UNIVERSITY OF KWAZULU- NATAL

THE ELECTRONIC MONITORING OF EMPLOYEES IN THE WORKPLACE

DARREN CAVELL SUBRAMANIEN

Masters in Law

University of KwaZulu-Natal, Pietermaritzburg

2009

CONTENTS

PART 4

PART 5

PART 6

INTRODUCTION

The use of new information and communication technologies in the workplace, including the increasing amount of work completed online, whether on the Internet or intranet have revolutionized the way business is conducted.

The use of these new communicating technologies in the workplace provides:

a) a cost effective way of communicating;
b) an expeditious means of communication;
c) the possibility to conduct business at remote places without the interruption of telephones;
d) the user with a comprehensive source or research material.

But there is a negative side to the use of these modern communication tools in the workplace. Apart from the problems raised by computer abuse, the rising employee liability for the abuse of electronic communication facilities, especially the abuse of the Internet is a cause of great concern for the employer. As a result employers may choose to increase the level of the monitoring of electronic communication in the workplace.

The principal focus of this work is the law that governs and regulates the monitoring of employees in terms of South African law.

This works commences by examining the right to privacy in the employment context in relation to South African, American, German, Italian and French law. The key question is how do employers balance the economic interest of their businesses without infringing on the employees' right to privacy. If the employers do have a legitimate interest in intruding upon an employee's privacy, it needs to be determined when this can occur.

Thereafter, the focus shifts to the legislation in South African law that regulates the interception and monitoring of employees in the workplace.

The abuse of these electronic communication tools by employees pose serious problems for employers. These problems may arise where employees defame, sexually harass and discriminate others using the employer's electronic communication system. These issues will be examined in greater detail.

As the threat of employer liability has increased, employers seek more advanced methods of monitoring and surveillance of employees. This often entails the purchase and adoption of new software and hardware. This work provides a discussion of some these new technologies that are currently available and those that will be available in the near future.

In order for the dismissal by an employer to be fair, an employer must have obtained substantive evidence against the employee. The evidence of abuse of the electronic equipment in the workplace by employees is normally obtained by the employer resorting to electronic monitoring devices, such as, monitoring software, telephone tapping and video recordings. There are instances however where the employer may have a legitimate reason or reasons to monitor the activities of their employees in the workplace but the information obtained or the method used cannot result in employee liability. These situations will be examined.

This work will evaluate permissive employer policy with regards to monitoring electronic communications in the workplace, and will assess how effective this is, as a means of controlling and monitoring the activities of employees, thus curbing improper electronic communication in the workplace, while at the same time respecting the employee's right to privacy.

CHAPTER 1

Workplace Privacy in relation to Electronic Communications in the Workplace

The right to privacy has been often described as 'the right to be left alone'[1], 'the right to live one's life with the minimum degree of interference'[2] and the right to decide 'when and under what conditions private facts may be made public'. The right to privacy entails the right to be free from intrusions and interference by the state and others in one's personal life as well as unauthorized disclosures of information about one's private life.[3] Privacy is a valuable and an advanced aspect of personality. Sociologists and psychologists around the world agree that a person has a fundamental need for privacy. An individual therefore has an interest in the protection of his or her privacy.[4]

Jayne Ressler describes privacy, more specifically information privacy as, "the claim of individuals, groups or institutions to determine for themselves when and how, and to what extent information about them is communicated to others", another reasoned that such privacy "is the control over knowledge about oneself".[5] But it is not simply control over the quantity of information abroad; there are modulations in the quality of the knowledge as well. We may not mind that a person knows a general fact about us, and yet feel our privacy invaded if he knows the details".[6] In the case of *Investigating Directorate: Serious Economic Offences and Others v Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001

---

[1] Brandeis J, dissenting in *Olmstead v United States* 277 US 438 478, 48 S Ct 564 (1928).

[2] International Commission of Jurists *Conclusions of the Nordic Conference on the Right to Privacy* (1976) 2 et seq.

[3] D McQuoid -Mason "Invasion of privacy: common law v constitutional law delict: does it make a difference?". (2000) *Acta juridica* 227 [see generally J Neethling, "The concept of privacy in South African law: notes". (2005) 122 (1) *SALJ* 18-28].

[4] *South African Law Commission*. *Privacy and Data Protection*. (2005). 15

[5] J S. Ressler. "Privacy, Plaintiffs, and Pseudonyms: The Anonymous Doe Plaintiff in the Information Age" (2004) 53. (1) *The University of Kansas Law Review*. 202, [quoted in D J. Solove & M Rotenberg, Information Privacy Law (3ed) (2003)].

[6] Ibid

(1) SA 545 (CC), the court held that the right to privacy guaranteed in s 14 of the Constitution does not relate solely to the individual within his or her intimate space but includes instances when persons move beyond this established 'intimate core'; in these instances individuals still retain a right to privacy in the social capacities in which they act.[7] Thus, when people are in their offices, in their cars or on mobile telephones, they still retain a right to be left alone by the State unless certain conditions are satisfied. From the above we can conclude that the right to privacy would come into question wherever a person has the ability to decide what he or she wishes to disclose to the public provided of course, that expectation of privacy was reasonable.[8]

The concerns around a person's privacy are not a new social phenomenon. Louis Brandeis and Samuel Warren's unease at the turn of the century regarding loss of privacy was prompted by the technological and media developments of their time.[9] First, the development of a new form of sensationalist journalism, known as yellow journalism, made newspapers wildly successful and led to dramatically increased circulation.[10] Second, technological developments, specifically photography, caused "great alarm for privacy". The Internet and related technological advancements may very well constitute the yellow journalism of the new millennium.[11]

The courts have held that certain intrusions into a person's private life or affairs, or aspects of his or her 'inner sanctum' to be warranted.[12] These have included a raid on a brothel; the persistent shadowing of a person; watching a person undress or bath; 'bugging' or entering a person's room, reading of private documents or correspondence; listening to private telephone conversations; improperly interrogating a detainee; and taking unauthorized blood tests.[13] Most of these

[7] *Investigating Directorate: Serious Economic Offences and Others v Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001 (1) SA 545 (CC), para [16] at 557A/B - C.

[8] supra note 7

[9] Ressler op cit note 5, 196

[10] Ressler op cit note 5, 196

[11] Ressler op cit note 5, 196

[12] *National Media Ltd and Another v Jooste* 1996 (3) SA 262 (A), at 271

[13] supra note 12

intrusions involve individuals becoming acquainted with private information about others without their consent.[14]

The right to privacy allows an individual to determine the destiny of private facts. The individual concerned is entitled to dictate or determine the ambit of disclosure, the disclosure may have been made for example to a circle of friends, a professional adviser or to the public at large.[15] He or she may prescribe the purpose and method of the disclosure. Similarly, a person is entitled to decide when and under what conditions private facts may be made public.[16]

A common law right to privacy under the *actio injuriarum* has existed for many years;
"But injuria is committed not only when someone is beaten , say, with fists or clubs or even if he flogged but also if a clamour be raised against him or his property be possessed as though he were a debtor, by one who knows him not to be in debt; or if, to bring another into disrepute, a person write, compose, publish a libel, or , by his deliberate act, ensure that any of these things be done; or again if one fellow a matron or one under seventeen, whether male or female, or there be a person whose chastity is said to be impugned; and, in short, it is plain that injuria might be committed in great variety of ways".[17]

According to the common law, infringements of private communications have long been regarded as wrongful.[18] The courts have found in the past that it was unreasonable for private detectives in matrimonial disputes to use eavesdropping devices and electronic surveillance equipment. The use of such was deemed an unlawful invasion of privacy by the courts. [19] Likewise the stealing of tape recordings of confidential business meetings and offering them to a third party has been held to be

---

[14] supra note 12

[15] supra note 7, at 271G-272B

[16] supra note 7, at 271G-272B

[17] Institutes of Justinian 4.4.1 [AD 533]

[18] McQuoid -Mason op cit note 3 , 252

[19] Ibid

unlawful invasion of privacy.[20] The Canadian courts have held that a reasonable expectation of privacy is violated when a telephone conversation is intercepted by a third party without the knowledge or consent of the participants.[21] Our courts have suggested that the mere fact that parties using a telephone are aware that they must be careful when talking to one another cannot be regarded as consent to the violation, or waiver of their expectation to privacy.[22]

Section 14 (d) of the Constitution of the Republic of South Africa Act 108 of 1996 provides that: *everyone has the right to privacy, as well as protection against certain specific infringements of privacy, viz: searches, seizures, which includes the right not to have the privacy of their communications infringed.*

It must be remembered however that no right is absolute. This right would involve the balancing of competing rights such as those of the common law and the employer to preserve their property and society's interest in eradicating unlawful conduct.[23]

Section 14 of the Constitution[24]must be read together with s 32 of the Constitution, that is, the section on Access to information. In terms of s 32:

(1) Everyone has the right of access to -

a. any information held by the state ; and
b. any information that is held by another person and that is required for the exercise or protection of any rights.

(2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.

It can be seen however that neither of these sections deals directly with the problems of the information age. Section 14 sets out to guard against improper and unlawful infringements to the

[20] McQuoid -Mason op cit note 3 , 253

[21] Ibid

[22] *S v Naidoo* 1998 (1) SACR 479 (N) at 89.

[23] C Mischke "Workplace Privacy, e- mail interception and the law". (2003). 12 (8) *CLL 78*

[24] The Constitution of the Republic of South Africa Act 108 of 1996

right of privacy. Section 32 enables access to information that a person needs to protect or exercise his or rights.[25] These sections fail to establish a general right of access to information. An individual is not entitled to demand access to information that a person may have against another individual. The right of access to information exists only when the individual is seeking to exercise or protect some other recognized right.[26]

It has been argued that, whether or not consent or notification measures are in place, employers should always legitimize the need to invade an employee's privacy[27] with reference to s 36(1) of the Constitution: 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, including:[28]

(a) the nature of the right;
(b) the importance of the purpose of the limitation;
(c) the nature and extent of the limitation;
(d) the relation between the limitation and its purpose
(e) less restrictive means to achieve the purpose.[29]

Despite the fact that an individual's 'will to preserve privacy' ('privaathoudingswil') is clearly an important component of his right to privacy, it is also evident that the limits of the individual's right to privacy are not determined exclusively by the will of the person concerned.[30] The ambit of the right to privacy is, as in the case of any other subjective right, in the final instance determined

[25] R LE Roux "Aspects of South African law as it applies to corruption in the workplace". (2004) 17 (2) *SACJ* 174.

