion of Privacy? E-mail Monitoring is on the Rise" *InformationWeek* (1999-2-21) 142-146.

336 Cohen "Thought Cop" *InfoWorld* (2001-2-23).

4 2 3 US opponents of monitoring employee electronic communications

Public interest groups such as Privacy International and the American Civil Liberties Union (ACLU)³³⁸ aim to protect basic human rights. Specifically, the ACLU stands to protect those basic rights of US citizens that were preconditions of democracy, including freedom of speech, assembly and the press. Barbour notes

"Even if these non-profit citizens' organisations do not fully represent the public, they do operate in independence from the main centres of economic power, and they often defend environmental and human values neglected by government agencies and private interest groups."³³⁹

The ACLU focussed attention on the need to limit government surveillance, which led to the passing of the US Privacy Act in 1974. They continue to raise awareness on disability rights, free speech, immigrants rights, lesbian and gay rights, racial equality, religious liberty, reproductive rights, women's rights, etc. Some of the things the ACLU is pushing for include:

- (a) Employers may use electronic surveillance to collect any information so long as
 - (i) the information is collected at the employer's premises; and (ii) the information is confined to the employee's work.

- (b) An employer engaging in any type of electronic monitoring shall provide prior notice to all employees who may be affected. This notice shall provide the following:
 - (i) the information which is to be collected;
 - (ii) the means by which this information is to be collected;
 - (iii) the times at which the monitoring is to occur;
 - (iv) the location of the monitoring equipment;
 - (v) what the information which is collected will be used for
 - (vi) the identity of the employees who will be monitored.However, there is an exception ie where an employer has reasonable

337 Vaught, Taylor & Vaught 2000 *American Business Review* 107-114.

338 See <http://www.aclu.org/>.

339 Barbour *Ethics In An Age of Technology*.

grounds to believe that employees are engaged in conduct, which violates the legal rights of the employer or the employer's employees.

- (c) Information concerning employees which is collected through electronic monitoring may be disclosed only with prior written consent of the employee (such consent shall not be a condition of employment).
- (d) Employers may not discharge, discipline, or in any other manner discriminate against an employee because the employee has asserted any of his or her right(s) or assisted other employees in asserting their rights, reported violations of such rights, or participated in enforcement actions related to violations of such rights.

These conditions infer that the ACLU value the individuals' right to privacy, understand people's behaviour changes when they know they are being watched, and understand the strain of constant surveillance. The ACLU's mission is "to fight civil liberties violations wherever and whenever they occur". Most of their clients are ordinary people who have experienced an injustice and have decided to fight back. In addition, the ACLU is visible in both national and state capitals in their "fight to ensure that the Bill of Rights will always be more than a 'parchment barrier' against government oppression and the tyranny of the majority".³⁴⁰

4 2 4 US laws

The US laws differ between what is allowed in the public and private sectors respectively. Even though employees working in the public sector could expect US Constitutional protection, the Constitution does not provide clear-cut application. The typical private sector employee is thus inclined to seek remedy under other sources of legal protection against intrusive employer surveillance, such as claims brought under various state statutes or the common law tort "invasion of privacy". The protection provided by these remedies varies widely from jurisdiction to jurisdiction. At the same time definitions are wide in ambit. For example, Bill HR1900 defines

340 See <http://www.aclu.org/about/aboutmain.cfm>.

"electronic monitoring" broadly to mean, in essence, "any software or hardware that runs on electricity from which data on a workers' activities can be obtained".³⁴¹

Employers and employees are faced with laws complex in application and definition. For example, federal and state "wiretap" laws cover much more than tapping into telephone lines, eavesdropping on oral conversations and intercepting or accessing phone or electronic communications. Employers considering technological methods of monitoring communications should carefully examine whether the contemplated actions would be lawful under these laws. This is by no means a simple task.

In 1986, the United States Congress passed the Electronic Communications Privacy Act (ECPA), which prohibits unwarranted monitoring or interception of electronic communications by government, private agencies and individuals. However, the ECPA³⁴² permits "an agent of a provider of wire or electronic services to intercept, disclose, or use that communication in the normal course of his employment".³⁴³ The ECPA³⁴⁴ is a federal statute that governs protection of electronic communications that "affect interstate or foreign commerce" and expanded the wiretapping statute to include the interception of electronic communications. It amended the Omnibus Crime Control and Safe Street Act of 1968, the so-called wiretap statute. It has two chapters, one governing interception of communications³⁴⁵ and one governing access to electronically stored communications.³⁴⁶ It provides both criminal penalties (fines and imprisonment) for violations and a private civil action to recover damages. A person whose communications are unlawfully intercepted may sue for injunctive relief, the greater of actual damages (including any profits made by the violator) or

341 Verdisco *Security threat: Anti-monitoring bills Discount Merchandiser* (1994) 8.

342 Electronic Communications Privacy Act of 1986.

343 See article 2511, s 2 of the Electronic Communications Privacy Act of 1986.

344 Electronic Communications Privacy Act of 1986.

345 See 18 USC s 2510. Also see <http://www.usdoj.gov/criminal/cybercrime/18usc2510.htm>.

346 See 18 USC s 2701. Also see <http://www.usdoj.gov/criminal/cybercrime/usc2701.htm>.

statutory damages of either \$10,000 or \$100 for each day of the violation, punitive damages, and attorney fees and costs. If the violation consists only of accessing an electronically stored electronic or wire communication, punitive damages are not available, and statutory damages are limited to \$1,000.

The ECPA³⁴⁷ defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system", but "any wire or oral communication" is excluded.³⁴⁸

Under the ECPA,³⁴⁹ electronic communications are divided into two groups namely:

(a) communication in transit; and

(b) stored communication.

Under the ECPA,³⁵⁰ electronic communication in transit has almost the same level of protection as voice communication, meaning that intercepting such communication is prohibited.

347 Electronic Communications Privacy Act of 1986.

348 Adams, Scheuing & Feeley Stacey "E-mail Monitoring in the Workplace: The Good, the Bad and the Ugly" 2000 *Defence Council Journal* 32-46.

349 Electronic Communications Privacy Act of 1986.

350 Electronic Communications Privacy Act of 1986.

Electronic communications, which do not include the human voice, constitute "electronic communications" under the federal statutes.³⁵¹ The 1986 amendments to the ECPA³⁵² added a new chapter, which prohibits - with certain exceptions³⁵³ - accessing wire or electronic communications that are in electronic storage. The exceptions under this chapter differ from those in the chapter that prohibits the interception of communications. For this reason and because the legal remedies for a violation are not as broad, some commentators³⁵⁴ have questioned whether accessing email messages would constitute violations of both chapters. This issue was addressed in a court decision albeit not in the employment context. In *Steve Jackson Games v US Secret Service*,³⁵⁵ the court noted that the definition of "electronic communication" does not include the content of such communications while in electronic storage. Therefore, the court ruled that the chapter prohibiting the interception of electronic communications would only apply if communications were acquired "while it was in transit".³⁵⁶ As such, email messages that are accessed while stored electronically will

351 See definition of "electronic communication" in the Electronic Communications Privacy Act of 1986.

352 Electronic Communications Privacy Act of 1986.

353 One such exception provides that accessing stored electronic communications is not unlawful if authorised by the person or entity providing the wire or electronic communications service. This exception should allow employers free access to email messages stored on email systems provided by the employer, although there may be some question as to the lawfulness of access to email messages delivered to the workplace through an independent service provider. It is therefore good practice if an employer publishes a policy informing employees that the company reserves the right to access and monitor all email messages stored on its computer systems, regardless of their origin or content. This will allow employers to establish implied consent from the employee to such access. In addition, an employer who obtains the written acknowledgement or consent of its employees to such a practice should have even greater protection.

354 See Adams, Scheuing & Feeley *Stacey* 2000 *Defence Council Journal* 32-46.

355 *Steve Jackson Games v US Secret Service* 1994 US 36 F 3d 457.

356 Accessing stored electronic communication, such as email sitting on a hard drive or server waiting to be sent, is not illegal. The US courts (see *Steve Jackson case supra*) have ruled that since the email is not physically travelling anywhere it is not "in transit" and does not have the same level of protection.

not constitute an "interception" and the legality of that action will be determined only under the 1986 chapter of the ECPA,³⁵⁷ addressing the accessing of electronically stored communications. The ECPA³⁵⁸ is more concerned with interstate systems than intra-workplace email, resulting in more clear-cut regulations on the email that you send from home than on what you send within the workplace.

The ECPA³⁵⁹ does not explicitly offer protection from employers who access or intercept the electronic communications of their own employees. Instead, it appears to offer protection only from the unauthorised interception by outside parties, or from another employee who has exceeded his authority when accessing, intercepting, or disclosing information on a private company system.

Although none of the provisions in the ECPA³⁶⁰ appear to limit its applicability to the monitoring of employee email, Kopp³⁶¹ discusses three primary exceptions it does contain that may have the same practical effect: (a) the provider exception;³⁶² (b) the ordinary course of business exception;³⁶³ and (c) the consent exception.³⁶⁴

357 Electronic Communications Privacy Act of 1986.

358 Electronic Communications Privacy Act of 1986.

359 Electronic Communications Privacy Act of 1986.

360 Electronic Communications Privacy Act of 1986.

361 Kopp "Electronic Communications in the Workplace: E-mail Monitoring and the Right of Privacy" 1998 *Seton Hall Constitutional Law Journal* 1-30.

362 See 2511 2(a)(i) of title 18 of the United States Code (as amended by s 102 of the Electronic Communications Privacy Act of 1986).

363 See 2511 2(a) of title 18 of the United States Code (as amended by s 101 of the Electronic Communications Privacy Act of 1986).

364 See 2511 2(d) of title 18 of the United States Code (as amended by s 102 of the Electronic Communications Privacy Act of 1986).

The provider exception contained in the ECPA³⁶⁵ generally exempts email service providers from the ECPA³⁶⁶ prohibitions against the interception of email communications in the workplace, for certain purposes.³⁶⁷ A private employer will be exempt from the ECPA³⁶⁸ liability so long as it is the direct provider of the email system. As a result, employers are allowed an unrestricted right to monitor employee email. However, the exception should not apply to an employer that merely provides email services through a third party service provider.

Information transmitted in the ordinary course of business is excluded from information transmitted by "electronic, mechanical, or other devices", as defined in the ECPA,³⁶⁹ and the interception of such information is not prohibited in terms of the ECPA.³⁷⁰ This exception has yet to be applied to email communications in the workplace.

The consent exception generally applies in the event that one party to the communication has given prior consent to the interception of the communication. As a result the ECPA³⁷¹ prohibitions will not apply where interception follows express consent by either of the parties.

Employers may use the ECPA³⁷² exception relating to the provider of a wire or electronic communications service, to intercept communications as necessary for the rendition of the service or the protection of the rights or property of the provider. If that exception is not broad enough to cover the desired scope of email or Internet

365 Electronic Communications Privacy Act of 1986.

366 Electronic Communications Privacy Act of 1986.

367 See 2511 2(a)(i) of title 18 of the United States Code (as amended by s 102 of the Electronic Communications Privacy Act of 1986).

368 Electronic Communications Privacy Act of 1986.

369 Electronic Communications Privacy Act of 1986.

370 Electronic Communications Privacy Act of 1986.

371 Electronic Communications Privacy Act of 1986.

372 Electronic Communications Privacy Act of 1986.

interception deemed necessary, the employer should take all required steps to publish its policy of intercepting messages while in transit and thereby obtain implied consent of employees. Presumably, the business extension exclusion for voice communications over telephone lines would not apply if the interception were not accomplished through the use of "telephone equipment" used in the ordinary course of business.³⁷³

In summary, it is safer for employers to access stored email messages (which includes storage on an email server) than to intercept them while in transit. Access to stored internal email messages on a company's computer system should be lawful under the ECPA.³⁷⁴ For extra protection, or if interception of email messages in transit is desired employers should publish their policy of monitoring email messages.