[26] J Hofman …et al. *Cyberlaw: A Guide for South Africans Doing Business Online.* (1999) 51

[27] LE Roux op cit note 25, 174 – 175

[28] Ibid

[29] Section 36 of the Constitution of the Republic of South Africa Act 108 of 1996, see also *Troker Bros (Pty) Ltd and Keyser* (2005) 26 ILJ 1366 (CCMA), at p 1373

[30] *National Media Ltd and another v Jooste* 1994 (2) SA 634 (C) at 645E, G and H-I.

by objective norms, and attempts to completely subjectify the test for the wrongfulness of acts which *prima facie* constitute an invasion of privacy are therefore not acceptable.[31] In certain cases employers may have a legitimate right to know the detailed and specific manner in which employees conduct themselves and it does not matter how the information was obtained. It is submitted by Mason[32], that, where the continuous monitoring of employees' communication goes too far, it should be regarded as unreasonable, and should be regarded as *prima facie* evidence of breach of the employees' constitutional right to privacy. Such employers should then be asked to justify their conduct in terms of s 36 of the Constitution.[33]

In the case of *Toker Bros (Pty) Ltd and Keyser* (2005) 26 ILJ 1366 (CCMA), the employer party referred a dispute to arbitration in terms of s 188A of the Labour Relations Act 66 of 1995, to determine whether the employee party should be dismissed for misconduct. The employee was charged with dishonesty in that she excessively misused the company computer for her personal use in working hours and without permission. She was further charged with misconduct in that in an e-mail sent from the company computer she had made defamatory remarks about her employer. The employer alleged that this had destroyed the employment relationship. The employee denied the dishonesty. She maintained that her employer was aware that she was accessing the Internet, and that her access was mainly work related. Her personal use related to a school reunion that she was organizing, and which her employer knew about. She admitted the defamatory statement, but maintained that it was contained in a private communication and that the manner in which the employer accessed her private e-mail was illegal and an invasion of her privacy. Only the issue with regard to the second charge is relevant here. On the second charge the commissioner noted that s 14 (d) of the Constitution 1996 protects an employee's right to privacy and that an employer is prohibited from intercepting, monitoring or otherwise acquiring any private communication of an employee, except where consent has been given or a clear policy on monitoring and intercepting of private communication is in force at the workplace. Section 35(5) of the Constitution further provides that evidence obtained in a manner that violates any right in the Bill

[31] supra note 30, at 645E, G and H-I.

[32] McQuoid -Mason op cit note 3

[33] McQuoid - Mason op cite note 3, 253

of Rights must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice. The commissioner took into account the possibility that the employer could be held vicariously liable for the content of e-mails sent via its system, and also the highly offensive and insensitive nature of the particular e-mail message complained of.[34] The commissioner concluded that it was undisputed that the applicant in this matter came across the personal e-mails in its investigation into the respondent's abuse of the Internet facility. The commissioner held that it could be accepted that the breach of privacy was incidental and that the applicant's discovery of the e-mails was not maliciously intended. Although the respondent argued that she could continue working for the company the commissioner found the he could not envisage how this was possible after her own indication to her friend that she had no regard for her employer especially after the applicant had seen the content of the e- mail. The commissioner held that the employment relationship was certainly damaged as the e- mail with the defaming content had utterly shocked the owner of the business and insulted his dignity as he was Jewish and any reference to the holocaust in the e- mail was deemed to be exceptionally sensitive.[35] In an employment relationship trust is paramount to the harmonious and operational existence of the relationship. The commissioner held that on both charges the trust relationship between employer and employee had been seriously challenged and that subsequently dismissal was thus justified.[36]

If the plaintiff establishes that his or her right to privacy has been impaired the defendant's conduct may not be wrongful if the latter can show that the invasion of privacy was reasonable and justifiable in terms of s 36 (1).[37]

The constitutional safeguard of privacy by its nature protects a wide range of overlapping and inter-related rights. This is particularly true of the workplace where employees share offices and where computers, the Internet, and telephones are used as means of communication to perform

[34] *Toker Bros (Pty) Ltd and Keyser* (2005) 26 ILJ 1366 (CCMA), at p 1374

[35] supra note 34 , at 1369 F-G

[36] supra note 34, at 1375

[37] McQuoid - Mason op cit note 3 , 254

activities of varying nature in the employer's interest, but often also in an employee's private interest.[38] In the international context, it has been stated that personal privacy in the workplace is directly related to one of the basic principles of the concept 'quality of working life' — an individual employee is a whole human being and should be treated as such.[39] In cases where evidence was obtained (illegally) by invading the individual's privacy, the courts and The Commission for Conciliation Mediation and Arbitration (the CCMA) have balanced the employer's right to economic activity with the employee's right to privacy in accordance with the limitation clause s 36 of the Constitution.[40]

It is generally accepted that 'a law of general application' includes the common law. In this instance it is the common law right of the employer to protect its property and business interests that may potentially limit the employee's right to privacy.[41] The weight of factors listed in s 36(1) can only be determined with reference to the facts of the particular case. The following factors may guide a presiding officer:[42]

A) This will be determined by the operational realities of the workplace. This would also include the efforts made by the employer to notify the employees by means of notices of possible invasions as well as clear policies regarding private activities in the workplace. The employer must take steps to regularly warn employees of the terms of the contract and polices regarding monitoring.
B) The right to privacy enjoys specific protection in the Constitution. The right to economic activity enjoyed protection under the interim Constitution but not under the final Constitution. In the case of *Moonsamy v Mailhouse* 1999 (20) ILJ 464 (CCMA), Commissioner Van Dokkum believed this signaled a clear indication that the right to privacy of the employee are preferred to the employer's right to economic activity. This has been submitted to indicate that the employer must provide evidence that his business has been seriously threatened in order to

[38] LE Roux op cit note 25 , 174 -175

[39] Ibid

[40] Ibid

[41] Ibid

[42] Ibid

condone any serious invasion of employee privacy. [43]

C) An important consideration is the extent to which similar evidence can be secured by conventional means. If these conventional means cannot be used, the onus is on the employee to show that prior notification was given and that the consent of the employee was present, provided that the employee had a clear understanding of what he had consented to.[44]

In order to determine the extent to which an employee's privacy may be undermined by electronic monitoring by the employer, is to consider why privacy is important. Privacy according to Hazel Oliver[45] can be divided into two broad categories, - those relating to autonomy and democracy, and those relating to dignity and personal well - being.[46] Personal autonomy relates to the ability of individuals to choose freely how to live their lives and is thought of as particularly valuable in democratic societies.[47] Autonomy is threatened by invasions of privacy because individuals are thereby deprived of the opportunity to explore different options free from external observation and social pressures, thus allowing individuals to develop and explore different ideas before releasing their thoughts to others.[48] An individuals autonomy can also be affected by invasions of privacy even where those individuals do not know for sure whether or not it is occurring. The suspicion alone that one is subject to surveillance while at work may have a detrimental effect on the exercise of rights.[49] As far as the impact that privacy has on an individual's emotional well being, Oliver submits, that private time and space gives individuals the opportunity for emotional release, which is important for physical and psychological well being of employees, and provides scope for limited and protected personal communication.[50] This view has been supported by the

[43] *Moonsamy v Mailhouse* 1999 (20) ILJ 464 (CCMA) at 471G-H

[44] LE Roux op cit note 25 , 175-176

[45] H Oliver "E- mail and Internet Monitoring in the Workplace: Information Privacy and Contracting - Out". (2002) (31) *ILJ* 321

[46] Ibid 322 - 323

[47] Ibid 323

[48] Ibid

[49] Ibid 322

[50] Ibid 323

International Labour Office, which has specifically noted that the use of monitoring and surveillance as a management technique has serious negative consequences for working conditions and worker health.[51]

The protection of the privacy of employees in the workplace can be seen to promote the voluntary sharing of private information amongst employees, which enhances the fundamental relationships in the workplace and helps the employees define themselves.[52]

In the Canadian case of *R v Dyment*[53], La Frost J described three zones of privacy which may require protection - 'those involving territorial or spartial aspects, those related to the person, and those that arise in the information context'.[54]

Information privacy relates to the preservation of the confidentiality of information about individuals, and it is this type of privacy that is most relevant to the issue of e- mail and Internet monitoring.[55] Electronic surveillance of employees is potentially a threat to employee privacy largely because of the likelihood that the employer will obtain private information about employees - whether directly because this is the purpose of monitoring, or indirectly as a result of surveillance for other purposes.[56] If the focus is on information privacy , then perhaps Alan Westin's definition of privacy as 'the claim of individuals , groups or institutions to define themselves and when, how and to what extent information about them is communicated to others', is the most appropriate in the context of e- mail and Internet monitoring in the workplace.[57] The definition above summarises and describes the main concerns about such practices - namely the fact that employees may thereby be denied the opportunity to define when, how and to what extent

---

[51] International Labour Office, "Monitoring and Surveillance in the Workplace". (1993), Vol 12, Part 1, *Conditions of Work Digest* at 11.

[52] Oliver op cit note 45, 322

[53] *R v Dyment* 1988 2 SCR 417

[54] supra note 32, at 428

[55] Oliver op cit note 45, 322

[56] Oliver op cit note 45, 322

[57] Oliver op cit note 45, 322

personal information about them is communicated to their employer.[58]

The scope of a person's right to privacy extends only to aspects of his or her life or conduct in regard to which a legitimate expectation of privacy can be sought.[59] The subjective component of the test recognizes that a person cannot complain about an invasion of privacy if he or she has explicitly or implicitly consented to the invasion.[60] The objective component is more important, but it is often quite difficult to assess due to the kinds of privacy expectation that society would regard as objectively reasonable.[61] An individual's subjective expectation of privacy in respect of these three concerns will usually be regarded as objectively reasonable.

In the first instance, the right to privacy seeks to protect certain aspects of a person's life in respect of which every person is entitled to be left alone, this includes a person's body, certain places, and certain relationships. Secondly, the right to privacy aims to protect the opportunities for an individual to develop his or her personality, and so extends to certain forms of individual and personal self-realization or fulfillment. Thirdly, the right to privacy seeks to protect the ability of individuals to control the use of private information about themselves.[62] It is clear that all three these concerns are to some extent applicable to the employee in the workplace.

The requirement that the employee have a 'legitimate expectation' that her privacy will be respected indicates that one must have a subjective expectation of privacy. But, at the same time, society must recognize this as objectively reasonable.[63]

Initially, the courts argued about the parameters of the right to privacy in the workplace, usually in the context of telephone calls. The South African Constitutional Court in the case of Bernstein *v*

[58] Oliver op cit note 45, 322

[59] See the case of *Mistry v Interim Medical and Dental Council of South Africa and Others* 1998 (4) SA 1127 (CC) where the court held that "the scope of a person's privacy extends only to those aspects to which a legitimate expectation of privacy can be harboured".

[60] A Dekker. "Vices or Devices: Employee Monitoring in the workplace." (2004) 16 *SA Merc LJ* 624

[61] Ibid 624-625

[62] Ibid 624

[63] Ibid 625

Bester 1996 (4) BCLR 449 (CC) provided some clarity. In this case Ackerman J emphasized that, "while privacy is acknowledged in respect of a person's inner sanctum (such as family life, sexual preference and home environment), protection erodes as he or she moves into communal relations and activities such as business and social interaction".[64]

There is great concern that in addition to the invasion of employee privacy, the monitoring of electronic communications of employees may in result in the following problems: [65]

1. Lack of trust among workers, supervisors, and management. Employee monitoring may and has the potential to undermine workplace morale and create distrust and suspicion between employees and their supervisors or management. It is no co- incidence that as employee morale declines, so does the production levels.[66]
2. The potential increase in stress levels. Due to the increased monitoring of their behaviour, employees may experience high levels of stress and anxiety in the workplace.[67]
3. Repetitive strain injuries (RSI). RSI is a set of work related muscular skeletal disorders caused by repeated and prolonged body movement resulting in damage to the fibrous and soft body tissues like tendons, nerves, and muscles. RSI is the consequence of a demand on a person to perform a task that exceeds the person's working capacity. This may occur when employees who need to take needed breaks fail to do so. The failure to take breaks arises due to the fear of

[64] *Bernstein v Bester* 1996 (4) BCLR 449 (CC) at 792 G-I, 793 E, and 795D , - **"**The truism that no right is to be considered absolute implies that, from the outset of interpretation, each right is always already limited by every other right accruing to another citizen. In the context of privacy, this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community. This implies that community rights and the rights of fellow members place a corresponding obligation on a citizen, thereby shaping the abstract notion of individualism towards identifying a concrete member of civil society. Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly". [see also the case of *Magajane v Chairperson North West Gambling Board and others* (2006) 5 SA 250 (CC) at, 50 A-G]

[65] J M Kizza & J Ssanyu "Electronic Surveillance". In *Electronic Monitoring in the Workplace: Controversies and Solutions.* J Weckert. 12- 14

[66] Ibid

[67] Ibid

being considered lazy by their employers.[68]

4. Lack of individual creativity. Most highly monitored jobs do not require personal creativity. The employee usually is not allowed to vary the procedures, but must follow them to the letter. Employees also have a fear of exercising creativity that is outside normal procedures because they fear being questioned or even losing their jobs in the event of anything going wrong.
5. Reduced or no peer or social support. Highly monitored employees are usually given separate stations where specific equipment can monitor them in full view. An employee is thus forced to be where he or she can be seen.[69]
6. Lack of self esteem. The isolation, and daily routine of work coupled with a lack of freedom to vary employee activities lowers employee morale and consequently self esteem. This lack of self esteem amongst employees emanates from the belief that they are lazy or incompetent and thus need to be highly monitored in the workplace.[70]
7. Employee alienation. Alienation is higher among employees in industries and companies with automated monitoring technologies. This is due to the fact that high levels of automated monitoring are associated with lack of worker freedom, control, purpose, function, and self involvement in employee's work.[71]
8. Lack of communication. It is well established that information technology does affect communication. When information technology is used for surveillance it can further affect communication by reducing or eliminating the need for individual workers to be involved in communication. Employees who find themselves in this situation become objects of information collection without participating in the process of exchanging information.[72]
9. Psychological. The mere presence of electronic monitoring in a workplace may give rise to the perception among employees that their movements are being watched, even if that is not the case. This may ultimately lead to adverse psychological effects on an employee.[73]

---

[68] Ibid

[69] Ibid

[70] Ibid

[71] Ibid

[72] Ibid

[73] Weckert op cit note 65, 13-14

In terms of s 36 of the Constitution Act 108 of 1996 (the limitation clause), the infringement of the right to privacy can sometimes be justifiable in the context of the employment relationship. To determine justifiability, it is necessary to balance the competing interests of the employer (the right to economic activity) and the employee (the right to privacy).[74]

The need to engage in a balancing of interests was discussed in the case of *Goosen v Caroline's Frozen Yoghurt Parlour* (1995) 16 ILJ 396 (IC) at 400C. The employee in this case recorded telephone conversations between the chairman of the disciplinary enquiry and the employer in order to prove bias on the part of the chairman. The permissible limitation on the employee's constitutional right that was applicable here was that of the interim Constitution. In terms of the limitation clause in the interim Constitution, the right to privacy could be restricted if it was reasonable and justifiable, and if the restriction did not negate the essential content of the right. The limitation clause provided certain levels of scrutiny, in terms of which stronger protection was given to certain rights, which required that it be proved that the infringement of those rights would also be necessary. The right to privacy did not fall within that category, and so the restriction of the right to privacy had only to be shown to be reasonable and justifiable. To determine the meaning of 'reasonable', the court looked at the Canadian Charter for Human Rights. According to the Canadian courts, it should first be determined if there had been an infringement of a fundamental right. If so, the inquiry had to determine whether the infringement was reasonable. According to the court an infringement would be reasonable if the "interest underlying the limitation is of sufficient importance to outweigh the constitutionally protected right and the means must be proportional to the objective of the limitation". The presiding officer held that the recordings were admissible.[75]

The case of *Protea Technology Ltd and another v Wainer and others* 1997 (9) BCLR 1225 (W), was decided in terms of the final Constitution. It concerned the interception of a telephone conversation by an employer. The court held that in this case that the scope of a person's privacy extends only to those aspects in regard to which a legitimate expectation of privacy can be harbored. Whether there is a legitimate expectation of privacy depends, the High Court held, on a

[74] Dekker op cit note 60, 625

[75] *Goosen v Caroline's Frozen Yoghurt Parlour* (1995) 16 ILJ 396 (IC) at 404D

'subjective expectation of privacy which society recognizes as objectively reasonable'.[76] The conversations taped were by the employee, conducted from the employer's business premises during business hours, and so did not enjoy Constitutional protection. Relying on the Bernstein decision the High Court held:

> *"Thus he may receive and make calls which have nothing to do with his employer's business. The employee making such calls has a legitimate expectation of privacy. Although he must account to his employer if so required for the time so spent, the employer cannot compel him to disclose the substance of such calls. The content of conversations involving his employer's affairs (whether directly or indirectly) is a different matter. The employer is entitled to demand and obtain from his employee as full an account as the latter is capable of furnishing. In this sense also, the company can fairly be regarded as the owner of the knowledge in the employee's mind".*[77]

In the case of *Moonsamy v The Mailhouse* (1999) 20 ILJ 464 (CCMA), the arbitrator considered what would be regarded as a justifiable infringement of the right to privacy in view of the Constitutional limitation clause. In question was whether the employer was entitled to use evidence which had been obtained by way of an interception, listening and recording device that was connected to the employee's office telephone. The evidence the employer obtained using the telephone tap was led at the disciplinary hearing against the employee. It was clear that the evidence was obtained in contravention of the Interception and Monitoring Prohibition Act of 127 of 1992 (IMP Act). The commissioner held that evidence obtained in breach of the IMP Act was not necessarily inadmissible and that admissibility or otherwise of such evidence would depend on the circumstances of the case.

The arbitrator held that the issue was one of balancing the competing interests of the employer and the employee, that is, the employer's the right to economic activity (in terms of the interim Constitution[78]) as against the employee's right to privacy. [79] It was held to be "extremely difficult

---

[76] *Protea Technology Ltd and another v Wainer and others* 1997 (9) BCLR 1225 (W), at 1226 F

[77] supra note 76, at 1240 D.

[78] Section 26 of the Constitution of the Republic of South Africa Act 200 of 1993.

[79] supra note 43

to clarify, at least with any degree of precision, the nature of the right to privacy of an employee on the premises of the employer during working hours".[80] The arbitrator structured his reasoning on five premises based on the factors set out in section 36 of the Constitution to be considered when fundamental rights are limited.

The first premiss concerned the nature of the right. The arbitrator relied on American case law[81] to the effect that a person is entitled to a 'reasonable expectation' of privacy. This expectation exists only when *(a)* the individual has a subjective expectation of privacy, and *(b)* where society recognized the expectation as reasonable. Within the context of the employment relationship, it is determined largely by the operational requirements of the workplace. In another American case,[82] the court held that the operational reality of the workplace may render some employee expectations of privacy unreasonable, but these might be found to be reasonable in other non-employment contexts. It was clear that office practices and procedures, and legitimate employer regulations, might reduce the employees' expectations of privacy in their offices, desks, and filing cabinets. Given the great variety of working environments, the question is whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.

The CCMA in *Moonsamy*[83] noted that the employer's conduct in the case before it went further than rummaging in an employee's desk or filing cabinet. A telephone interception with the express purpose of monitoring all the employee's conversations was in issue. Whilst one may argue that the telephone conversation took place on the employer's telephone (which indicated ownership), on the employer's premises, and was related to the employer's business, telephone conversations by their nature demand a higher degree of privacy than the employee's office desk. The court stated it could be argued that if a telephone call related to the employer's business, the employer was entitled to be privy to that conversation. But if the employer were allowed to make that initial decision regarding the nature of the call (personal versus business), the right to privacy would be meaningless. The right would then amount to having a tribunal decide, after the interception of the

[80] supra note 43, at 469H–I.

[81] *Katz v US* 389 US 347 (1967).

[82] *O'Connor v Ortega* 480 US 709 (1987).

[83] supra note 43.

call, that the call did not relate to the business of the employer and so was confidential. In a nutshell, the employee's right to privacy regarding work-related matters had to be qualified on the basis of the fiduciary relationship between employee and employer that entitled the employer to loyalty and honesty.[84] The employer argued that it considered its actions necessary for its financial self-preservation, as the employee conducted business that was damaging to the employer. At the same time, the employer's business necessity could legitimately impact on the employee's personal rights in a manner not possible outside the workplace. So there had to be a clear balancing of rights. The court held that section 22 of the Constitution emphasized the employee's personal right and was to be preferred to the more 'amorphous (and consequently controversial) right to economic activity'.[85]

The third premiss concerned the nature and extent of the limitation. Telephone calls were considered to be very private.[86] An employer might have the right to ask an employee to disclose the number of personal as opposed to business calls that he made during working hours. But the right to disclosure ended at this point, unless the employer could show, when it sought prior authorization, that there were compelling reasons within the context of business necessity for the content of those conversations to be disclosed.[87]

The fourth premiss related to the limitation and its purpose. The interception of the telephone calls was intended to provide evidence against the employee. The commissioner emphasized that there must have been other methods to accumulate evidence of wrongdoing. If an employer could show that telephone interception was the only method of securing evidence, in circumstances where the employee was clearly causing harm to the employer, then telephone tapping might be justified. In this instance the employer still had to seek prior authorization.[88]

The fifth premiss was that less restrictive means had to be used to achieve the purpose. If an

[84] supra note 64, at 470I–J.