373 Telephone conversations constitute "wire communications" under the federal statute, since they are "aural" (containing the human voice) and are transmitted over wire, cable, or similar facilities. With certain exceptions, it is unlawful to "intercept" wire communications. The term "intercept" is defined to mean the acquisition of the contents of the communication through the use of any "electronic, mechanical, or other device". It is also unlawful to use or disclose the contents of any wire communication, which was unlawfully intercepted. The statute's definition of "electronic, mechanical, or other device" excludes telephone equipment furnished by the provider of the communication service (eg the phone company) or by the user for connection to the facilities of the service and used in the ordinary course of business. This is commonly referred to as the "business phone extension" exclusion. There have been numerous court decisions addressing this exception, some finding it applicable and others not. See *James v Newspaper Agency Corp* 1979 US 591 F 2d 579; *Simmons v Southwestern Bell Telephone Co* 1979 US 611 F 2d 342; *United States v Harpel* 1974 US 493 F 2d 346; *Briggs v American Air Filter Co* 1980 US 630 F 2d 414; *Deal v Spears* 1992 US 980 F 2d 1153; *Watkins v L.M. Berry & Co* 1983 US 704 F 2d 577.

374 Electronic Communications Privacy Act of 1986.

According to the ECPA,³⁷⁵ computer files that do not contain the human voice cannot be "wire communications".³⁷⁶ Since the definition of "electronic communication" is limited to "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system", computer files that are created and then stored on a computer would generally not constitute "electronic communications", since there is no "transfer" or "transmission". If that is the case, access to computer files is not restricted by the ECPA.³⁷⁷ Likewise, computerised systems that track, for example, the number of keystrokes or errors by an employee, or the number and duration of customer service phone calls handled, would not be subject to the ECPA,³⁷⁸ since such systems do not acquire the content of any communications.

To the extent that a computer file is a transferred communication, for example, a computer file attached to an email message, the analysis above concerning access to or the interception of email messages would apply.

Federal law prohibits employer surveillance of union activity.³⁷⁹ Employers conducting monitoring activities are prohibited from targeting such activity and should cease any monitoring that detects union activity. In an Associated Press news article dated June 19, 1995, it was reported that the Kmart Corporation had reached a settlement with the Teamsters over the union's complaint that the company had spied on union activities. Kmart reportedly agreed to instruct outside agencies (used to investigate employee theft or drug use) not to observe union activities, and also

375 Electronic Communications Privacy Act of 1986.

376 See definition of "electronic communication" in the Electronic Communications Privacy Act of 1986.

377 Electronic Communications Privacy Act of 1986.

378 Electronic Communications Privacy Act of 1986.

379 See National Labour Relations Act 29 USC §§ 151–169. The National Labour Relations Act, enacted by congress in 1935, is the law that gives the private sector workers legal rights to join unions and bargain collectively with their employer. Its provisions give workers (including those who are not in unions) the right to act "collectively" (in groups of two or more) to improve workplace conditions, including health and safety conditions.

agreed to post notices that the company would not observe union activities. Where unions represent employees, employers wishing to implement new monitoring practices should first consult legal counsel to explore whether the employer has a legal duty to bargain with the union over the proposed monitoring.

Electronic monitoring may uncover communications among employees expressing dissatisfaction with terms and conditions of employment or possible means of seeking redress. Federal law prohibits retaliation against such employees for concerted activity relating to employment, even in a non-union context.³⁸⁰ Other federal statutes prohibit retaliation against employees include actions in opposition to discriminatory practices,³⁸¹ unsafe working conditions and violations of wage/hour laws. If employers are considering taking action against employees based on information uncovered through such monitoring, they should evaluate whether any state or federal law might prohibit the contemplated action.

Furthermore, employers conducting monitoring activities should consider appropriate steps to control the dissemination of information obtained through such monitoring since unnecessary disclosure of information could also give rise to a claim of outrageous conduct.³⁸²

380 National Labour Relations Act 29 of 1935.

381 Civil Rights Act of 1964 (as amended).

382 For a plaintiff to prevail on the claim for outrageous conduct under US law, plaintiff must establish by the preponderance of the evidence four elements. These elements are: (a) that defendants conduct was atrocious, intolerable and so extreme and outrageous as to exceed the bounds of decency; (b) that defendants acted with the intent to inflict emotional distress or acted recklessly when it was certain or substantially certain emotional distress would result from the conduct; (c) that the actions of defendants caused plaintiff to suffer emotional distress; and (d) that the emotional distress suffered by plaintiff was so severe that no reasonable person could be expected to endure it. After considering all the evidence, a US court may conclude that plaintiff has not proved any one or more of these elements by preponderance of the evidence. If the court determines that any element of plaintiff's claim for intentional infliction of the emotional distress has not been proven against defendants, then defendants are not liable. Also see *Travis v Alcon Laboratories Inc* 1988 US 202 369 504 2d 419.

In addition, the Americans with Disabilities Act³⁸³ include provisions governing the confidentiality of medical records and information.

4 2 5 US Constitutional rights

According to Thomas Jefferson, the US was founded on a citizen's "unalienable rights of life, liberty and the pursuit of happiness".³⁸⁴ Exercising such individual autonomy requires a certain amount of privacy.

The right to privacy is not unique to the US. In the executive summary of the Privacy International's Privacy & Human Rights 2000 report, David Banisar states

"Privacy is a fundamental human right recognised in all major international treaties and agreements on human rights."

Privacy is an essential state required right for a person to make choices regarding their personal and intimate activities. In the book "Ethics in an age of Technology: The Gifford Lectures Volume 2" the author explains that

"The right to privacy can be defended as a form of respect for persons as unique individuals. Freedom of thought in entertaining unpopular ideas requires some emotional and intellectual space protected from social intrusion. Divulging personal information about ourselves to other people gives them power over us and make us more vulnerable. Privacy sets limits on the power exerted over individuals by the state, by organisations, and by social groups. This aspect of privacy is consistent with the biblical understanding of the value and uniqueness of each individual in the sight of God. It is also supported by the emphasis on human autonomy and self-determination since the Enlightenment."³⁸⁵

383 S 933 of the Americans with Disabilities Act of 1990.

384 See <http://www.freelaunch.com/essays/liberty.html>.

385 Barbour *Ethics In An Age of Technology*.

Some US employees assume that if a postal letter is private, so is their email. Too many US employees believe that the Fourth Amendment³⁸⁶ of the US Constitution provides them with an unconditional moral and legal right to privacy, when in fact, it only controls the government's rights with regards to search and seizure. According to US lawyers Samuel Warren and Louis Brandeis J "privacy" is the "right to be left alone". They described privacy in the light of a tort action. This concept of a privacy tort was gradually picked up across the US as part of the US common law.³⁸⁷ But, according to Steven Winters, an advocate for protecting employee privacy, particularly with respect to email, these sources (state, local and common laws) do not adequately protect an individual's privacy in the workplace.³⁸⁸

While the US Constitution contains no express privacy provision, decisions of the United States supreme court beginning with its opinion in *Griswold v Connecticut*³⁸⁹ have recognised the existence of an implied right to privacy. Protection of individual rights and liberties afforded by the US Constitution largely applies to actions of local, state, or federal governments, or a branch or arm of such authority. Acts of such an authority is referred to as "state action". Generally speaking, in the absence of "state action", a cause of action cannot be maintained for deprivation of rights under the US or state constitutions. Employers in the private sector are generally not arms of a local, state, or federal government and their employment practices do not generally constitute "state action". Consequently private employers generally are not required to afford employees' protections granted exclusively under the US and state

386 The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and warrants shall not be issued, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. See US Constitution: Fourth Amendment.

387 Banisar "Privacy & Human Rights 2000" *Privacy International* (2001-02-20).

388 Adams, Scheuing & Feeley Stacey 2000 *Defence Council Journal* 32-46.

389 See *Griswold v Connecticut* 1965 381 US 479 85 1678 where it was held that the Connecticut statute forbidding use of contraceptives violates the right of marital privacy which is within the penumbra of specific guarantees contained in the US Bill of Rights.

constitutions. However, at least one state, the state of California, has ruled that private employers must comply with the state constitution's protection of privacy rights.³⁹⁰

The US supreme court recognised in *O'Connor v Ortega*,³⁹¹ that public employees may have a legitimate expectation of privacy at their place of employment and that they do not lose their fourth amendment rights against unreasonable searches and seizures merely because they work for the government. The Ortega ruling involved a university hospital physician's suit against the hospital and various individuals who conducted a search of his desk and file cabinets while he was away from the office. While noting that a public employee could have a legitimate expectation of privacy, the court held that in determining the appropriate standard for a search conducted by a public employer in areas in which an employee has a reasonable expectation of privacy, the question of what constitute a reasonable search depends on the context within which the search takes place, and requires a balancing of the employee's legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace. The court reasoned that requiring an employer to obtain a warrant whenever the employer wishes to enter an employee's office, desk, or file cabinet for a work related purpose would seriously disrupt the routine conduct of business and would be unreasonable. The court further noted that requiring a probable cause standard for searches of the type at issue would impose intolerable burdens on public employers. Consequently, intrusions on the constitutionally protected privacy interests of government employees for non-investigatory and work related purposes, as well as for investigations of work related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this standard, the court concluded, both the inception and the scope of the intrusion must be reasonable.

390 Johnson "Technological Surveillance in the Workplace" *Farfield and Woods* 1995

391 *O'Connor v Ortega* 1987 107 US 1492.

In Pennsylvania, a court decision held that employees do not have a right of privacy in their employer-provided email. In *Smyth v Pillsbury Company*³⁹² the court dismissed a lawsuit filed against the company's invasion of the employee's privacy by a terminated employee. The Pillsbury Company fired an employee for transmitting inappropriate and unprofessional comments. The company had intercepted some messages that were sent by Smyth to his supervisor. Such messages contained threatening and humiliating phrases, such as "Kill the backstabbing bastards" and referring to an upcoming holiday party as the "Jim Jones Koolaid affair". The Pillsbury Company had explicitly assured all its employees that the email system was private and confidential, and that email would never be intercepted or used as grounds for termination. Despite Smyth's claim that his discharge violated public policy, the court threw out the employee's suit before trial for the reason that the company has the right to fire the employee, because its right to fire any employee was not limited by its assurances. The court further stated that

"Once a plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an email system which was apparently utilised by the entire company, any reasonable expectation of privacy was lost."

As a result, cautious US public employers wishing to monitor their employees should preferably notify their employees of their policy on electronic communication monitoring. If employees were made aware that their communications are subject to monitoring, a court would be less likely to find any reasonable expectation of privacy, without which there can be no violation of constitutional rights. In addition, employers in the public sector should try to keep monitoring activities within reasonable limits. Such monitoring should also be related to legitimate organisational needs and goals.

392 *Smyth v Pillsbury Co* 1996 US.

4 2 6 US common law

Due to the lack of clear constitutional and statutory protection, the primary sources of employee privacy protection in the private sector workplace has been state tort law and related case law. According to Kopp³⁹³, tort law recognises four distinct torts protecting the right of privacy namely (a) unreasonable intrusion upon the seclusion of another; (b) appropriation of another's name or likeness; (c) unreasonable publicity given to another's private life; and (d) publicity that unreasonably places another in a false light before the public. The tort of "intrusion upon seclusion" is probably the one that is most closely associated with email monitoring in the workplace and will be discussed below.

It holds that one who intentionally intrudes, physically or otherwise, on the solitude or seclusion of another, or another's private affairs or concerns, is subject to liability for invasion of privacy if the intrusion would be highly offensive to a reasonable person. In holding that the invasion may be "physical or otherwise", this tort could possibly be extended to protection against email monitoring. It also imposes a standard of objective reasonableness. Thus, in deciding whether the intrusion is into a private matter, courts require not only that the employee has a subjective expectation of privacy, but also that the expectation is objectively reasonable.

The common law tort of "invasion of privacy" has been applied in two cases involving email monitoring in the workplace. In the *Bourke v Nissan Motor Corp*³⁹⁴ case, the plaintiffs brought action against their employer for intercepting and reviewing several personal email messages. The court rejected this claim and held that the employees did not have a reasonable expectation of privacy in their email communications because they had signed a waiver stating that email use was limited to company business. In addition, the court noted that the employees were aware that other co-workers had read their email messages in the past, even though they were not the intended recipients of the messages. Furthermore, the court rejected the plaintiffs' argument that a subjective expectation of privacy existed by virtue of having personal

393 Kopp 1998 *Seton Hall Constitutional Law Journal* 1-30.

394 *Bourke v Nissan Motor Corp in USA* 1993 No B068705.

passwords - as well as their being told to safeguard their passwords - to access the email system.