[85] supra note 64, at 471 G-H

[86] supra note 64, at 471 I

[87] supra note 64, at 272A

[88] supra note 64, at 472 D

employer actually could have used other more conventional methods of obtaining incriminating evidence against an employee, it should have done so. Put differently, other less restrictive means had to be considered. If there were none, the employer had to seek prior authorization to tap the telephone. Prior consent could be obtained by way of employee consent as a condition of the employment contract, or by authorization by the Labour Court.[89]

The commissioner held that the right to privacy in the context of the employment relationship is unique and very difficult to clarify. At the same time, the commissioner did not accept the right to privacy as being unlimited and absolute and he took into account the relevant issues arising from the employment relationship:

> *"An employee stands in a fiduciary relationship to his employer and the employer is entitled to expect loyalty and honesty from the employee, especially during work hours. For this reason alone, and due to the exigencies of the workplace, it is clear that the employee's right to privacy , at least regarding work related matters , must be qualified".*[90]

The commissioner further held that the employer is contractually entitled to know the content of the employee's calls in so far as they relate to business. It is also in the financial preservation of the employer's business to determine if the employer is doing something to prejudice or cause damage to the employer's business.

> *"The rights that a citizen is entitled to in his or her personal life cannot simply disappear in his or her professional life as a result of the employer's business necessity. At the same time the employer's business necessity might legitimately impact on the employee's personal rights in a manner not possible outside the workplace. Therefore there is a clear balancing of rights".*[91]

Employers are increasingly adopting the practice of monitoring their employees' telephone conversations, e- mail and use of the Internet in the workplace. It has become all too easy for employers to carry out, in what in most instances can be seen as pervasive surveillance of

[89] Section 158 of the Labour Relations Act 66 of 1995

[90] supra note 64, at 470 I

employee activity by electronic means. The result is that such practices have potentially serious implications for employee privacy.

Privacy protects a number of values which are held to be very important by society, and this is as true of the workplace as elsewhere. If privacy is worth protecting, then its costs will often be worth bearing. It should be noted that in certain instances employers do have business reasons for electronic monitoring of employees in order to ensure that the employer's rights are not compromised.

[91] supra note 43, at 471G

CHAPTER 2

FOREIGN LAW

1. The United States of America

In the United States most if not all employers admit to having some form of employee monitoring. To find the reason and to understand why, one need only look at the statistics of Internet and e-mail misuse by employees and the potential liability for employers created thereby.

This topic continually brings about a huge uproar and debate concerning the privacy rights of employees, who often act under the assumption that the web sites they visit and the e-mail messages they send and receive are confidential.[92] It has become more and more difficult on a daily basis to distinguish between the conduct of employees that is seen to be of a private nature from the conduct that provides employers with legitimate grounds to monitor their employees. The reason for this is the development almost on a daily basis of technology and case law on this subject.[93]

Perhaps the best starting point is to first determine whether there is a need for employees to be monitored while at work in the United States of America (USA).

A two-year study was conducted by Alexa Research.[94] The results of this study was alarming. It showed that 'sex' was the most popular search term on the Internet. 'Porn' was the fourth most-searched term, followed by 'Nude,' 'XXX,' 'Playboy,' and 'Erotic Stories,' all of which

[92] L Court and C Warmington. "The Workplace Privacy Myth: Why Electronic Monitoring is here to Stay". (2004) *Oklahoma City University Law Review: Employment and Labor Law* 15. *Westlaw.* Accessed: 20 February 2007.

[93] Ibid

[94] The Centre for Online Addiction, at http://www.netaddiction.com/workplace. Accessed :23 February 2007

were in the top twenty most-searched list.[95] According to another study conducted by Websense Enterprise, an Internet management business, 70 percent of all Internet porn traffic occurs during the 9:00 a.m. to 5:00 p.m. workday.[96] The results of one survey showed that, more than 60 percent of companies report having disciplined employees, and more than 30 percent having terminated the employment of employees, for inappropriate use of the Internet.[97]

The misuse by employees made headlines when Dow Chemical Company fired fifty employees and suspended two hundred more for sending and storing pornographic and/or violent e-mail messages.[98] The New York Times, in December 1999, terminated over twenty employees for sending inappropriate and offensive e-mail messages.[99] According to The Wall Street Journal the employees of IBM, Apple Computer, and AT&T were among the most frequent visitors to Penthouse Magazine's website. It was estimated that these employees spend the equivalent of over 347 eight-hour days in a single month visiting pornographic websites. Internet misuse is not, of course, limited to the private sector.[100] A study by the Internal Revenue Service showed that many of its employees viewed sexually explicit websites. Internet misuse by employees was even uncovered at the Departments of Commerce and Housing and Urban Development and even former White House administrations. Due to the increase in the misuse of the internet some psychologists now specialise in helping persons overcome web addictions.[101]

The following are the most overwhelming arguments raised by employers in the United States in favour of electronic monitoring of employees in the workplace.

---

[95] Ibid

[96] Ibid

[97] Ibid

[98] Ibid

[99] Ibid

[100] Ibid

[101] Ibid

The first of these relates to issues that revolve around productivity. The argument is that even if employees are not viewing inappropriate or offensive websites at work, they are likely to be spending time looking at other non-work related sites.[102] According to a survey conducted by Vault.com, 25.1 percent of employees admitted to spending ten to thirty minutes a day surfing non-work-related sites, 11.9 percent admitted to spending one to two hours a day, and an astonishing 12.6 percent spent over two hours a day surfing non-work-related sites.[103]

Employees admit to using the Internet to read the news each day, book flights, buy shares, and to shop for gifts.[104] This was proved to be true by a survey conducted in November of 2000. According to respondents of the survey between a half day to two days per week is spent shopping on the Internet for holiday gifts.[105] E-mail is a serious productivity culprit with the impact on businesses being enormous. According to the survey mentioned above, half of the employees surveyed admitting to sending and/or receiving one to five non-work-related e-mails each workday.[106] It has been estimated that a company with five hundred Internet users could lose almost a million dollars in productivity annually from just a half hour of daily Internet surfing by employees. [107]

The results of a survey conducted by the American Management Association reveal that 68 percent of employers cite potential legal liability as their main reason to monitor employee activities.[108] This point is supported by the increase in the number of claims against employers for

[102] Court and Warmington op cit note 1

[103] Results of Vault.com Survey of Internet Use in the Workplace, at http://www.vault.com/surveys/internetuse2000/results2000.jsp. Accessed : 23 February 2007

[104] Ibid

[105] Ibid

[106] Ibid

[107] Ibid

[108] AMA Survey, Workplace Monitoring and Surveillance: Policies and Practices (American Management Assoc. 2001), at http:// www.amanet.org/research/pdfs/emsfu_short.pdf. Accessed 23 February 2007

employee misuse of the Internet and e-mail[109]. Liability on the part of the employer can be costly. This was illustrated in a $2.2 million settlement by the employer, Chevron.[110] This case involved a sexual harassment lawsuit involving, in part, an Internet message entitled 'Why Beer Is Better Than Women'.[111] However, sexual harassment lawsuits are not the only concern for employers. Other types of liability have also increased and pose serious risks to employers such as and what has become known as 'cyber liability' not to mention racial and other forms of discrimination that has become prevalent on the World Wide Web.[112] While no court has ever ruled that an employer must monitor electronic communications, many courts have suggested that such monitoring would be wise.[113] The following cases illustrate this point. One federal circuit court judge opined that "the abuse of access to workplace computers is so common ... that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible".[114]

Three major US corporations – RR Donnelly and Sons Co., Morgan Stanley and Co and Citicorp's Citibank N.A. were sued by black employees for racial discrimination. The action was based on the circulation of certain e- mail messages that contained racist jokes.[115] In *Harley v. McCoach*[116] , a Pennsylvania employer faced a claim of racial harassment that involved an e- mail identifying the plaintiff as Brown Sugar. The plaintiff's allegations however were insufficient to support a claim of a hostile work environment.

Employees' sexual e- mail messages or graphics are now a commonplace in sexual harassment

---

[109] *Muick v. Glenayre Elec.*, 280 F.3d 741, 743 (7th Cir. 2002) , cited in Court and Warmington op cit note 1.

[110] supra note 18

[111] supra note 18

[112] Court and Warmington op cit note 1

[113] Ibid

[114] Ibid

[115] *Owens v Morgan Stanely and Co. Inc*., No. 96 Civ. 9747, 1997 WL 403454 (S.D.N.Y 1997), cited in Court and Warmington op cit note 1.

[116] *Harley v. McCoach,* 928 F. Supp. (E.D. Pa. 1996)533, cited in Court and Warmington op cit note 1.

cases.

In *Blakey v. Continental Airlines*,[117] the New Jersey Supreme Court considered the issue of whether an employer could be held liable for sexual harassment that was rendered through the use of the Internet. The issue in point was the use of the 'Crew Members Forum,' an on-line electronic bulletin board which was used by Continental pilots and crews to post messages and communicate with one another.[118] The plaintiff was a female pilot for Continental. She alleged that the Forum had been used to publish derogatory gender-based messages about her in the middle of a federal lawsuit she had filed against the airline involving claims of sexual discrimination. When the plaintiff discovered the on-line messages, she instituted a state court action against her co-employees for defamation, as well as against the airline for a hostile work environment arising from the allegedly defamatory statements.[119]

The trial court granted the Continental's (the respondent) motions to dismiss and for summary judgment. The Plaintiff appealed. The Appeals Court agreed with the trial court's finding and held that Continental "was not vicariously liable for defamatory statements by ... [Continental] pilots".[120] The court went further and found that because Continental did not require employees to access the bulletin board, and because employees bore the cost of using the board, Continental was not liable under the doctrine of respondent superior.

The matter was then sent to the New Jersey Supreme Court. The New Jersey Supreme Court reversed the Appeal Court's decision and held that although employers are not specifically required to monitor their employees' communications, employers do have a duty to try to stop employee harassment when the employer knows or has reason to know that such harassment is occurring in the workplace.[121] The evidence established that the only way pilots were able to access the electronic bulletin board was through a personal computer and modem accessed through

---

[117] *Blakey v. Continental Airlines, Inc*., 751 A.2d 538 (N.J. 2000), cited in Court and Warmington op cit note 1.

[118] supra note 26, at 544.

[119] supra note 26 , at 547

[120] supra note 26, at 548

[121] supra note 26, at 552

the airline's contracted Internet service provider, CompuServe.[122] It is important in terms of the judgment that the court found no difference between a 'bulletin board' on the Internet and an actual bulletin board in the pilot's lounge. The court noted:

> *"the fact that the electronic bulletin board may be located outside of the workplace (although not as closely affiliated with the workplace as was the cockpit in which similar harassing conduct occurred), does not mean than an employer has no duty to correct off-site harassment by co-employees. Conduct that takes place outside the workplace has a tendency to permeate the workplace".*[123]

However, the court stated that it was unclear in this case whether the Forum "was such an integral part of the workplace that harassment on the Crew Members Forum should be regarded as a continuation or extension of the pattern of harassment that existed in the respondent's workplace".[124] This issue was referred back to the lower court.[125] The court suggested that the trial court should first determine whether Continental obtained a substantial workplace benefit from the overall relationship with CompuServe (noting that the record did not contain Continental's contract with CompuServe), the number of current users of CompuServe services, and whether Continental sought the inclusion of the Forum in the services provided by CompuServe.[126]

Whether the defamatory statements sent via e-mail was circulated on the internet or internally may not absolve the employees or their employers from liability. It is possible that an employer may be held liable for an employee's e-mail on principal/agent grounds or on vicarious liability/negligence grounds.[127]

---

[122] supra note 26, at 544-45

[123] supra note 26, at 549

[124] supra note 26, at 550

[125] supra note 26, at 558-59

[126] supra note 26, at 551-52

[127] W M Gavre "E-Mail Sexual Harassment, Company Liability and Document Production". (2000). http://www.parsonsbehlelaw.com/publications.asp?ID=267&Topic. Accessed : 04 October 2007

Employers will have to defend themselves and the interests of the company against claims of defamation that are initiated via e- mail communications.[128] In the case of *Meloff v New York Life Inc*[129]., a discharged employee brought an employment discrimination and defamation claim against her former employer because of an e- mail sent to others at the company improperly stating that the reason for her termination was credit theft and fraud. *Meloff* had worked almost three decades with New York Life when she was fired from her position as a service consultant, allegedly for misuse of her corporate credit card. At the trial the evidence showed that Meloff had violated company policy by using her corporate credit card to charge personal expenses for which she never reimbursed the employer.[130] She met a number of times with her supervisors, and her services were ultimately terminated. Immediately following the meeting that preceded in her termination, one of her supervisors sent an e-mail to seven persons which had the subject title "FRAUD" and which stated:

> *"WE FOUND IT NECESSARY TODAY TO TERMINATE PHYLLIS MELOFF, WHO USED HER CORPORATE AMERICAN EXPRESS CARD IN A WAY IN WHICH THE COMPANY WAS DEFRAUDED. PHYLISS HAD APPROX 27 YEARS WITH NEW YORK LIFE, AND WHOM WE CONSIDERED TO BE A VALUED ASSOCIATE. THIS ACTION REFLECTS OUR COMMITMENT TO "ADHERE TO THE HIGHEST ETHICAL STANDARDS IN ALL OUR BUSINESS DEALINGS." I SEND THIS TO YOU FOR YOUR OWN INFORMATION".*

After a trial a jury awarded Meloff $250,000 in compensatory damages and $1,000,000 in punitive damages on the defamation claim. The Second Circuit Court of Appeals upheld the jury's finding that the employer acted with malice in sending the e-mail and thereby abused its qualified privilege, because one of the supervisors had assured Meloff, after the credit card abuse was initially discovered, that it was "no problem," but less than a week later sent the inflammatory email.

Employers can face liability for copyright infringement. This can occur where an employee

---

[128] Ibid

[129] *Meloff v. New York Life Inc*, 51 F.3d 372 (2nd Cir. 1995), on remand at No. 92 CIV .7126 KTD, 1999 WL 604871 (S.D.N.Y., 10 August 1999), cited in Court and Warmington op cit note 1.

[130] supra note 38

improperly places copyrighted materials on the Internet.[131] In the case of *Marobie – FL, Inc. v. Nat. Ass'n of Fire Equip. Dist*[132]*.,* a software company successfully brought a claim against the association for copyright infringement after an employee placed files containing copyrighted clip art on the association's web page.

Following is an analysis of the U.S. laws regarding the various forms of monitoring of an employee, with reference to federal and state responses to the issue of privacy in the workplace.

When defining an employee's right to privacy in the workplace, it is essential to determine whether the employer is a government agency or a privately owned operation.[133] When the government employs, it must honour the constitutional rights to privacy that all employees are entitled to. This right comes to the fore when an employer has reason to search an employee's work space or take other steps which have the potential to infringe upon its employees' constitutional rights to privacy, such as monitoring e-mail and Internet usage.[134]

The issue of workplace privacy was addressed in the landmark Supreme Court case of *O'Connor v. Ortega.*[135] In that case the Supreme Court recognized that employees may possess legally protected privacy interests, but the court stated that these rights are qualified. The court held that employees' individual privacy interests must be balanced against the realities of the workplace. The Supreme Court noted that even at work employees have a few areas in which an employee has

---

[131] Gavre op cit note 36

[132] *Marobie – FL, Inc. v. Nat. Ass'n of Fire Equip. Dist* 983 F. Supp. 1167 (N.D. III.1997), cited in Court and Warmington op cit note 1.

[133] *O'Connor v. Ortega,* 480 U.S. 709, 719 (1997) , where the court held that : "the Fourth Amendment applies to searches conducted by [public employers]"); (In *Gilmore vs. Enogex, Inc*., 878 P.2d 360, 365 (Okla. 1994) – it was held that "[t]he constitutional right of privacy affords protection against governmental intrusions and is not enforceable against private individuals or corporations ...."). However, it is important to note that the Fourth Amendment may be implicated for private employers who search pursuant to governmental regulations or essentially act as governmental bodies. (See *Skinner v. Ry. Labor Executives Ass'n.*, 489 U.S. 602, 614-16 (1989)- where the court found the Fourth Amendment applicable to company that complied with government drug testing regulations) and (*Marsh v. Alabama*, 326 U.S. 501, 508-10 (1946) – where it was held that a private corporation which acted essentially as a municipality in a company-owned town was a state actor).

[134] supra note 42

[135] supra note 42

a reasonable expectation of privacy. These areas may include, for example, desks and file cabinets. However, the Court also noted that these expectations with regard to privacy of an employee "may be reduced by virtue of actual office practices and procedures." An important aspect of this judgment is that the court recognized that with the question of privacy in the workplace there are no absolutes. The conclusion reached by the court was that the question of employee privacy and the expectation thereto is determined by specific practices within the employee's workplace, and the issue of whether an employee has a reasonable expectation of privacy "must be addressed on a case-by-case basis".[136]

The 'right to privacy' is not explicitly mentioned in the U.S. Constitution. There are however certain sections, which if read together do imply a right to privacy.[137] One such section is the Fourth Amendment. The Fourth Amendment guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." This, however, applies exclusively to the government, and not to private individuals.[138]

The Fourth and Fourteenth Amendments to the United States Constitution protect government employees from unlawful searches and seizures by the federal and state governments.[139] The intrusion upon any employee's privacy by a government employer can only be regarded as lawful if the employer's intrusion is proved to be reasonable. Such a search is deemed to be reasonable if it does not infringe upon an employee's reasonable expectation of privacy in the property searched.[140]

---

[136] M J Bassett et al. … "An Overview of E-Mail and Internet Monitoring in the Workplace. http://www.fmew.com/archive/monitoring/. Accessed: 04 October 2007.

[137] *Walter v. United States* , 447 U.S. 649, 662 (1980) - This Court has … consistently construed this protection as proscribing only governmental action; it is wholly inapplicable to search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official. See also Amagid "Work Computers Not Protected by Privacy Rules". .https://message.computerlaw.com/GH_PrintFriendly.asp?HID=40&CATID. Accessed : 05October 2007

[138] supra note 46

[139] supra note 46

[140] supra note 42 , at 714

The question as to whether a search intrudes upon an employee's reasonable expectation of privacy is to be determined on a case-by-case basis.[141] Therefore it is incorrect to hold the view that the search of an employee's computer, desk, file cabinet, or other work space, may or may not be searched under any circumstances. The constitutionality of each search depends on the circumstances surrounding it.[142] To determine the constitutionality of any intrusion into employee privacy by a governmental employer, it is essential to consider the reasons for and against the search.[143] The approach adopted by the courts is to balance the employer's justification for the search. This would include the need for supervision, control, and the efficient operation of the workplace, against the employee's legitimate expectations of privacy in the property searched.[144] If the employer's needs for the search outweigh the employee's reasonable expectations of privacy in the property searched, then the search will be upheld as constitutional.[145] It order to determine whether an employee has a reasonable expectation of privacy in certain property, or certain areas of work space it must first be considered whether or not the work area in question is given over to the "employee's exclusive use ... the extent to which others had access to the work space ... the nature of the employment ... and whether office regulations placed employees on notice that certain areas were subject to employer intrusions".[146]

Historically The Fourth Amendment has provided only limited privacy protection to governmental employees.[147] Courts have often given public employers the power to determine whether to search employee computers and other work areas, provided the employer can articulate a legitimate justification for the search and show that the employee had no reasonable expectation of

[141] supra note 42, at 714 and 718

[142] supra note 42, at 714 and 718

[143] supra note 42, at 714 and 718

[144] supra note 42, at 714 and 718

[145] supra note 42, at 719-720

[146] *Vega-Rodriguez v. P. R. Tel. Co*., 110 F.3d 174, 179 (1st Cir. 1997), cited in Court and Warmington op cit note 1.

[147] supra note 46

privacy.[148] For example, in *Bohach v. City of Reno*[149], the plaintiffs claimed that the City of Reno, Nevada, violated their constitutional right to privacy by intercepting messages sent between officers from their squad cars over a computerized communications system similar to e-mail. The court held that even though the officers' messages were intercepted their constitutional rights to privacy were not violated because they did not have an objectively reasonable expectation that their messages were protected from employer monitoring.[150] The e- mail system was designed in such a manner that all messages were received and stored in a central computer before being forwarded.[151] This meant that all messages were accessible to the employer at the central computer. It was held that the officers could not have a reasonable expectation that their messages would remain private because they had been notified by the police chief that all e-mail users would have their messages 'logged on the network' and that some messages (e.g. those violating the department's anti-discrimination policy) were banned.[152] The officers thus had notice from their employer that their messages were not private.[153]

Only certain states have constitutional provisions which also provide some privacy protection.[154] Thus far the state of California has attempted to extend this protection to private sector employees. This move has been met with opposition by a yet to be published California Superior Court opinion, which refused to recognize constitutional protection from e-mail monitoring by private employers.[155]

---

[148] supra note 42

[149] *Bohach v. City of Reno*, 932 F.Supp. 1232, 1233 (D. Nev. 1996), cited in Court and Warmington op cit note 1.