Another case that addressed the common law tort of invasion of privacy is *Smyth v Pillsbury*³⁹⁵, in which an employee brought suit against his employer for wrongful discharge. The plaintiff argued that his termination was against public policy as a violation of his common law right to privacy. The court analysed his claim under the definition of intrusion upon seclusion and found that the plaintiff could not have a reasonable expectation of privacy in email communications voluntarily made to his supervisor over the company email system. Even if he had a reasonable expectation of privacy in the contents of his email messages, the court would not consider the interception of those communications to be a substantial and highly offensive invasion of privacy, particularly since the email system belonged to the company. The court concluded saying that any privacy interest of the plaintiff was outweighed by the employer's interest in preventing inappropriate and unprofessional comments over its email system.

As the only cases so far applying common law invasion of privacy to tort email monitoring, *Bourke* and *Smyth* offer a grim outlook for email privacy in the workplace. These cases suggest that courts will provide a very narrow reading of employees' reasonable expectation of privacy. According to the *Bourke* case, maintaining a personal password to access an email system does not give rise to an objectively reasonable expectation of privacy. In the *Smyth* case there is evidence that an employer's policy, stating that employee email is private and confidential, will not necessarily give rise to an objectively reasonable expectation of privacy when tested in a court of law. Consequently, it can be reasoned that the current state of common law with respect to email monitoring in the US clearly favours employers above employees.

395 *Smyth v Pillsbury supra*. Also see discussion *supra*.

In addition, it should also be noted that a well-written employer email policy may not only immunise an employer from liability under the ECPA,³⁹⁶ but may also safeguard it from tort liability for invasion of privacy. In fact, the two cases above strongly support the proposition that a well-written email policy will be sufficient to render any expectation of privacy by an employee as unreasonable.

Aside from the court rulings in California and Pennsylvania,³⁹⁷ Colorado Courts have adopted the Restatement (2d) of Torts, S 652 (1977), which sets forth different forms of invasion of privacy:

(a) Unreasonable disclosure of personal facts -

This form of the invasion of privacy tort envisions the circulation and unnecessary disclosure to the public of those matters that concern the private life of another. This relates to those matters where the publicity is highly offensive to a reasonable person and is not of legitimate concern to the public. It is irrelevant that the facts disclosed may be true since the tort is based on the personal nature of the facts disclosed by the wrongdoer.

(b) Unreasonable intrusion into the private affairs of another -

If an employer intentionally intrudes (physically or otherwise) upon the solitude or seclusion of another or on his private affairs or concerns, and if the intrusion would be highly offensive to a reasonable person, he may be liable. The tort is based on the psychological distress caused by the intrusion itself. It is not necessary that the employer learns anything embarrassing or private about the person harmed or that the employer wrongfully discloses that information.

396 Electronic Communications Privacy Act of 1986.

397 See *Bourke* and *Smyth* cases *supra*.

(c) Publicity that unreasonably places another person in a false light -

Such is the occurrence when the employer instigates publicity that unreasonably places the employee in a false light before the public. Liability occurs if the false light in which the employee was placed is highly offensive to a reasonable person, and the employer had knowledge of or acted in reckless disregard as to the falsity of the publicised matter and the false light in which the other would be placed.

(d) Outrageous conduct -

The tort of outrageous conduct (also known as intentional infliction of emotional distress) has been recognised by the Colorado courts. Liability under this cause of action only arises where a plaintiff can show that the defendant's conduct was not merely wrongful or unjustified, but that it went beyond the bounds of human decency. Meanwhile, negligent infliction of emotional distress requires that the defendant's conduct cause the plaintiff physical manifestations or mental illness and that such conduct subjects the plaintiff to an unreasonable risk of bodily harm. Even though most forms of employer communication monitoring would not subject employees to an unreasonable risk of bodily harm, employers should take all precautions necessary to assure that such monitoring is performed safely since certain employees - because of their physiological or psychological make-up - might be more susceptible to physical and emotional injury from routine surveillance than others.

4 2 7 Summary

The monitoring of communications in the US workplace presents both practical and legal issues. From a practical point of view, employers should consider exactly what is to be gained through monitoring, and what alternatives may exist. Some commentators and organisations claim that employee monitoring may be counterproductive by resulting in lower morale, increased job stress, and perhaps even lower productivity. Extreme examples of monitoring exist, such as testimony before the Senate concerning an express-mail company employee whose computer logged the length and frequency of her trips to the restroom, and who was reprimanded for using the restroom four times in one day. Congress considered a bill entitled "Privacy

for Consumers and Workers Act" in 1993 and 1994, but it was not passed. The bill was drafted by the American Civil Liberties Union (ACLU) and would have required employers to inform employees as to when and how they are monitored, as well as prohibiting monitoring in certain areas such as restrooms and changing rooms. An article in the San Diego Union-Tribune dated 3 July, 1995, quoted an ACLU representative who indicated that the prospects for reintroduction of the bill look "very bleak" for the near future. Even so, employers should be aware of the possibility of future legislative action and the negative fallout that may result from employee monitoring.

While the lawmakers are introducing legislation to protect individual privacy on the Internet, attempts are orchestrated to control what employers are allowed to do. The proposed Privacy for Consumers and Workers Act in 1994, that did not pass, would have protected employees' privacy by disallowing intentional collection of personal data that was not job-related. Furthermore, it would have controlled the distribution of business information to only those who needed to know. In addition, it would have prohibited monitoring in bathrooms and locker rooms unless it was part of a criminal or civil investigation.³⁹⁸

In July of 2000, the Notification of Employee Monitoring Act (H.R. 4908) was introduced. This bill would not require employers to change their surveillance habits or notify employees each time they were being monitored. The bill only required employers to annually inform their employees that they were being monitored and "employees could sue their bosses for up to \$20,000 if they found they were being monitored without their knowledge".³⁹⁹ Introducing the bill, Senator Charles Schumer a New York Democrat, "predicted that the bill would pass Congress easily, given its modest scope". He further stated that

"This is so easy to comply with, almost every employer will do it."

398 Vaught, Taylor & Vaught 2000 *American Business Review* 107-114.

399 Sullivan *Reuters* (2000-7-21).

The Notification of Employee Monitoring Act (H.R. 4908) did not make it through subcommittee hearings in November 2000.⁴⁰⁰

Even though the US federal law allows electronic monitoring with little restriction, there are other statutory protections that an employer has to consider. For example,

"California law prohibits eavesdropping, intercepting confidential communications without consent of all parties to the communications."⁴⁰¹

It is likely that the dozens of consumer privacy bills moving through state legislation and congress may eventually bring closer scrutiny of the actions of employers.

The old saying "prevention is better than cure" is applicable when it comes down to employee monitoring. Employers should consider the expense of litigation, even if it appears likely that no specific law has been violated. Macworld (July 1993 issue) reported on two lawsuits filed in the state of California over employer acquisition of email messages. The trial courts dismissed both suites, and both were then appealed.

400 Borck *InfoWorld* (2000-11-20).

401 Barlow "Do Employees' Electronic Messages Spell Trouble for You?" *Personnel Journal* (2001-1-31) 135.

4 3 Comparison with South Africa

4 3 1 Vicarious liability

The term "cyberliability" includes various types of legal liability relating to business use of electronic communication. Liability for defamation, intellectual property, copyright infringement, breach of confidence, virus distribution, unauthorised contracts, criminal liability and computer hacking are all included.

The employer has a legal duty to protect employees from harassment and may be held vicariously liable for discrimination faced by employees in the workplace. In defending claims, the employer must show that it took all reasonably practicable steps to prevent its employees from committing discriminatory acts. This means that the failure to supervise the use of electronic communication once they come to the attention of management will increase the risk of liability.

If inappropriate material, such as pornography, is attached to an email and sent directly to another employee, this may form the basis for a discrimination complaint for which the employer could be vicariously liable. However, such material does not have to be used in a directly offensive manner for it to attract vicarious liability. A case in point is *Morse v Future Reality*,⁴⁰² which showed that employers risk discrimination complaints if they allow employees to create a hostile working environment by downloading and circulating sexually explicit material. Furthermore,

402 *Morse v Future Reality Ltd* 1996-10-22 Case no 54571/95.

M was required to share an office with several men. A considerable amount of the men's time was spent poring over sexually explicit or obscene images downloaded from the Internet. One or two of the pictures were specifically drawn to M's attention, as was a joke toy gorilla that performed a rather lewd trick, but for the most part the circulation and discussion of the images went on in the background. M accepted that these activities were not directed at her personally but they did cause her to feel uncomfortable. Eventually, she resigned and complained of sexual discrimination on grounds of harassment, citing the pictures, bad language and general atmosphere of obscenity in the office as the basis for her complaint. A tribunal held that all the above factors had had a detrimental impact on M such as to constitute sexual harassment and that FR Ltd was liable because no one had taken action to prevent the discrimination. The tribunal awarded damages for injury to feelings and three months' loss of earnings.

under the UK Defamation Act an employer can be held vicariously liable for defamatory statements made by his employee.⁴⁰³ In providing the facilities for access to the Internet, the employer may directly be liable as a publisher or disseminator of the offending statement. Norwich Union was publicly forced to apologise in the UK High Court to Western Provident Association and ordered to pay £450,000 in damages and costs for slander and libel arising out of employee email.

In the RSA, the general rule is that the employer is liable for the wrongful acts of his employee committed in the execution and during the course of his employment.⁴⁰⁴ Whether an employee may be dismissed for such conduct will depend on the nature of the offence and whether the dismissal can be justified in terms of the Labour Relations Act 66 of 1995.

Decisions of the UK courts continue to be invoked where they may illustrate general principles of the law of defamation or explain concepts adopted in South African law.⁴⁰⁵

403 *Godfrey v Demon Internet Limited* QBD 1999 4 All ER 342 2000 3 WLR 1020 2001 QB 201. In this case the court found that Demon Internet Ltd could not rely on a defence under s 1 of the Defamation Act 1996 in the period following Mr Godfrey's complaint about the offending posting on Demon's servers (whereby Demon was put on notice and required to take "reasonable care"). That judgement effectively left Demon with no substantive defence to the claim. Demon unsuccessfully argued that an ISP should be treated like a telephone company and should have no liability for the content of the material carried or displayed.

404 See *Mkize v Martens* 1914 AD 382; *Estate of Van der Byl v Swanepoel* 1927 AD 141; *Feldman (Pty) Ltd v Mall* 1945 AD 733; *Botes v Van Deventer* 1966 3 SA 182 (A); *Minister of Police v Rabie* 1986 1 SA 117 (A).

405 See *SA Associated Newspapers Ltd v Estate Pelsler* 1975 4 SA 797 (A) 810; *Waring v Mervis* 1969 4 SA 542 (W) 546 and *Johnson v Beckett* 1992 1 SA 762 (A).

4 3 2 Interception in South Africa compared

The definition of "electronic communications" as defined in the ECPA⁴⁰⁶ excludes "any wire or oral communication". "Communication" as defined in the Interception Act⁴⁰⁷ includes both direct (oral) and indirect (electronic) communications and therefore includes "oral communication".

4 3 2 1 Business exception

RIPA⁴⁰⁸ in the UK and the Interception Act⁴⁰⁹ of South Africa contains similar provisions relating to the monitoring of electronic communication. When compared to the ECPA⁴¹⁰ of the US it can be noted that the Interception Act⁴¹¹ is aligned with US federal legislation relating to interception and monitoring under the "business exception". Like the ECPA,⁴¹² it contains similar provisions relating to the monitoring of those electronic communications that are monitored "in the ordinary course of business" or with consent.

The Interception Act⁴¹³ contains a business exception that is similar to the "relevance to the business" exception contained in the Regulations published under RIPA.⁴¹⁴ Both these exceptions require that communication must be "relevant" or "relate" to

406 Electronic Communications Privacy Act of 1986.

407 70 of 2002.