[150] supra note 58, at 1234

[151] supra note 58, at 1234

[152] supra note 58, at 1235

[153] supra note 58, at 1234-35; In the case of *Williams v. Philadelphia Hous. Auth*., 826 F. Supp. 952, 954 (E.D. Pa. 1993) , the employee failed in a claim against his government employer for invasion of the employee's constitutional right to privacy, when the employer reviewed the contents of a computer disk left behind by the employee, since according to the court, the employer's search of the disk was in pursuit of "maintaining efficiency and productivity in the workplace".

[154] Court and Warmington op cit note 1, 24

[155] Ibid

Statutory Protections

Prior to 1986 there were laws in place to protect the privacy of mail and voice communications, but no laws existed to protect the privacy interests of persons who chose to communicate through the emerging use of telecommunications and computer technology.[156] To correct the situation in what lawmakers called a 'gap' resulting in legal uncertainty, the American Congress passed the Electronic Communications Privacy Act (ECPA) in 1986, to provide protection for electronic communications.[157] Title I of that Act amended the Federal Wiretap Act (which previously addressed only wire and oral communications) to protect against unauthorized interception of 'electronic communications'. Title II of the ECPA created the Stored Communications Act, which protects against unauthorized 'access' to electronic communication while it is in electronic storage. Civil and criminal penalties are both provided for in the Act. In essence then, a successful civil plaintiff may recover the greater of either: 1) actual damages suffered and any profits made by the violator, or 2) statutory damages (the greater of $100 a day for each day of the violation or $10,000). Attorney's fees and costs may also be awarded. Criminally, a violator may be punished with up to five years imprisonment and fines up to $5000.[158]

The ECPA is criticized for its ambiguity despite the efforts of the American Congress' to implement legislation that attempts to catch up with technology.[159] The reason for some of the difficulty may be attributed to the fact that the Act was written prior to the advent of the Internet. A further complication is the absence of any specific provisions relating to e-mail, which is transmitted and stored in much more complex ways than other forms of communication.[160] The legislative history does indicate that Congress intended the Act to cover e-mail, however the term

---

[156] Ibid 25

[157] Ibid

[158] Ibid 25

[159] *Fraser v Nationwide Mut. Ins. Co.,* 135 F. Supp. 2d 623,633 (E.D. Pa. 2001) - where the court described the ECPA as "a complex, often convoluted, area of the law". See aslo *United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998)*.

[160] Court and Warmington op cit note 1, 25

'e-mail' appears nowhere in the Act. Despite this, courts began to apply the ECPA to monitoring in the workplace, and in doing so, gave employees the privacy protections Congress desired.[161] As will be seen below, the exceptions to the Act nearly override the rule, and in the process makes the expectation of privacy nothing but a mere illusion.[162]

Analysis of the ECPA and Its Exceptions

Interception versus Storage

The ECPA has a two role, firstly of providing protection against unauthorized interception of communications, and secondly protection against unauthorized access to stored communications. The procedural and substantive requirements for each are markedly different.[163] The first stage of the enquiry is to determine whether the provider has in fact 'intercepted' an electronic communication. This question may not be easily answered because electronic communication, such as e-mail, by its very nature may go through stages of transmittal, sometimes remaining in 'intermediate storage' before it reaches the intended recipient.[164] Communications posted to electronic bulletin boards are not expressly catered for in the Act. All circuit courts called upon to consider the issue has ruled that an 'interception' of electronic communication will only be found to have occurred if it takes place at the same time with transmission. This is so, despite the many struggles all the circuit courts have had with interpretation of the statute.[165] For instance, two courts have held that an interception did not occur where e-mail was stored on an electronic bulletin board, even though it had not yet been read by the intended recipient. In another case, a

[161] Ibid

[162] Ibid 26

[163] *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003) - (where the court noted that stored communications are subject to less burdensome procedures).

[164] supra note 72 ; *Konop v. Hawaiian Airlines, Inc*., 302 F.3d 868 (9th Cir. 2002); *Steve Jackson Games, Inc. v. U.S. Secret Serv*., 36 F.3d 457, 459-62 (5th Cir.1994); see also *Wesley College v. Pitts, 974 F.* Supp. *375 (D. Del. 1997)*, summarily aff'd, 172 F.3d 861 (3d Cir. 1998).

[165] supra note 72, at 1050

court found no interception when the company accessed e-mails from the company's central file server, because the access did not occur at the time of the initial transmission.[166]

The Court of Appeals for the First Circuit recently found a web-monitoring company in violation of the ECPA. The violation involved the interception of information that concerned Internet users contemporaneously with their web use, and thereafter distributing such information to other interested parties. The court held that the system used by the web-monitoring company was, in effect, an automatic routing program.[167]

Both the Federal Wiretap Act and the Stored Communications Act of the ECPA contain exceptions, which, when used properly by employers, allow for monitoring in the workplace.[168]

Consent Exception

The first exception is the 'consent' exception. This exception applies when one party to the communication has given prior consent to the interception or access. This exception will not be applicable if the interception is accomplished for an unlawful purpose.[169] The consent required may be either express/actual or implied/tacit. The consent may not be constructive.[170] The courts have generally found that there has been implied consent when the employee knew or should have known of a policy of constantly monitoring calls, or when the employee conducts a personal conversation over a line that is explicitly reserved for business purposes.[171] In the case of *Griggs-Ryan v. Smith*,[172] the Court of Appeals for the First Circuit held that a tenant had consented

---

[166] supra note 72, at 1050

[167] *In re Pharmatrack, Inc*., 329 F.3d 9, 22 (1st Cir. 2003).

[168] Court and Warmington op cit note 1, 27

[169] Ibid 28

[170] Ibid 28

[171] Ibid 28

[172] *Griggs-Ryan v. Smith* ,904 F.2d 112 (1st Cir. 1990)

to his landlord's interception of incoming phone calls when he had been told on a number of occasions that all such calls would be recorded. In *Jandak v. Village of Brookfield*[173], a federal district court likewise found that a police officer consented to interception of his phone calls where he knew or should have known that the phone line he was using was constantly taped for police purposes, and because he was provided with an unmonitored line for personal use.[174] Courts may refuse to imply consent by an employee if the employer had only indicated that it *might* be forced to monitor telephonic conversations in order to determine the number of personal calls made by employees.[175]

It is possible for employees to consent to monitoring of only part of a communication or to only a specific set of communications.[176] Therefore, employers must be cautious in their drafting of policies that are directed at communications that are to be monitored. Employers must also ensure that any monitoring conducted must be kept within the set limits determined by that policy document.[177] If a policy as the one mentioned above is in place, any continued private use of the work e-mail system by an employee will be done with the implied consent of the employee.[178]

Provider Exception

The second general exception is the 'provider' exception. This exception relates to employers who

[173] *Jandak v. Village of Brookfield* , 520 F. Supp. 815, 824-25 (N.D. Ill. 1981)

[174] supra note 82; see also *Simmons v. Southwestern Bell Tel. Co*., 452 F. Supp. 392, 393-94, 396 (10th Cir. 1979)- (the court held that there was consent where the plaintiff made a personal call on a phone which was to be used exclusively for business purposes and which he knew was regularly monitored, instead of other phones that were specifically provided for personal calls).

[175] *Deal v. Spears*, 980 F.2d 1153, 1155-57 (8th Cir. 1992) - (the court found no implied consent where the employee was only notified that the employer 'might' monitor to cut down on the number of personal phone calls).

[176]In re Pharmatrack, Inc. supra note 76, at 19- (the court held that a court must inquire into the 'dimensions of the consent' and then determine whether the interception exceeded those boundaries); In *Watkin v. L.M. Berry & Co s*, 704 F.2d at 581- it was held that the employee consented to interception of business calls, but not personal calls.

[177] supra note 76

[178] supra note 76

own and provide their company e-mail networks.[179] The cases discussing the provider exception primarily concern telephone use, but one federal circuit court has discussed the exception in the context of e-mail. The Court of Appeals for the Third Circuit in *Fraser v. Nationwide Mutual*[180] held that access to an insurance agent's stored e-mail is exempt from the ECPA because the e-mail is stored on the insurance company's system, which the company administered as a provider. The Appeals court in this case relied on *Bohach v. City of Reno*,[181] in which a district court similarly held that the retrieval of alphanumeric pages stored on the police department's computer system was not a violation of the ECPA. The court noted that when it comes to accessing communications in storage, service providers may 'do as they wish'.[182]

The two *cases* discussed above involved access to stored communications, and were governed by the less restrictive Stored Communications Act. This Act provides complete exclusion to anyone who is a provider of an electronic communications service.[183] If, however, the provider is intercepting communications, additional requirements must be met under the Wiretap Act. These requirements include that the provider must be able to show that the interception occurred in the normal course of employment while engaged in an activity that is either a 'necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service'.[184] The few cases reported that discuss the interception of communications by providers indicate, that these additional requirements are not hard to meet. For instance in the case of *United States v. Mullins*[185], the Court of Appeals for the Ninth Circuit found that American Airlines acted lawfully in monitoring a travel agent's computer reservations because American Airlines, as the provider of the computer reservation system, was monitoring to uncover suspected fraud. The

[179] Court and Warmington op cit note 1 ,29

[180] *Third Circuit in Fraser v. Nationwide Mutual,* 352 F.3d 107 (2d Cir. 2003).

[181] supra note 58, at 1232

[182] supra note 58, at 1236.

[183] supra note 58

[184] Court and Warmington op cit note 1, 30

[185] *United States v. Mullins,* 992 F.2d 1472 (9th Cir. 1992).

court found that the airline security chief who monitored the travel agent's computer was doing so 'within the scope of her employment' and 'to protect the rights and property of her employer'. Therefore, no liability existed under the ECPA.[186]

Ordinary Course of Business Exception

For a violator to be regarded as liable under the ECPA, it must be shown that any interception of communication that occurred had been conducted with the use of an 'electronic, mechanical or other device'.[187] The phrase 'electronic, mechanical or other device' does not include any 'telephone or telegraph instrument, equipment or facility, or any component thereof', which is used by a provider of wire or electronic communication service 'in the ordinary course of its business'.[188] Thus far, this exception has only been applied to telephone monitoring and has not been extended to the monitoring of e-mail.

If the context approach is favoured then a court will examine the employer's motive for the monitoring and whether 'it had a legitimate business justification in doing so'.[189] Some courts that have used this approach have upheld monitoring where an employer had reason to believe that an employee was disclosing confidential information in violation of a loyalty agreement,[190] and where employees' telephone calls were being monitored for quality control.[191]

On the other hand a court using the content approach focuses not on the employer's business

[186] supra note 58, at 1478.

[187] Court and Warmington op cit note 1, 31

[188] Ibid

[189] Ibid

[190] *Briggs v. American Air Filter Co., Inc*., 455 F. Supp. 179, 180- 82 (N.D. Ga. 1978), aff'd, 630 F.2d 414 (5th Cir. 1980).

[191] *James v. Newspaper Agency Corp*., 591 F.2d 579, 581 (10th Cir. 1979).

reasons for monitoring, but rather on whether the monitored communication is of a business or personal nature.[192] This was illustrated in the case of *Watkins v. L.M. Berry & Co*[193]. In this case all the employees were aware that the employer was monitoring employees' phone calls in accordance with an established policy. The plaintiff sued under the ECPA. The reason for her action was her discovery that the company had monitored a personal phone call in which she discussed an interview for employment she had with another company.[194] The Court of Appeals for the Eleventh Circuit held that while business calls are necessarily monitored in the normal course of business, personal calls cannot be intercepted in the ordinary course of business except to the extent necessary to determine that they are in fact personal calls.[195] Another court using the content approach found that a call was not of a personal nature, and therefore validly monitored, where it occurred during office hours, between co-employees concerning their supervisors.[196]

Many states have formulated their own statutes regarding interception of electronic communication.[197] These state statutes have similar provisions to the ECPA, but there are some important exceptions. For example, several states require the consent of both parties to a conversation before monitoring can occur.[198] At least two states, Connecticut and Delaware, "require advance notice of any electronic monitoring ...." Therefore, even if an employer meets one of the above exceptions under the ECPA, the employer must also closely check relevant state law. If one has to put things into perspective, one can conclude that, while the ECPA prevents an employer from intercepting e-mail in transit, it offers the employees little additional privacy protection on their work computers from their employers. [199]

---

[192] *Watkins v. L.M. Berry & Co*., 704 F.2d 577, 582-84 (11th Cir. 1983).

[193] supra note 101

[194] supra note 101, at 579.

[195] supra note 101, at 583.

[196] *Epps v. St. Mary's Hosp. of Athens, Inc.*, 802 F.2d 412, 416-17 (11th Cir. 1986).

[197] *Bartnicki v. Vopper,* 532 U.S. 514, 541-42, n.1 (2001) (Rehnquist, C.J., dissenting) (collecting statutes).

[198] Court and Warmington op cit note 1, 32

[199] Court and Warmington op cit note 1, at 32

Lacking adequate protection under constitutional or statutory law, many employees turn to common law causes of action when challenging employer monitoring.

In terms of the American Common Law of Tort, there are four distinct state law torts that relate to the invasion of privacy: [200]

1. unreasonable intrusion into one's seclusion,
2. misappropriation of one's name or likeness,
3. public disclosure of private facts, and
4. false right.

The only theory that would be applicable to hold an employer liable for violating work computer privacy is 'intrusion upon seclusion,' for which a plaintiff must prove '(1) an intentional intrusion, physical or otherwise, (2) upon the plaintiff's solitude or seclusion or private affairs or concerns, (3) which would be highly offensive to a reasonable person'.[201]

The concept of intrusion upon seclusion is defined as: [202]

> *"One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for the invasion of his privacy, if the intrusion would be highly offensive to a reasonable person*".

To a large degree the common perception of employees is that employers should not have the right to monitor workplace e-mail and Internet use.[203] The law, however, has provided differently on this point. While employees are often under the misconception that any use of the Internet and

---

[200] M. Colucci. The Impact of the Internet and New Technologies on the Workplace. (2002). 158

[201] Ibid 158- 159

[202] Dichter and Burkhardt, "Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age". (June 1999), available at <http://www.mlb.com/art61499.html>> Accessed : 25 November 2006

[203] C J Muhl "Workplace e-mail and Internet use: employees and employers beware" February (2003) *Monthly Labor Review* 37

e-mail at the workplace is private, the courts have indicated on several occasions that there is no reasonable expectation of privacy in such use and have consistently permitted employers to monitor employee activity.[204]

The case of *Smyth v. Pillsbury Co*. [205]discusses common law privacy. In Smyth, the Pillsbury Company fired one of its regional operations managers for sending what the company 'deemed to be inappropriate and unprofessional comments over ... [the company's] e-mail system'.[206] The manager made threats against sales management to "kill the backstabbing bastards" and referred to the planned Holiday party as the 'Jim Jones Kool-Aid affair' when replying to e-mail messages from his supervisor over the company's e-mail system. Although the manager sent the messages via company e-mail, he did so from his personal computer at home, and did so based upon the company's assurances that "all e-mail communications would remain confidential and privileged".[207] The manager sued the company for wrongful discharge, when his contract was terminated, claiming that his termination violated Pennsylvania's public policy against terminating at-will employees after violating their right to privacy.[208]

The court balanced the company's reasons to intercept the manager's e-mail with the manager's reasonable expectations that the e-mail would remain private. The court held that the manager had no "reasonable expectation of privacy in e-mail communications voluntarily made ... over the company e-mail system notwithstanding any assurances that such communications would not be intercepted". The court went on to explain that once the manager made comments over "an e-mail system which was apparently utilized by the entire company, any reasonable expectation of

---

[204] Ibid

[205] *Smyth v. Pillsbury Co.,* 914 F. Supp. 97 (E.D. Pa. 1996), cited in Court and Warmington op cit note 1.

[206] supra note 114, at 98-99. see also L. Camille He'bert "Honesty in the Workplace: Common – Law Restrictions on Electronic Monitoring and Surveillance" *Employee Privacy Law*. Westlaw. Accessed: 20 February 2007.

[207] supra note 114, at 98-99.

[208] supra note 114, at 100.

privacy was lost". The court was of the view, which appears to be fatal for employees wishing to bring privacy claims based upon e-mail monitoring in Pennsylvania, that there are "no privacy interests in ... [email] communications". The court went on to hold that even if the manager could have had a reasonable expectation of privacy to the content of his e-mail messages, the company did not commit a "substantial or highly offensive invasion" of the manager's privacy by reading his messages. The court based its finding upon the fact that, unlike a compulsory employee drug or alcohol test conducted by the employer, the company merely monitored e-mail messages that the manager voluntarily sent over the company e-mail system. The important aspect of this judgment is that it seems to indicate that a company's interest in monitoring e-mails to prevent inappropriate and unprofessional comments, or even illegal activity over its e-mail system, outweighed any privacy interest the manager could have had in his comments.[209]

Recent cases have applied these principles to monitoring of e-mail. This is illustrated in the case of *McLaren v. Microsoft Corp*[210]., the Texas Court of Appeals held that an employee did not have a legitimate expectation of privacy in the contents of stored e-mail messages, despite the fact that they were stored in 'personal' folders under a private password. The court held that the e-mails were stored on a company computer given to the plaintiff to perform in the course and scope of his employment, and as such, were an "inherent part of the office environment," and not the employee's personal property. The court additionally pointed out that although the e-mails were stored in password-protected folders, they were initially sent over the network and were at some point accessible by another individual.[211] The court went further and held that even if the employee had some expectation of privacy in the e-mail messages, that a reasonable person would not find the search a "highly offensive invasion". The court held that the plaintiff was on leave pending a sexual harassment investigation at the time the e-mails were accessed and that some of the e-mails were indeed relevant.[212] The court held that the company's interest in preventing

[209] supra note 114, at 101.

[210] *McLaren v. Microsoft Corp*, 1999 WL 339015 (Tex. Ct. App. 1999), cited in Court and Warmington op cit note 1.

[211] supra note 119, at 4-5

[212] supra note 119, at 5.

inappropriate, or even unlawful conduct, outweighed any claimed privacy interest in those communications.[213] In cases based on similar facts the courts have held that no reasonable expectation of privacy exists under similar circumstances.[214]

In conclusion it is true to say that in terms of American law employees have no privacy rights in their e-mail and Internet use, and Federal law does not prohibit employers from monitoring that use. However the failure to monitor employees' e-mail and Internet use can lead to legal liability in more ways than one for the employer. Unless there is a reasonable expectation of privacy suggested by an employer, that employer is legally allowed to monitor the computer use of its employees on company computers. The onus then rests on all employees to carefully read and understand all relevant company codes and policies before engaging in any personal use of company computers.[215]

[213] supra note 114, at 5.

[214] *Garrity v. John Hancock Mutual Life Ins. Co., No*. CIV.A. 00- 12143-RWZ, 2002 WL 974676, at 2 (D. Mass. May 7, 2002) – (the court held that even if the plaintiffs had a reasonable expectation of privacy in their password-protected e-mails, the employer's legitimate business interest in protecting employees from sexual harassment outweighed those privacy interests).

[215] Amagid op cit note 46

2. The law on Employee Monitoring in the United Kingdom

There has been ever increasing number of employers monitoring staff e- mail and Internet activities in The United Kingdom (UK). It has been estimated that in the year 2000, 55 percent of employers monitored e-mail usage and 77 percent monitored Internet activities of their employees in the workplace.[216] It has been common practice that employees were given little to no protection against infringements of their privacy in the work place. This enabled employers to legitimately monitor and scrutinize workers on- line activities, irrespective of whether these communications were of a personal nature.[217] Thus it was deemed fair for employees to be dismissed for downloading inappropriate Internet material and also for making extensive Internet searches with regard to information that was not associated with their job description.[218]

The landmark case of *Halford v United Kingdom* [1997] IRLR 471 ECHR, dealt with the interception and monitoring of telephone calls in the workplace. It was argued in this case that the employee had a reasonable expectation of privacy in the workplace that had been infringed, as she had not been warned that her communications would be intercepted. The European Court of Human Rights acknowledged that the right to private life and correspondence can cover calls made at work.[219]

In light of the *Halford*[220] decision The Home Office issued a set of standards and guidelines for the use of telephone and communications surveillance devices at work. This was done in preparation for the implementation in the UK for the Human Rights Act (HRA).[221]

One of the main objectives of the HRA is to give further effect to domestic law to rights and

[216] Colucci op cit note 109, 95

[217] Ibid

[218] Ibid

[219] Ibid 95-96

[220] *Halford v United Kingdom* [1997] IRLR 471 ECHR

[221] www.new-law-journal.co.uk/Index/Index%201999%20.pdf . Accessed: 05 October 2007.