408 Regulation of Investigatory Powers Act of 2000.

409 70 of 2002.

410 Electronic Communications Privacy Act of 1986.

411 70 of 2002.

412 Electronic Communications Privacy Act of 1986.

413 70 of 2002.

414 Regulation of Investigatory Powers Act of 2000.

the business before lawful interception can take place.⁴¹⁵ However, under the Regulations an employer will be able to monitor all communications (even private ones with no relation to the business) in order to establish whether they relate to the business or not. Although the Interception Act⁴¹⁶ contains no clear provision which allows for interception in order to establish whether communications are "business related", it can be argued that employers may be allowed to intercept communications for such purpose under the "business exception".⁴¹⁷

Information transmitted in the ordinary course of business is excluded from the definition of "information transmitted by electronic, mechanical, or other devices", as defined in the ECPA.^{418 419} The ECPA⁴²⁰ allows "an agent of a provider of wire or electronic services to intercept, disclose, or use that communication in the normal course of his employment".⁴²¹ As such, the interception of electronic communication is lawful under the ECPA⁴²² if it is done for a legitimate business purpose. Electronic communication is considered business related if the employer has a legal interest in it

415 This is different to the "genuine business need" reference contained in the UK Code of Practice published by the Information Commissioner as to how the legal requirements of the Data Protection Act of 1998 should be implemented. The UK Code of Practice states that "monitoring should only take place where there is a genuine business need". Furthermore, the UK Code of Practice takes cognisance of the employee's privacy in that it states that "the methods used must be proportionate to the employer's legitimate aims, and where there is no undue invasion into the employees' privacy". Of course, the recommendations of the Commissioner are not legislation and serve only as a guide.

416 70 of 2002.

417 See s 6(2)(b)(i)(aa) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 which provides for lawful interception of indirect communications for the purpose of establishing the existence of facts.

418 Electronic Communications Privacy Act of 1986.

419 This exception has yet to be applied to email communications in the workplace.

420 Electronic Communications Privacy Act of 1986.

421 See 2511 2 of title 18 of the United States Code (as amended by s 102 of the Electronic Communications Privacy Act of 1986).

422 Electronic Communications Privacy Act of 1986.

or if interception is necessary to guard against the unauthorised use of electronic communication equipment. Therefore an employer will have a legal interest in electronic communication when it is either in pursuit of or detrimental to the employer's business. In this sense the ECPA⁴²³ regulation is wider than the one contained in the Interception Act which allows for interception provided that communication relates to business activities specifically.⁴²⁴

4 3 2 2 Consent

RIPA⁴²⁵ dictates that it will not be unlawful to intercept a communication if the interceptor reasonably believes that *both* parties to the communication consented to the interception.⁴²⁶ The ECPA⁴²⁷ allows for interception by means of the lawful consent of the originator, or intended addressee, or any recipient of communication.⁴²⁸ The Interception Act⁴²⁹ requires that any person may intercept any communication if *one* of the parties to the communication has given their prior written consent.⁴³⁰

423 Electronic Communications Privacy Act of 1986.

424 See s 6(2) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

425 Regulation of Investigatory Powers Act of 2000.

426 See s 3 of the Regulation of Investigatory Powers Act 2000.

427 Electronic Communications Privacy Act of 1986.

428 See 2511 2(d) of title 18 of the United States Code (as amended by s 102 of the Electronic Communications Privacy Act of 1986).

429 70 of 2002.

430 A further requirement is that the communication may not be intercepted for the purpose of committing a criminal offence. See s 5(1) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

4 3 2 3 Access to stored information

RIPA⁴³¹ does not allow the interception of electronic communications "in the course of its transmission".⁴³² Electronic communication stored on a hard-drive will normally not qualify as "in the course of its transmission", since the hard-drive is not part of the file server which is used for storing it "in a manner that enables the intended recipient to collect it or otherwise to have access to it".⁴³³ As such, information stored on a hard-drive is not protected under RIPA.⁴³⁴

The ECPA⁴³⁵ is not concerned with what happens to information once it is stored as electronic communication. Accessing stored electronic communication sitting on a server waiting to be sent is not illegal. The US courts⁴³⁶ have ruled that since the email is not physically travelling anywhere, it is not "in transit" and therefore does not have the same level of protection under the ECPA.⁴³⁷

Similarly to RIPA,⁴³⁸ communications classified as falling outside the "course of transmission" will not be prohibited from being intercepted under the Interception Act.⁴³⁹ Information stored on the hard-drive of an employee's computer is communication outside the "course of transmission" and is not afforded protection under the Interception Act,⁴⁴⁰ since the hard-drive is not used to transmit such information.

431 Regulation of Investigatory Powers Act of 2000.

432 See s 1 of the Regulation of Investigatory Powers Act 2000.

433 See s 2(7) of the Regulation of Investigatory Powers Act 2000.

434 Regulation of Investigatory Powers Act of 2000.

435 Electronic Communications Privacy Act of 1986.

436 *Steve Jackson Games v US Secret Service* 1994 US 36 F 3d 457.

437 Electronic Communications Privacy Act of 1986.

438 Regulation of Investigatory Powers Act of 2000.

439 70 of 2002.

440 70 of 2002.

4 3 2 4 Disclosure of intercepted information

An important question relates to what use is allowed with respect to information once it has been intercepted?

Under the ECPA⁴⁴¹ an employer may disclose intercepted electronic communication that is business related.⁴⁴² An electronic communication is considered business related if the employer has a legal interest in it or if the interception is necessary to guard against the unauthorised use of electronic communication equipment. An employer will also have a legal interest in an electronic communication when it is either in pursuit of the employer's business or is a detriment to the employer's business.

The UK Data Protection Act (DPA) of 1998 sets out what may and may not be done with the information once it has been obtained. As a general rule, compliance with the relevant data protection principles contained in the DPA⁴⁴³ means that employees must be advised beforehand of the purposes for which personal data about them will be processed.⁴⁴⁴ If employee consent has not been obtained, it is necessary for the employer to show that the collection and use of personal information is necessary for (a) the performance of the employment contract; or (b) is in the vital interests of the employee or (c) falls within one of the statutory exemptions (the most likely of which is that processing is necessary in order to detect or prevent crime).

The Interception Act⁴⁴⁵ does not have a requirement similar to the DPA⁴⁴⁶ whereby employees must be advised when personal data about them will be processed. S 42 of the Interception Act⁴⁴⁷ prescribes that no person may disclose any information that is

441 Electronic Communications Privacy Act of 1986.

442 See 2511 of title 18 of the United States Code (as amended by s 102 of the Electronic Communications Privacy Act of 1986).

443 Data Protection Act of 1998.

444 See Part II, Schedule I of the Data Protection Act 1998.

445 70 of 2002.

446 Data Protection Act of 1998.

obtained through powers conferred in the Act, subject to certain exceptions.^{448 449} These exceptions include (a) persons requiring or supplying information out of necessity for the performance of their functions under the Interception Act;⁴⁵⁰ and (b) information required in terms of any law or as evidence in any court.⁴⁵¹ From the exceptions it appears that employers will be able to disclose intercepted information provided the information fall into one of the exceptions contained in s 42(1) of the Interception Act.⁴⁵²

4 3 2 5 Communication-related information

Communication-related information does not relate to the contents of electronic communications (such as email) but rather to information associated with it, such as origin, destination etc.

Information relating to electronic communication, which excludes the content, is excluded from protection under the ECPA.^{453 454} As a result, employers have access to such information and may disclose it.⁴⁵⁵

447 70 of 2002.

448 See s 42(1)(a) to (d) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

449 Similarly, service providers and their employees or decryption key holders may not disclose information obtained in the exercising of their powers or duties in terms of the Act, subject to the exceptions contained in s 42(1).

450 70 of 2002.

451 See s 42(1)(a) to (c) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

452 70 of 2002.

453 Electronic Communications Privacy Act of 1986.

454 See s 2510 of title 18 of the US Code (as amended by the Electronic Communication Privacy Act of 1986).

455 See s 2511 of title 18 of the US Code (as amended by the Electronic Communication Privacy Act of 1986).

RIPA⁴⁵⁶ governs the lawful acquisition and disclosure of communications data. Under s 22 certain "designated persons" in "relevant public authorities" (which include the Police, the National Criminal Intelligence Service, the Intelligence Services, the Inland Revenue and Customs & Excise) may require a postal or telecommunication operator to obtain and/or disclose communications data in its possession. This may only be done, if necessary, on limited grounds, which include the interests of national security, crime detection and/or prevention, public safety and public health.⁴⁵⁷

The Interception Act⁴⁵⁸ contains a general prohibition against supplying communication-related information to anyone besides the customer of a service provider, provided that the information relates to that customer.⁴⁵⁹ Certain exceptions apply, such as supplying information to a third party as per specific written authorisation of the customer and supplying it under a real-time or archived communication-related direction.⁴⁶⁰ In general, employers will be able to have access to such information, but may have trouble in disclosing it.⁴⁶¹ In particular, no specific exceptions for disclosures seem necessary for court proceedings.

4 3 2 6 Infrastructure - set-up for interception

The US congress passed the Communications Assistance for Law Enforcement Act (CALEA) in August 1994, largely in response to the FBI's concern that new technologies could be used to impede criminal investigation.⁴⁶² With this legislation

456 Regulation of Investigatory Powers Act of 2000.

457 See s 22(2) of the Regulation of Investigatory Powers Act of 2000.

458 70 of 2002.

459 See s 12 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

460 See s 13 and 14 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

461 See s 42(1) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

462 See report of the EC Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications (96/C 329/01).

the government intended to secure its ability to eavesdrop on rapidly evolving digital services offered by new telecommunications carriers.⁴⁶³ In ensuring telephone companies will comply with this law or risk \$10,000 per day in fines, a subsidy fund of 500 million US dollars was established. In essence, CALEA⁴⁶⁴ requires a redesign of the US communications network to facilitate surveillance on all forms of electronic media.⁴⁶⁵ This law requires telecommunications companies to wire surveillance technology into their networks, which could force Internet telephony firms to configure their systems to allow for streamlined wiretapping by law-enforcement agencies. The FCC has stated that CALEA⁴⁶⁶ applies to all "packet-switched technology" that is used to provide telecommunications services.⁴⁶⁷

RIPA⁴⁶⁸ assigns the duty in determining fair compensation for telecommunication service providers in rendering assistance with the execution of interception warrants to the Secretary of State.⁴⁶⁹

The requirements imposed on service providers in the Interception Act⁴⁷⁰ are similar to those entrenched in CALEA.⁴⁷¹ For example, the Interception Act⁴⁷² requires that

463 Frezza "The CALEA Time Bomb is Still Ticking" *Network Computing* (1997-7-10). See <http://www.networkcomputing.com/813/813colfrezza.html>.

464 Communications Assistance for Law Enforcement Act of 1994.

465 Included in this redesign is a call for standards that require every cell phone to provide location information of users to police.

466 Communications Assistance for Law Enforcement Act of 1994.

467 McCullagh "Wiretapping Internet Phone Lines" *Wired News* (1998-11-10). Many intelligence agencies have also lobbied to limit the security features in GSM in order to facilitate interception of cellular telephony. See Lagan & Davies "New Digital Phones On-line Despite Objections" *The Sydney Morning Herald* (1998-4-28).

468 Regulation of Investigatory Powers Act of 2000.

469 See s 14(1) of the Regulation of Investigatory Powers Act of 2000.

470 70 of 2002.

471 Communications Assistance for Law Enforcement Act of 1994.

472 70 of 2002.

"a telecommunication service provider must (a) provide a telecommunication service which has the capability to be intercepted; and (b) store communication-related information".⁴⁷³ Furthermore, the Interception Act⁴⁷⁴ provides for the minister to prescribe the "forms of assistance" by, and "compensation" payable to, a "postal service provider, telecommunication service provider or decryption key holder" for providing assistance with the execution of a direction.

4 3 2 7 Liability

The ECPA⁴⁷⁵ provides for criminal penalties (in the form of fines and imprisonment) and private civil actions to recover damages, in cases of transgression. RIPA⁴⁷⁶ differentiates between a private and criminal tort when dealing with unlawful interceptions on private and public networks in turn. The Interception Act⁴⁷⁷ contains no such distinction and stipulates that the transgression of the Act is an offence, which may attract a fine or imprisonment.

4 3 3 Expectation of privacy

The question can be raised whether employees have an expectation to privacy given the Constitution.⁴⁷⁸ The court's decision in the *Protea Technology* case *supra* indicates that our judiciary is less inclined to provide employees with extensive privacy rights under the Constitution⁴⁷⁹ when they abandon the private sphere for that of their employer. Furthermore, employees that are made aware of the fact that employers subject their communications to interception should have little expectation

473 See s 30(1) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

474 70 of 2002.

475 Electronic Communications Privacy Act of 1986.

476 Regulation of Investigatory Powers Act of 2000.

477 70 of 2002.

478 108 of 1996.

of privacy in the workplace. The US courts⁴⁸⁰ have supported a similar proposition that employees should not have an expectation of privacy where employers have made them aware, by means of a well-written user policy for example, of possible interception of their electronic communications. The European Court of Human Rights expressed a similar view in the *Halford*⁴⁸¹ case.

4 3 4 Constitution

The South African Constitution⁴⁸² makes specific, although not exhaustive, reference to a number of possible constitutional violations concerning surveillance laws. The US case *Katz v United States*⁴⁸³ refers to the interception of communications as constituting a "search and seizure". This might also have application to the South African situation.⁴⁸⁴ S 14(a) and (b) of the Constitution,⁴⁸⁵ which prohibits a violation of person, home or property, supports this assertion. John Locke pronounced the idea that "every man has a property in his own person".⁴⁸⁶ Therefore, all that man creates and becomes is part of "his own person" and nobody has any right other than to himself.⁴⁸⁷ Courts around the world have through the years echoed this sentiment by saying: "the most comprehensive of rights and the right most valued by civilised men

479 108 of 1996.

480 See *Smyth v Pillsbury* cases *supra*.

481 See *Halford v United Kingdom* 1997 73/1996/692/884.

482 108 of 1996.

483 See *Katz v United States* *supra*.

484 On search and seizure generally, see Neethling *Law of Personality* and McQuoid-Mason *The Law of Privacy* *supra*. For an interpretation of the scope of the right to privacy and its limitations regarding search and seizure, see the comments of Sachs J in *Mistry* *supra* at par 23.

485 108 of 1996.

486 Locke *The Second Treatise of Civil Government* (1960) cited in Konovitz *Privacy and the Law: A Philosophical Prelude* (1966).

487 See McQuoid-Mason *The Law of Privacy* 3.

is the right to be let alone".⁴⁸⁸ It appears that s 14 of the Constitution⁴⁸⁹ as read to pertain to surveillance laws, sets an inordinately high standard for a limitations review, especially in the light of the specific guarantee in s 14 pertaining to the privacy of communications.

Article 8 of the Human Rights Act (incorporating the European Convention on Human Rights) acknowledges the right of an individual to "respect for privacy". In addition, the US Constitution affords citizens an "implied" right to privacy. However, it would appear that this right only applies to what the US government may or may not do with regards to "search and seizure". US court cases such as *Griswold v Connecticut*⁴⁹⁰ has recognised an applied right to privacy. Consequently, private employers are generally not required to afford employees protections granted under the US Constitution.⁴⁹¹ In SA, the Constitution⁴⁹² provides every person (including private employees) with the right to privacy. Furthermore, s 14 (d) provides everyone with the right to not have the privacy of their communications infringed. This right applies to the state as well as employers and employees in the private sphere.

488 See *Olmstead v United States supra* at 478, per Brandeis J.

489 108 of 1996.

490 See *Griswold v Connecticut* 1965 381 US 479 85 1678.

491 See *O'Connor* and *Smyth* cases *supra*. Also see *Bourke* and *Smyth* cases *supra* on the US common law tort of "invasion of privacy".

492 108 of 1996.

5 Practical suggestions for employers faced with implementing data security policies and monitoring processes

5 1 Where to from here?

Businesses today are geared towards turning a profit. Simply put, the making of a profit is more vital to a company's existence than any other factor.

Companies use monitoring tools to stay on top of their game. Employers need to ensure that employees are able to perform the required functions they were employed to do. In addition, the employer wants to safeguard itself against a myriad of legal liabilities associated with employees using its telecommunication systems. However, employers should not have "free-reign" over their employees in order to monitor them secretly and at will. The solution is to adopt a middle ground that balances certain aspects by means of a compromise that is both reasonable and just.

5 2 Practical suggestions

South African employers are faced with implementing legislation, such as the Interception Act,⁴⁹³ in addition to those general requirements set out in the Constitution.⁴⁹⁴ This is by no means an easy task since the practical implications are often removed from the intention of the legislator. Even then, legislators cannot foresee all possible results following their legislation. However, good old-fashioned common sense can be applied when dealing with ways to address the issues faced by employers.

The following suggestions are intended to help employers that are faced with the practical implementation of electronic communication and data security policies, as well as monitoring processes. However, it should be noted that these suggestions are of general application and guidance, and should therefore not be relied upon to the exclusion of separate legal advice.

493 70 of 2002.

494 108 of 1996.

5 2 1 General

Both parties to the employment relationship share the same goals and preferences. They both desire favourable working conditions and relations, manageable stress levels and a successful business that turns a profit. If the parties can keep these mutually beneficial ideals in mind, it will help to strengthen the bond between them, and neither will feel slighted. One way of doing this is for employers to create comfortable working conditions for their employees and to keep their welfare at heart. Likewise, employees need to understand that a successful business will ultimately mean successful careers for everyone involved.

Employers should accept some personal use of their electronic communication facilities, as segregating work from personal activities might result in a net decline in employee work performance and morale.⁴⁹⁵

A new study conducted in December 2002 by the University of Maryland Robert H Smith School of Business (along with marketing company Rockbridge Associates) have found that employees with Internet access spend an average of 3.7 hours per week "surfing" sites for personal use at work. However, they spend an average of 5.9 hours per week, logging in from home for work purposes. This survey suggests that even though employees may waste time "surfing" the Internet at work, they make up for it working from home in their off hours.⁴⁹⁶

5 2 2 Employee consent

An element common to both the Interception Act⁴⁹⁷ and IMPA⁴⁹⁸ is that of consent. For the purposes of monitoring and interception, securing employee consent is the best approach. As far as the fundamental right to privacy and the Interception Act⁴⁹⁹ is

495 Bowman "Office Surfers Aren't Slackers" *Intelligence: Total Business magazine* (2003-5-01) 13.

496 Bowman *Intelligence: Total Business magazine* (2003-5-01).

497 70 of 2002.

498 127 of 1992.

499 70 of 2002.

concerned, once consent has been obtained the issue of compliance largely disappears. Of course, it must be noted that an allowance is made for interception in the course of "carrying on of the business" of the employer under the Interception Act.⁵⁰⁰

Coupled with consent is the requirement that employers must be able to demonstrate that "reasonable efforts" were taken to inform employees that the monitoring of electronic communications could be performed. Such efforts may include the following:

- (a) employees may be provided with a copy of the employer policies related to the use of electronic communication and their enforcement - employees may also be asked to acknowledge their receipt and understanding by means of a signature;
- (b) employees may be informed periodically of related employer policies;
- (c) electronic "alerts" by means of pop-up messages can also be used to create awareness that monitoring and interception activities may be performed.

5 2 3 Employer policy guidelines

Employees must be made aware of the "do's and don'ts" relating to the use of employer services and equipment. The need for clear and explicit employer policies and the communication thereof is of vital importance in the employer/employee working relationship. The following suggestions relate to those policies that may contain employer instructions and guidelines with respect to the employee use of electronic communication:

- (a) As a condition of employment, employers should require all employees to acknowledge receipt of the employer's electronic communication policy. This should include the use of both email and the Internet.

500 See s 6 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

- (b) The policy should explicitly address the procedures that will be followed in disciplining employees who violate or abuse any privilege contained in the policy.
- (c) Such a policy should include the *caveat* that the employer's electronic communication system is neither confidential nor private and as such may be monitored.
- (d) Electronic communication guidelines (Netiquette) as to the right way of making use of employer electronic communication resources should be included. Employers should not just list a myriad of unacceptable uses but also let employees know what they regard as constituting acceptable use.
- (e) The policy may also state that the employer may, for legitimate and lawful business activities, access any contents of electronic communication. Some specific prohibitions may include:
 - (i) private use outside boundaries set by employer for private business use;
 - (ii) sending or forwarding of chain letters;
 - (iii) sending of obscene or unwarranted content;
 - (iv) sending of discriminating content;
 - (v) sending of confidential or unauthorised employer information;
 - (vi) sending of objectionable content relating to language or unethical matters;
 - (vii) internet use outside the boundaries set by an employer such as participating in non work related bulletin boards (BBS);
 - (viii) uploading of software from the internet or other medium without following an employer procedure policy - this could be relevant to both virus protection and copyright issues;
 - (ix) use thereof to conduct a criminal activity;
 - (x) allowing non-employees to use employer facilities;

- (xi) sending private adverts.

- (f) Electronic communications such as email often remain unchecked and do not require adherence to any specific format. This may cause employer liability in a number of situations. It should be remembered that email sent out under the auspices of company communication are like any other communication, be it a letter or document, a communication of that specific employer. As such, it should be treated with the same care. Specific disclaimers should be included within email signatures, and on any other electronic services such as web sites, to provide a clear distinction between the employee's own personal comments and their statements on behalf of the employer.

However, it is important to remember that the existence of an electronic communication policy will on its own not be enough. An employer will also have to ensure that the policy is adhered to in practice and is consistently applied. For example, an employer will have difficulty justifying a dismissal for email abuse if the employee can show that a blind eye has been turned in respect of other employees in similar circumstances. Whilst the precise content of a policy will vary depending on the culture within different companies, it is necessary to ensure that offences are specified if the rules are to be successfully relied on by the employer.

5 2 4 Monitoring

The use of alternative monitoring techniques should be employed whenever possible. The monitoring of electronic communication should only be performed when it is the only means to achieve an accurate assessment of the employee, or when the employee's actions are in reasonable suspicion. Other monitoring techniques that have been employed in the past should not be excluded if such techniques are still reasonable. For example, co-workers working directly with their colleagues are certainly qualified to give an accurate report of their fellow employees. As a result, employee evaluation can be successfully executed by means of peer evaluation. In addition, supervisors should also be qualified and capable in providing accurate reports relating to the work ethic of those that serve under them. Substituting experienced judgement with monitoring may be seen as suspicious, since monitoring is often an inaccurate method of evaluating an employee.

Selective monitoring should be kept to a minimum and only executed in very specific cases. If factors necessitate monitoring, employees should be targeted as a whole, rather than individuals. A positive spin-off in targeting groups rather than individuals may include:

- (a) reducing individual stress;
- (b) building team spirit and foster group motivation towards meeting common goals;
- (c) group members can help to compensate for those that have fallen behind;
- (d) building unity, team spirit and trust among employees.

Monitoring should only be executed in reasonable time frames. For example, monitoring by the minute will often contribute to higher stress levels in employees than monitoring by the hour. The reason for this is that employees monitored on such a small time scale might feel trapped, as if they cannot loose one second for fear of not meeting the standards set by the employer.

Employers should communicate monitoring activities (and the criteria used) to staff before the event in order for staff to prepare for employer scrutiny.

Employers should refrain from "snooping" into the personal electronic communication of employees barring a just cause. Employers should keep in mind that personal items in cyberspace (such as an email message) should not be any different than personal physical items like a handbag for example.

5 2 5 Intellectual property

The issues of intellectual property may be dealt with as part of the employment contract, job description, or by confidentiality clauses within a contract for consultants and self-employed workers. Today, most employers require, as part of a contract of employment, that they have the right (or right of "first refusal") to anything that the employee creates during their term of employment. This may also include work product created at home, provided that it is related to the function for which they are employed. Problems may occur in the following scenarios:

- (a) Employees use the employer's services (equipment and software) in their homes. In this case, the employer could claim that developments or information was produced at their expense.
- (b) Employees replicate parts of the information they use in the workplace at home. The employer could argue a right of ownership to the material, or, if not, that the employee has breached the employer's copyright.

In order to avoid confusion, an employee that wishes to produce material in their own right should (a) seek to obtain either a contractual demarcation of their own work from that of their regular employment (if it is produced within the employee's home); or (b) if the employee intends to use the facilities provided by the employer, negotiate some official form of licensing agreement that reserves the employee's rights, or some form of leasing agreement that allows the employee to use the employer's facilities without giving over any rights to the employer.

In the end the employer has to make sure that the policies and procedures implemented must withstand legal scrutiny. Ultimately, it entails a balancing act between the rights of the employer and employee.

6 Conclusion

Electronic communication tools such as computers, computer networks and the internet/intranet have become inextricably linked to day-to-day working activities of most employees. Our working activities have been transformed by electronic communication in less than a generation.

A large portion of productivity time is wasted as employers monitor the electronic communication of their employees, and employees constantly think about whether they are in fact transgressing a company rule in performing their current activity. As a result, employee morale and company productivity decrease while a deadlock results in the relationship of employer and employee.

Electronic communication has played a major role in most successful modern-day companies and organisations throughout the world. Despite the heavy use of manual internal information exchange, the rise of electronic commerce has proved what important role electronic communication play in business. As such, employees are not only dealing with internal documents, but also with external client communications, such as contract proposals, orders, customer support, etc, via an employer's electronic communication system. There can be no doubt that electronic communication has become a backbone of business, especially international electronic commerce.⁵⁰¹

With the increased focus on electronic communication the law has become a complex myriad of legislative "do's and don'ts" catering for most communication aspects of the daily working life. In addition, there are constitutional considerations when dealing with electronic communication monitoring on the workplace. These include the potential infringement on the "right to privacy of communications" entrenched in our Constitution⁵⁰² and the constitutionality of the newly enacted Interception Act.⁵⁰³

501 Cavanagh "Workplace Privacy: in an Era of New Technologies" *Cavanagh Associates Inc.* See <http://www.ema.org/html/pubs/mmv2n3/workpriv.htm>.

502 108 of 1996.

503 70 of 2002.

6 1 Interception Act

Although the newly ascerted Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 ("Interception Act") is not yet in use, it will repeal the Interception and Monitoring Prohibition Act 127 of 1992 once a commencement date is announced.

The Interception Act⁵⁰⁴ contains a general prohibition against the interception (included in the definition are both interception and monitoring) of communications (both direct and indirect), meaning that both voice communications (direct) and electronic communications such as email (indirect) are prohibited from being monitored subjected to certain provisions. This gives effect to the s 14(d) Constitutional right of a person "not to have the privacy of communications infringed". However, it does not end there since the Interception Act⁵⁰⁵ contains several exceptions where the general prohibition against interception would not apply. These include interceptions under an "interception direction" issued by a judge,⁵⁰⁶ interception by one of the parties to a communication,⁵⁰⁷ interception with the written consent of one of the parties to a communication⁵⁰⁸ and interception under the "business exception".⁵⁰⁹

Of particular importance to this thesis are the last three, since they will most often occur during a working relationship of an employer and employee. Of note is that

504 70 of 2002.

505 70 of 2002.

506 See s 3 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

507 See s 4 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

508 See s 5 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

509 See s 6 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

these three exceptions differ as to the ambit of the communications that may be intercepted. The "party to" and "consent" exceptions apply to both direct and indirect communications. The "business exception" only applies to indirect communications. Although employers will be able to use the exception allowing interception as a party to the communication provided in s 4,⁵¹⁰ it should be noted that it will be safer to obtain written consent in terms of s 5, since it should often happen that in making a communication employees will not be seen as "acting on behalf of the employer" or that the communication will be addressed to the employer. In such cases, an employer will not be allowed to rely on s 4.

The Interception Act⁵¹¹ contains a general prohibition against the interception of communication that falls within the "the course of its occurrence or transmission" provision. An employer that intercepts such communication will have to comply with the exception requirements as set out in the act. The Interception Act⁵¹² does not prohibit the interception of communication outside the "the course of its occurrence or transmission" and employers will not be contravening the Interception Act⁵¹³ if they intercept such communication. As discussed, it seems likely that the interpretation of the phrase "in the course of its occurrence or transmission" will include communication stored on an email server, but exclude communication stored on the hard-drive of an employee's computer.

A controversial exception contained in the Interception Act⁵¹⁴ is the business exception. It is unclear as to what will constitute "in the course of carrying on a business". The word "business" is broadly defined as "any business activity conducted by any person". The question is raised whether the interpretation of "in the course of carrying on a business" will include communications of employees that take place

510 An employee may act on behalf of an employer, which means the employer will be a party to the communication through its employee or "agent".

511 70 of 2002.

512 70 of 2002.

513 70 of 2002.

514 70 of 2002.

during a lunch hour, when employers may expect their employees to be busy with private rather than "business" matters? Under the US Electronic Communications Privacy Act of 1986, electronic communication is considered business related if the employer has a legal interest in it or if interception is necessary to guard against the unauthorised use of electronic communication equipment. The Regulations published under the UK Regulation of Investigatory Powers Act of 2000, allows an employer to monitor all communications (even private ones with no relation to the business) in order to establish whether they relate to the business or not. If guidance is to be taken from such legislation it appears that little (if any) communication of employees will be excluded from interception. It will be interesting to see how the South African courts will interpret this.

With the writing into law of the Interception Act,⁵¹⁵ South Africa has joined other first world countries in regulating the interception of electronic communication. However, employees in South Africa are generally still ignorant of the fact that their electronic communications may be subjected to monitoring. The Interception Act⁵¹⁶ aims to change this by requiring employers to communicate interception activities under the business exception to employees and thereby informing them of when, how and under what conditions such activities will take place.⁵¹⁷

6 2 Improving the Interception Act

The Interception Act⁵¹⁸ is not merely a piece of legislation enacted to confuse employers and employees alike. A lot of deliberation went into its drafting. However, certain confusing issues remain which are open for interpretation. In addition, the legal ramifications (such as the stiff penalties) are severe and non-compliance could result in more than just a slap on the wrist. With this in mind, the following improvements may be able to clarify some of the shortcomings of the act:

515 70 of 2002.

516 70 of 2002.

517 See s 6(2)(d) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

- (a) The DPA Code of Practice was drafted to act as a benchmark for UK employers that have to comply with the DPA⁵¹⁹ itself. The "benchmarks" contained in the Code of Practice are designed to suggest that failure to comply means failure to comply with the DPA⁵²⁰ itself. It is therefore a practical measure for employers to judge their own compliance, leaving less room for guesswork. Such a "code of practice" aimed to help employers comply with the Interception Act⁵²¹ would invariably help SA employers and employees alike. For example, employers should only monitor electronic communication when a "real business need" has been established, and if the methods used are proportionate to the aims of the employer and not unduly invasive upon employee privacy.
- (b) The phrase "in the course of carrying on of the business" could be better defined. Exceptions should be noted, such as when employees spend time on private issues where there is a legitimate expectation of privacy; for example during meal intervals or simply dialling in from home after-hours.
- (c) The Interception Act⁵²² fails to differentiate between indirect communications that are received from third parties which may have no relevance to the business of the employer, and those originating from employees which stand in a working relationship with the employer. It is suggested that the former type of communication be afforded more protection under the Act.

The Interception Act⁵²³ is a new piece of legislation and will mature through interpretation by the South African courts in interpreting those provisions, which remain unclear. At the same instance, it comes at a time when SA employers desperately need legal guidance on electronic communication matters relating to their

518 70 of 2002.

519 Data Protection Act of 1998.

520 Data Protection Act of 1998.

521 70 of 2002.

522 70 of 2002.

523 70 of 2002.

businesses. What remains to be seen is whether it will mature like good red wine or become sour in the mouths of employers and employees alike, and regarded as another Act which acts as a barrier to technological advancement and business initiative.

6 3 Constitution

S 14 (d) of the Constitution⁵²⁴ provides for the right not to have the privacy of communications infringed. As such, it contains a general prohibition against the interception and monitoring of communications. The Interception Act⁵²⁵ clearly places limitations on this constitutional right. The question then becomes whether the Interception Act⁵²⁶ can survive constitutional scrutiny under the Constitution's⁵²⁷ limitation clause. As discussed, it appears that the Interception Act,⁵²⁸ in general, may be held to be constitutional. However, certain sections such as the "business exception" may be found too wide in reach, and be found unconstitutional. For example, an employer intercepting the communication of an employee is one thing, but what is the justification for intercepting the incoming communication of a third party that has no relevance to the employer or his business, save for the fact that he is sending an indirect communication that happens to be routed through the telecommunication system of the employer? These and other "far reaching" implications will most likely be factors in deciding the constitutionality of the Interception Act,⁵²⁹ or parts thereof.

524 108 of 1996.

525 70 of 2002.

526 70 of 2002.

527 108 of 1996.

528 70 of 2002.

529 70 of 2002.

Intercepting communication that fall outside the provisions of the Interception Act⁵³⁰ may still be challenged in terms of the Constitution.⁵³¹ Such interception may potentially infringe on the right to privacy of communications and relief may be sought under s 14(d) of the Constitution.⁵³² Courts⁵³³ have asked whether a "reasonable expectation" to privacy exist. In defending such claims employers will have to show that a "reasonable expectation" did not exist, of which the outcome will largely depend on the facts.

It would appear that obtaining consent prior to interception is the best course of action for employers. Not only will it afford them an exception under the Interception Act,⁵³⁴ but will also aid in proving that employees were aware their communications may be intercepted and that they therefor did not have a "reasonable expectation" to privacy of communications.

530 70 of 2002.

531 108 of 1996.

532 108 of 1996.

533 See *Bernstein v Bester supra*.

534 70 of 2002.

Glossary of computer terms⁵³⁵**Backbone**

A high-speed line or series of connections that forms a major pathway within a network. The term is relative as a backbone in a small network will likely be much smaller than many non-backbone lines in a large network.

Bandwidth

How much stuff you can send through a connection. Usually measured in bits-per-second. A full page of English text is about 16,000 bits. A fast modem can move about 57,000 bits in one second. Full-motion full-screen video would require roughly 10,000,000 bits-per-second, depending on compression.

Baud

In common usage the baud rate of a modem is how many bits it can send or receive per second. Technically, baud is the number of times per second that the carrier signal shifts value - for example a 1200 bit-per-second modem actually runs at 300 baud, but it moves 4 bits per baud (4 x 300= 1200 bits per second).

BBS (Bulletin Board System)

A computerized meeting and announcement system that allows people to carry on discussions, upload and download files, and make announcements without the people being connected to the computer at the same time. In the early 1990's there were many thousands (millions?) of BBS's around the world, most are very small, running on a single IBM clone PC with one or two phone lines. Some are very large and the line between a BBS and a system like AOL gets crossed at some point, but it is not clearly drawn.

⁵³⁵ See <http://www.matisse.net/files/glossary.html>. Used with permission from Matisse Enzer - Copyright © 1994-2002 by Matisse Enzer.

Bit (Binary DigIT)

A single digit number in base-2, in other words, either a 1 or a zero. The smallest unit of computerized data. Bandwidth is usually measured in bits-per-second.

Browser

A program (software) that is used to look at various kinds of Internet resources.

Client

A software program that is used to contact and obtain data from a server software program on another computer, often across a great distance. Each Client program is designed to work with one or more specific kinds of server programs, and each server requires a specific kind of Client. A Web Browser is a specific kind of Client.

CPU (central processing unit)

CPU is an older term for processor and microprocessors, the central unit in a computer containing the logic circuitry that performs the instructions of a computer's programs.

Cyberliability

Cyberliability is a generic term coined in the late 1990s for various types of legal liability arising from business use of the Internet and email.

Cyberspace

Term originated by author William Gibson in his novel Neuromancer the word Cyberspace is currently used to describe the whole range of information resources available through computer networks.

Download

Transferring data (usually a file) from another computer to the computer you are using. The opposite of upload.

Email (Electronic Mail)

Messages, usually text, sent from one person to another via computer. E-mail can also be sent automatically to a large number of addresses.

FTP (File Transfer Protocol)

A very common method of moving files between two Internet sites.

FTP is a way to login to another Internet site for the purposes of retrieving and/or sending files. There are many Internet sites that have established publicly accessible repositories of material that can be obtained using FTP, by logging in using the account name "anonymous", thus these sites are called "anonymous ftp servers".

FTP was invented and in wide use long before the advent of the World Wide Web and originally was always used from a text-only interface.

GUI

A GUI (usually pronounced GOO-ee) is a graphical (rather than purely textual) user interface to a computer. The term came into existence because the first interactive user interfaces to computers were not graphical; they were text-and-keyboard oriented and usually consisted of commands you had to remember and computer responses that were infamously brief. The command interface of the DOS operating system (which you can still get to from your Windows operating system) is an example of the typical user-computer interface before GUIs arrived.

Today's major operating systems provide a graphical user interface. Applications typically use the elements of the GUI that come with the operating system and add their own graphical user interface elements and ideas. A GUI sometimes uses one or more metaphors for objects familiar in real life, such as the desktop, the view through a window, or the physical layout in a building. Elements of a GUI include such things as: windows, pull-down menus, buttons, scroll bars, iconic images, wizards, the mouse, and no doubt many things that have not been invented yet. With the increasing use of multimedia as part of the GUI, sound, voice, motion video, and virtual reality interfaces seem likely to become part of the GUI for many applications. A system's graphical user interface along with its input devices is sometimes referred to as its "look-and-feel".

Home Page (or Homepage)

Several meanings. Originally, the web page that your browser is set to use when it starts up. The more common meaning refers to the main web page for a business, organization, person or simply the main page out of a collection of web pages, eg "Check out so-and-so's new Home Page".

Hypertext

Generally, any text that contains links to other documents - words or phrases in the document that can be chosen by a reader and which cause another document to be retrieved and displayed.

Internet

The vast collection of inter-connected networks that are connected using the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's.

The Internet connects tens of thousands of independent networks into a vast global internet and is probably the largest Wide Area Network in the world.

Intranet

A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use. Compare with extranet.

Maillist (or Mailing List)

A (usually automated) system that allows people to send email to one address, whereupon their message is copied and sent to all of the other subscribers to the mail list. In this way, people who have many different kinds of email access can participate in discussions together.

Mainframe

Mainframe is an industry term for a large computer, typically manufactured by a large company such as IBM for the commercial applications of Fortune 1000 businesses and other large-scale computing purposes. Historically, a mainframe is associated with centralized rather than distributed computing. Today, IBM refers to its larger processors as large servers and emphasizes that they can be used to serve distributed users and smaller servers in a computing network.

Microcomputer

A microcomputer is a complete computer on a smaller scale and is generally a synonym for the more common term, personal computer or PC, a computer designed for an individual.

Modem (MODulator, DEModulator)

A device that connects a computer to a phone line. A telephone for a computer. A modem allows a computer to talk to other computers through the phone system. Basically, modems do for computers what a telephone does for humans.

Mosaic

The first WWW browser that was available for the Macintosh, Windows, and UNIX all with the same interface. Mosaic really started the popularity of the Web. The source-code to Mosaic was licensed by several companies and used to create many other web browsers.

Mosaic was developed at the National Center for Supercomputing Applications (NCSA), at the University of Urbana-Champaign in Illinois, USA. The first version was released in late 1993.

Netiquette

The etiquette on the Internet.

Netscape

A WWW Browser and the name of a company. The Netscape (tm) browser was originally based on the Mosaic program developed at the National Center for Supercomputing Applications (NCSA).

Network

Any time you connect two or more computers together so that they can share resources, you have a computer network.

Password

A code used to gain access (login) to a locked system. Good passwords contain letters and non-letters and are not simple combinations such as virtue7.

A good password might be:

5%df(29)

Posting

A single message entered into a network communications system.

Search Engine

A (usually web-based) system for searching the information available on the Web.

Some search engines work by automatically searching the contents of other systems and creating a database of the results. Other search engines contains only material manually approved for inclusion in a database, and some combine the two approaches.

Server

A computer, or a software package, that provides a specific kind of service to client software running on other computers. The term can refer to a particular piece of software, such as a WWW server, or to the machine on which the software is running, eg "Our mail server is down today, that is why email isn't getting out".

A single server machine can (and often does) have several different server software packages running on it, thus providing many different servers to clients on the network.

Spam (or Spamming)

An inappropriate attempt to use a mailing list, or USENET or other networked communications facility as if it was a broadcast medium (which it is not) by sending the same message to a large number of people who did not ask for it. The term probably comes from a famous Monty Python skit, which featured the word Spam repeated over and over. The term may also have come from someone's low opinion of the food product with the same name, which is generally perceived as a generic content-free waste of resources. (Spam® is a registered trademark of Hormel Foods Corporation⁵³⁶, for its processed meat product.)

536 See <http://www.spam.com>.

TCP/IP (Transmission Control Protocol/Internet Protocol)

This is the suite of protocols that defines the Internet. Originally designed for the UNIX operating system, TCP/IP software is now included with every major kind of computer operating system. To be truly on the Internet, your computer must have TCP/IP software.

Telnet

Telnet is the way you can access someone else's computer, assuming they have given you permission. (Such a computer is frequently called a host computer.) More technically, Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. On the Internet, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

Telnet is most likely to be used by program developers and anyone who has a need to use specific applications or data located at a particular host computer.

Terminal

A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry. Usually you will use terminal software in a personal computer - the software pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.

Tymnet

Tymnet is a gateway system, like Telnet.

Unix

Unix (often spelled "UNIX", especially as an official trademark) is an operating system that originated at Bell Labs in 1969 as an interactive time-sharing system. Ken Thompson and Dennis Ritchie are considered the inventors of Unix. The name (pronounced YEW-nihks) was a pun based on an earlier system, Multics. In 1974, Unix became the first operating system written in the C language. Unix has evolved as a kind of large freeware product, with many extensions and new ideas provided in a variety of versions of Unix by different companies, universities, and individuals.

Partly because it was not a proprietary operating system owned by any one of the leading computer companies and partly because it is written in a standard language and embraced many popular ideas, Unix became the first "open" or standard operating system that could be improved or enhanced by anyone.

Unix operating systems are used in widely sold workstation products from Sun Microsystems, Silicon Graphics, IBM, and a number of other companies. The Unix environment and the client/server program model were important elements in the development of the Internet and the reshaping of computing as centered in networks rather than in individual computers. Linux, a Unix derivative available in both "free software" and commercial versions, is increasing in popularity as an alternative to proprietary operating systems.

Upload

Transferring data (usually a file) from a computer you are using to another computer. The opposite of download.

UUCP -- (Unix-to-Unix Copy Protocol)

UUCP is a set of Unix programs for copying (sending) files between different UNIX systems and for sending commands to be executed on another system.

Web

Short for "World Wide Web"

WWW (World Wide Web)

World Wide Web (or simply Web for short) is a term frequently used (incorrectly) when referring to "The Internet"; WWW has two major meanings:

First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools.

Second, the universe of hypertext servers (HTTP servers) which are the servers that allows text, graphics, sound files, etc. to be mixed together.

Bibliography

Books

Barbour *Ethics In An Age of Technology: The Gifford Lectures II* (1993)

Basson, Christianson, Garbers, Le Roux, Mischke & Strydom *Essential Labour Law I* (1998)

Bernard & Evans *New Microcomputer Techniques for Anthropologists Human Organization* (1983) 182-185

Butterworths *The Law of South Africa Volume 13(1) Labour Law*

Carby-Hall *Worker Participation in Europe* (1977)

Davies & Friedland *Kahn-Freud's Labour and the Law* (1983)

De Waal, Currie & Erasmus *The Bill of Rights Handbook* (1998)

Dionisopoulos & Ducat *The Right to Privacy* (1976)

Du Plessis 'n *Arbeidsregtelike Studie met betrekking tot die Deelname van Werknemers in die Besluitnemingsprosesse in Nywerhede* (1984) Unpublished thesis University of South Africa

Du Plessis & Corder *Understanding SA's Transitional Bill of Rights* (1994)

Freedman *Social Security Law: General Principles* 515–517

Government Gazette *Recommendations of Ministerial Task Team – Explanatory Memorandum* 16259 110

Hanau & Adomeit *Arbeidsrect* 113

Hall *Constitutional Law Journal* (1998) 1-30

Hogg *Constitutional Law of Canada 3ed II* (1996) 45-70

Hubbatt *The New Battle Over Workplace Privacy* (1998) 212

Jones & Griffiths *Labour Legislation in South Africa* (1980)

Kerr *The Law of Agency 3ed* (1991) 28-38

Konovitz *Privacy and the Law: A Philosophical Prelude* (1966)

Locke *The Second Treatise of Civil Government* (1960)

- McQuoid-Mason *The Law of Privacy in South Africa* (1978) 3-9
- Neethling *Law of Personality* 4ed (1998)
- Nel & Van Rooyen *Worker Representation in Practice in SA* (1987)
- Robinson *Worker Participation* 49
- Schminke *Managerial Ethics: Moral Management of People and Processes* (1998)
- Scholtens *Conclusion of Contracts of Hire of Services* (1959) SALJ 28
- Strydom *The Employer Prerogative from a Labour Law Principle* (1997) LLD thesis
Pretoria University of South Africa 46–51
- The Guide to American Law VIII* (1984)
- Van Jaarsveld, Van Eck & Kruger *Kompendium van Suid-Afrikaanse Arbeidsreg*
(1992)
- Verdisco *Security threat: Anti-monitoring bills Discount Merchandiser* (1994) 8
- Wallis *Labour and Employment Law* (1992) 8–9
- Weil & Rosen *TechnoStress: Coping With Technology @Work @Home @Play*
(1997)
- Westrum *Technologies and Society Belmont* (1991)
- Zöllner & Loritz *Arbeitsrecht* 437

Magazines, journals and periodicals

Adams, Scheuing & Feeley Stacey "E-mail Monitoring in the Workplace: The Good, the Bad and the Ugly" 2000 *Defence Council Journal* 32-46 29

"Alleged Hoax E-mailers to Face Charge of Sabotage" *ANC Daily News Briefing* (2001-9-18)

Banisar "Privacy & Human Rights 2000" *Privacy International* (2001-02-20)

Barlow "Do Employees' Electronic Messages Spell Trouble for You?" *Personnel Journal* (2001-1-31) 135

"Big Brother?" *The New York Times* (1987-5-10) 14

Borck "Full, Open Disclosure of E-resource Policies Yields Better Feelings in Your Employees" *InfoWorld* (2000-11-20) 80

Bowman "Office Surfers Aren't Slackers" *Intelligence: Total Business magazine* (2003-5-01) 13

Brown "The Mess Made for Business Junk Mail" *Business Week* (1999-4-19)

Bullock "Committee of Inquiry on Industrial Democracy" 6706 *Report Command Paper*

Carleton "Somebody's Watching, Worker Beware, as Companies Crack Down on E-Mail Abuses" *The Capital Times* (1999-4-9)

Cavanagh "Workplace Privacy: in an Era of New Technologies" *Cavanagh Associates Inc*

Cohen "Thought Cop" *InfoWorld* (2001-2-23)

Fader "Want Some Privacy? Stay at Home" *Chicago Tribune* (1998-5-28) 1-3

Ford "Surveillance and Privacy at work" 1998 *London: Institute of Employment Rights* 50

Frezza "The CALEA Time Bomb is Still Ticking" *Network Computing* (1997-7-10)

Jackson "Survey: Legal Liability of Web Access a Top Concern" *Computer News* (1999-1-11)

Johnson "Technological Surveillance in the Workplace" 1995 *Farfield and Woods*

Kokmen "Firms E-mail Computer Policies, Employees' Personal Use a Concern" *Denver Post* (1999-3-22)

Kopp "Electronic Communications in the Workplace: E-mail Monitoring and the Right of Privacy" 1998 *Seton Hall Constitutional Law Journal* 1-30

Lagan & Davies "New Digital Phones On-line Despite Objections" *The Sydney Morning Herald* (1998-4-28)

Lewis "American Workers Beware: Big Brother is Watching" *USA Today* (2000-2-19)

McCullagh "Wiretapping Internet Phone Lines" *Wired News* (1998-11-10)

Nicholson "Oops Wrong E-Mail Address List. A Dirty Joke Goes Global" *Philadelphia Inquirer* (1999-5-8)

Oliver "Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out" 2002 *Industrial Law Journal* 336

"Over 24 Percent of Employee Time is Non-Work Related" *Business Week* (1998-8-11)

"Sanlam Fires One of the E-mail Hoax Brothers" *The Herald* (2001-9-28)

Smith "Managing Privacy: Information Technology and Corporate America" 1994 *Chapel Hill: The University of North Carolina Press* 176-177

Sullivan "U.S. Lawmakers Introduce Workplace Privacy Measure" *Reuters* (2000-7-21)

Vaught, Taylor & Vaught "The Attitudes of Managers Regarding the Electronic Monitoring of Employee Behavior: Procedural and Ethical Considerations" 2000 *American Business Review* 107-114

Wiehahn Report RP 47/1979

York "Invasion of Privacy? E-mail Monitoring is on the Rise" *InformationWeek* (1999-2-21) 142-146

Table of cases

- A Mauchle (Pty) Ltd t/a Precision Tools v NUMSA* 1995 ILJ 349 (LAC)
- Almeida-Sanchez v United States* 1973 413 US 266 273
- Bernstein and others v Bester & others NNO* 1996 2 SA 751 (CC)
- Bernstein v Bester* 1996 4 BCLR 449 (CC) 484D 491G–H
- Botes v Van Deventer* 1966 3 SA 182 (A)
- Boucher v Du Toit* 1978 3 SA 965 (O)
- Bourke v Nissan Motor Corp in USA* 1993 No B068705
- Briggs v American Air Filter Co* 1980 US 630 F 2d 414
- Carephone (Pty) Ltd v Marcus* 1998 10 BCLR 1326 (LAC)
- Case v Minister of Safety and Security* 1996 3 SA 617 (CC)
- Colonial Mutual Life Assurance Society Ltd v Macdonald* 1931 AD 412 433
- Council for Scientific & Industrial Research v Fijen* 1996 ILJ 18 (A)
- Cronje v Toyota Holdings* 2001 3 BALR 213 (CCMA)
- D v K* 1997 2 BCLR 209 (N)
- Davies v Clean Deale CC* 1992 ILJ 1230 (IC)
- De Beer v Thomson & Son* 1918 TPD 70
- Deal v Spears* 1992 US 980 F 2d 1153
- Diablo Trade 28 (Pty) Ltd v Madiba Air (Pty) Ltd* 1999 3 All SA 305 (W)
- Estate of Van der Byl v Swanepoel* 1927 AD 141
- Fedics Group v Matus* 1997 9 BCLR 1199 (C)
- Feldman (Pty) Ltd v Mall* 1945 AD 733
- Fijen v Council for Scientific & Industrial Research* 1994 ILJ 759 (LAC)
- Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 2 SA 451 (A)
- FPS Ltd v Trident Construction (Pty) Ltd* 1989 3 SA 537 (A)

- George v Liberty Life Association of Africa Ltd* 1996 8 BLLR 985 (IC)
- Godfrey v Demon Internet Limited QBD* 1999 4 All ER 342 2000 3 WLR 1020 2001 QB 201
- Griswold v Connecticut* 1965 381 US 479 85 1678
- Halford v United Kingdom* 1997 73/1996/692/884
- Hall v Cognos Ltd* 1998-2-17 Case no 1803325/97
- Info DB Computers v Newby* 1996 ILJ 32 (W)
- Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 1 SA 545 (CC)
- Jacqueline Bamford and Four Others v Energizer (SA) Limited* (CCMA) 2001-6-22
- James v Newspaper Agency Corp* 1979 US 591 F 2d 579
- Jefferies v President Steyn Mine* 1994 ILJ 1425 (IC)
- Jeffrey v Persetel (Pty) Ltd* 1996 ILJ 388 (IC)
- Johnson v Beckett* 1992 1 SA 762 (A)
- Katz v United States* 1967 389 US 347
- Kopp v Switzerland European Court of Human Rights* 1998 13/1997/797/1000
- Lawrence v I Kuper & Co (Pty) Ltd t/a Kupers* 1994 ILJ 1140 (IC)
- Lebowa Platinum Mines Ltd v Hill* 1998 7 BLLR 666 (LAC)
- Liberty Life Association of Africa Ltd v Niselow* 1996 ILJ 673 (LAC)
- Lichaba v Shield Versekeringsmpy Bpk* 1977 4 SA 623 (O)
- Marshall v Vistech Communications (Pty) Ltd* 1994 ILJ 1365 (IC)
- Meerholz v Norman* 1916 TPD 332
- Mhlongo v Minister of Police* 1978 2 SA 551 (A)
- Minister of Police v Rabie* 1986 1 SA 117 (A)
- Mistry v Interim Medical and Dental Council of SA* 1998 4 SA 1127 (CC)
- Mkize v Martens* 1914 AD 382

- Moonian v Balmoral Hotel* 1925 NPD 215
- Moonsamy v The Mailhouse* 1999 20 ILJ 464 (CCMA)
- Morse v Future Reality Ltd* 1996-10-22 Case no 54571/95
- Mtambo v SA Clothing Industries Ltd* 1993 ILJ 983 (LAC)
- NAAWU v Borg Warner SA (Pty) Ltd* 1994 ILJ 509 (A)
- National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 1 SA 6 (CC)
- National Media Ltd v Jooste* 1996 3 SA 262 (A) 271
- NUM v East Rand Gold & Uranium Co Ltd* 1991 ILJ 1221 (A)
- O'Connor v Ortega* 1987 107 US 1492
- Oliver v United States* 1984 466 US 170
- Olmstead v United States* 1928 277 US 438 475-476 478
- Potchefstroom Municipal Council v Bouwer* 1958 4 SA 382 (T)
- President of the RSA v Hugo* 1997 6 BCLR 708 (CC)
- Protea Technology Ltd v Wainer* 1997 9 BCLR 1225 (W)
- PSASA v Minister of Justice* 1997 ILJ 241 (T)
- R v AMCA Services Ltd* 1959 4 SA 207 (A) 212
- R v Feun* 1954 1 SA 58 (T)
- S v A* 1971 2 SA 293 (T)
- S v Bailey* 1981 4 SA 187 (N)
- S v Bhulwana* 1995 1 SA 509 (C)
- S v Kidson* 1999 1 SACR 338 (W)
- S v Gwadiso* 1995 12 BCLR 1579 (CC)
- S v Lyons Brooke Bond (Pty) Ltd* 1981 4 SA 445 (ZA)
- S v Makwanyane* 1995 6 BCLR 665 (CC)

S v Naidoo 1998 1 BCLR 46 (D)

SA Associated Newspapers Ltd v Estate Pelser 1975 4 SA 797 (A) 810

SA Defence Union v Minister of Defence 1999 ILJ 299 (T)

Sasverbijl Beleggings & Verdiskonterings Mpy Bpk v Van Rhynsdorp Town Council
1979 2 SA 771 (W)

Secretary for Inland Revenue v Somers Vine 1968 2 SA 138 (A)

Silverman v United States 1961 US 365 505 511

Simmons v Southwestern Bell Telephone Co 1979 US 611 F 2d 342

Smit v Workmen's Compensation Commissioner 1979 1 SA 51 (A) 60-61

Smyth v Pillsbury Co 1996 US

Steve Jackson Games v US Secret Service 1994 US 36 F 3d 457

Strachan v Prinsloo 1925 TPD 709

Sun Packagings (Pty) Ltd v Vreulink 1996 ILJ 633 (A)

TAWU v Natal Co-operative Timber Ltd 1992 ILJ 1154 (D)

Toerien v Stellenbosch University 1996 ILJ 56 (C)

Travis v Alcon Laboratories Inc 1988 US 202 369 504 2d 419

United States v Harpel 1974 US 493 F 2d 346

United States v Mancini 1993 US 8 F 3d 104 109

Valasek v Consolidated Frame Cotton Corporation Ltd 1983 ILJ 277 (N)

Visagie v Prestige Skoonmaakdienste (Edms) Bpk 1995 ILJ 421 (IC)

Waring v Mervis 1969 4 SA 542 (W) 546

Watkins v L.M. Berry & Co 1983 US 704 F 2d 577

Whitehead v Woolworths (Pty) Ltd 1999 ILJ 2133 (LC)

Table of legislation and treaties

Americans with Disabilities Act (ADA) of 1990

Basic Conditions of Employment Act 75 of 1997

Civil Rights Act of 1964

Companies Act 61 of 1973

Constitution of the Republic of South Africa (Interim Constitution) 200 of 1993

Constitution of the Republic of South Africa 108 of 1996

Constitution of the United States - The U.S. Constitution was written at a convention held during 1787. Signed by 39 of the 55 state delegates, it was submitted for ratification in September of that year. The constitution took effect following its ratification by the ninth state in 1788.

Criminal Procedure Act 51 of 1977

EC Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications (96/C 329/01)

Electronic Communications and Transactions Act 25 of 2002

Electronic Communications Privacy Act of 1986

Employment Equity Act 55 of 1998

European Community Council Directive 94/45/EC of 22 Sep 1994 (institution of a European Workers Council)

European Convention on Human Rights - proclaimed by the General Assembly of the United Nations on 10 December 1948

European Union Directive 95/46/EC

Fire Brigade Services Act 99 of 1987

Freedom of Information Act 2000

Human Rights Act 1998

Income Tax Act 58 of 1962

Insolvency Act 24 of 1936

Interception and Monitoring Prohibition Act 127 of 1992

Internal Security Act 74 of 1982

International Covenant on Civil and Political Rights - G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force Mar. 23, 1976.

Labour Relations Act 66 of 1995

Magistrates Act 90 of 1993

National Labour Relations Act (NLRA), 29 USC §§ 151–169

Obscene Publications Act 1959

Occupational Health and Safety Act 85 of 1993

Post Office Act 44 of 1958

Private Security Industry Regulation Act 56 of 2001

Professional Land Surveyors' and Technical Surveyors' Act 40 of 1984

Promotion of Access to Information Act 2 of 2000

Protection of Children Act 1978

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

Skills Development Act 97 of 1998

Skills Development Levies Act 9 of 1999

The Data Protection Act 1998

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 SI 2000/2699

The Telecommunications Act 103 of 1996

Title 18 of the United States Code (as amended by the Electronic Communications Privacy Act of 1986)

Town and Regional Planners Act 19 of 1984

Unemployment Insurance Act 63 of 2001

United States Privacy Act of 1974

Universal Declaration on Human Rights - Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948

Online sources

<http://news.zdnet.co.uk/story/0,,s2073980,00.html>

<http://www.aclu.org/>

<http://www.aclu.org/about/aboutmain.cfm>

<http://www.anc.org.za/anc/newsbrief/2001/news0918.txt>

<http://www.dictionary.com>

<http://www.ema.org/html/pubs/mmv2n3/workpriv.htm>

<http://www.eherald.co.za/herald/2001/09/28/news/e-mail.htm>

<http://www.freelaunch.com/essays/liberty.html>

<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

http://www.hrcr.org/docs/Eur_Convention/euroconv2.html

<http://www.hri.org/docs/ECHR50.html>

<http://www.hrweb.org/legal/cpr.html>

<http://www.ietf.org/>

<http://www.informationcommissioner.gov.uk>

<http://www.iproof.biz/legalInfo.asp>

<http://www.law.cornell.edu/constitution/constitution.overview.html>

<http://www.legislation.hmso.gov.uk/acts/acts2000/20000023.htm>

<http://www.legislation.hmso.gov.uk/si/si2000/20002699.htm>

<http://www.matisse.net/files/glossary.html>

<http://www.networkcomputing.com/813/813colfrezza.html>

<http://www.nua.ie/surveys>

<http://www.socitm.gov.uk>

<http://www.spam.com>

<http://www.un.org/Overview/rights.html>

<http://www.usdoj.gov/criminal/cybercrime/18usc2510.htm>

<http://www.usdoj.gov/criminal/cybercrime/usc2701.htm>

<http://www.websense.com/company/news/pr/02/emea/131102b-uk.cfm>

ooOoo