freedoms guaranteed under the European Convention on Human Rights (ECHR). The most relevant of these rights for the use and monitoring of e- mail and the Internet at work is article 8. Article 8 affirms the right to have one's private life and correspondence respected. [222]

J Morris believes that under the HRA, article 8 has an impact on domestic law in following ways: [223]

1. *"The HRA requires all legislation to be read and given effect in a way which is compatible with the Convention rights. This obligation may affect the interpretation given by the courts to the relevant legislation.*
2. *The Act makes it unlawful for a public authority to act in way which is incompatible with a Convention right unless, as a result of the provisions of primary legislation, it could not have acted differently. The victims of such acts may bring proceedings against a public authority, or rely upon Convention rights in any other proceedings. Thus, employees employed by 'public authorities' who allege that their employer has violated their rights under article 8 may sue them".*

Two sets of legislation regulate the use and monitoring of e- mail and the internet at work:
a) The Regulation of Investigatory Powers Act 2000 and b) The regulations made under the authority of that Act, and the Data Protection Act 1998. For the purposes of this dissertation only the former piece of legislation is relevant.[224]

The main purpose of the Regulation of Investigatory Powers Act (RIPA) 2000 would be to ensure that the relevant investigatory powers are used in accordance with human rights. These powers are:[225]

- The interception of communications;

[222] Colucci op cit note 109, 95

[223] J. Morris, "The Use and Monitoring of E- mail and the Internet at Work in English Law", *Bulletin of Labour Law and Industrial Relations,* No. 40, 2001, Kluwer Law International., cited in Colucci op cit note 81, 96

[224] Colucci op cit note 109, 95

[225] Ibid

- The acquisition of communications data
- Intrusive surveillance (on residential / in private vehicles)
- Covert surveillance in the course of specific operations;
- The use of covert human intelligence sources
- Access to encrypted data

For each of these powers, the Act will ensure that the law clearly covers:

- the purpose for which they may be used;
- who should authorise each use of the power;
- which authorities can use the powers;
- the use that can be made of the material gained;
- independent judicial oversight ;
- a means of redress for the individual

Section 1 (3) of the RIPA provides that:
"Any interception of a communication which is carried out at any place in the UK by, or with the express or implied consent of, a person having the right to control the operation or the use of a private telecommunication system shall be actionable at the suit or instance of the sender or recipient, of the communication if it is without lawful authority and is either:

1. An interception of that communication in the course of its transmission by means of that private system; or
2. An interception of that communication in the course of its transmission, by means of a public telecommunications system, to or from apparatus comprised in that private telecommunication system".

Section 1(3) of the RIPA, creates civil liability for unlawful interception on a private person who may bring an action under this subsection. This includes the sender, recipient or intended recipient. Therefore, either the employee or the third party may sue the employer where there is reason to believe that an employer has unlawfully intercepted a telephone conversation between an

employee and the third party. [226]

Section 1 (1) of the RIPA prescribes the circumstances in which interception of a communication being transmitted by a public postal service or public telecommunication system is a criminal offence.[227]

In terms of the aforementioned section, it would be a criminal offence for a person to intentionally and without lawful authority to intercept, at any place in the UK, any communication in the course of its transmission (a) by means of a 'public telecommunications system', or (b) by means of a 'private telecommunications system'.[228] A 'public telecommunications system' means any such parts of a telecommunications system by means of which any public telecommunications service is provided as are located in the United Kingdom; a ' public telecommunications service' means any telecommunications service which is offered or provided to, or to substantial section of, the public in any one or more parts of the UK.[229]

Section 1(2) of the RIPA sets out the circumstances when the interception of a communication being transmitted by a private telecommunication system is an offence. [230] A 'private telecommunications system' means any telecommunications system which, without itself being a telecommunications system, is a system which (a) is attached, directly or indirectly and whether or not for the purposes of the communication in question to a public telecommunications system; and (b) there is apparatus comprised in the system which is both located in the UK and used (with or without other apparatus) for making the attachment to the public telecommunications system. This provision is deemed to totally exclude self standing systems, such as secure office intranet.[231]

---

[226] Colucci op cit note 109, 99

[227] Colucci op cit note 109, 99

[228] Ibid

[229] Ibid

[230] Ibid

[231] Ibid

What constitutes the interception of a communication in the course of its transmission by means of a telecommunication system is explained in section 2 (2) of the RIPA. This is relevant to the criminal offence and civil liability in section 1of the RIPA; and to the issuing of a warrant by the Secretary of State which authorises or requires the interception in section 5 of the RIPA. In terms of the RIPA, a person intercepts a communication if he or she:

1) modifies or interferes with the system , or its operation,
2) monitors transmissions made by means of the system , or
3) monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.[232]

Any conduct which relates only to the traffic data comprised in or attached to a communication, or which relates only to so much of the content of the communication as is necessary in order to identify this traffic data is excluded from the definition of interception in the Act.[233] Where any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently are also specifically included within the definition of interception.[234]

The provision thus allows the sender or recipient of a communication to seek an order against, or claim damages for any loss incurred from an employer who intercepted a communication to or from its system, provided that it was done 'without lawful authority'.[235]

The Act specifies a range of circumstances where the requisite authority is considered to be present, two of which are relevant to employment. The first of these is where the communication is one which the person intercepting has reasonable grounds for believing, is sent by a person who has consented to the interception and secondly the case where the intended recipient of the

[232] The "Regulation of Investigatory Powers Act" is available at, << http://www.legisaltion. hmso.gov.uk/acts/acts2000/20000023.htm>>. Accessed: 25 May 2007.

[233] The " Regulation of Investigatory Powers Act", section 2 (5)

[234] The " Regulation of Investigatory Powers Act", section 2 (5)

[235] The " Regulation of Investigatory Powers Act", section 2 (5)

communication has also consented to the interception.[236] Employers may prove that the requisite consent was present. They can do this by simply showing that the employee's contract permitted interception.[237] In some instances it may be possible to argue that a practice of interception familiar to the employee could be sufficient. However, the duty of the courts under the Human Rights Act to interpret legislation compatibly with Convention Rights, as well as the terms of the European Convention (EC) Directive 97/96, may lead to the conclusion that this would be insufficiently unequivocal.[238] Employer's therefore tend to choose rather to rely upon a second set of exceptions, contained in the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under the authority of the Regulation of Investigatory Powers Act, which do not require the consent of either party.[239]

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 authorises certain interceptions of telecommunication communications which would otherwise be prohibited by section 1 of the Regulation of Investigatory Powers Act 2000.[240] In terms of article 5 .1 of the Directive 97/66/EC, any interception has to be with the consent of a person carrying on a business (which includes the activities of government departments, public authorities and others exercising statutory functions), the purposes of which must be relevant to that person's business and using that business's own telecommunication system.

In terms of the above regulations interceptions are authorized for monitoring or recording communications in the following circumstances:[241]

- to prove a set of facts;

---

[236] The " Regulation of Investigatory Powers Act", section 3(1)

[237] The " Regulation of Investigatory Powers Act", section 3(1)

[238] Colucci op cit note 101, 101

[239] Ibid

[240] The complete text of these regulations are available at <<www.hmso.gov.uk/si2000/20002699.htm>>

[241] Colucci op cit note 109, 102

- to determine compliance with regulatory requirements including certain specified procedures;
- to ascertain or demonstrate standards which are ought to be achieved in the interests of national security (in which case only certain specified public officials may make the interception);
- the prevention of crime,
- then investigation of unauthorized use of telecommunication systems;
- to promote effective system operation,
- to monitor received communications in order to determine whether they are business or personal communications,

These interceptions can have a lawful and legitimate purpose provided that the interceptor/manger of the telecommunications system has made all reasonable efforts to inform employees and potential users that interceptions may be made. A proper and legitimate effort would include clauses in the employment contract and/ or regular notices, reminders on notice boards in offices and stickers on computers and telephones.[242]

An employer will be liable for court action if any communications are monitored in breach of instructional regulations. It is thus essential that any evidence collected, is stored and used in the appropriate manner.[243] If there is a need for any disciplinary action, such action must be taken in accordance with the provisions of the Human Rights Act, and natural justice in general.[244]

The Regulation of Investigatory Powers Act (RIPA) 2000 including its supplementary provisions govern the situations under which employers may monitor the use of e- mail and the Internet at work. In light of these aforementioned Regulations, interceptions for specified purposes (which includes investigating or detecting unauthorized use of a telecommunications system and determining whether communications relate to the business) are authorized provided that the

[242] Ibid 109-110

[243] Data Protection Act 1998, available at <http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm>>

[244] Data Protection Act 1998, available at <http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm>>

employer has made all reasonable efforts to inform those who may use the system that interceptions may take place.[245]

In the UK there is no legal requirement for monitoring to be discussed with employee representatives. This being the case, government has indicated that it encourages businesses to agree with employees on appropriate levels of recording or monitoring if they wish, but does not oblige them to engage in collective bargaining on this matter.[246]

It would constitute repudiatory breach of contract in terms of the common law should an employee fails to comply with the regulations laid down by the employer with regard to the use of the e- mail, Internet and other electronic devices of the workplace. In such cases this could justify dismissal of the employee without notice.[247] A single act of misconduct can justify dismissal only if it is of particularly serious nature. The downloading of child pornography is a good example. [248]

Employees do have statutory protection against unfair dismissal. In terms of this protection employers are required to have a fair reason for the dismissal of employees. This would involve consideration as to whether the employer followed fair procedure for dismissal. In terms of the Human Rights Act 1998, legislation should be interpreted compatibly with the European Convention on Human Rights.[249] The effect of this is that, should an employer dismiss and employee in violation of any right in the Convention, the dismissal would not be regarded as fair. However European courts have held that the use of illegally obtained evidence in criminal proceedings suggests that the fact that an employer may have obtained the information leading to the decision to dismiss in breach of the Convention, may not in itself render that information inadmissible in court.[250]

---

[245] Colucci op cit note 109, 110

[246] Ibid 111

[247] Ibid

[248] Ibid

[249] Ibid 112

[250] Ibid 111- 112

3. GERMANY

There is no explicit right to privacy in The German Constitution. The right to privacy in terms of German law is derived from a general constitutional personality right. This personality right is further derived *(Allegemines Personlichkeitsrecht)* from the protection of dignity against abuse of state power *(Recht auf Schutz der Menschenwiirde),* and the individual's right to free development of one's personality *(Recht auf freie Entfaltung).*[251] The Federal Labour Court has regarded the aforementioned rights to be applicable to an employment relationship.[252] The protection of employees' privacy is protected by the Constitution and many legislature enactments. The State in terms of the Constitution is bound to respect and protect a person's right to privacy.[253] All employees have the right to the free development of their personality insofar as this does not violate the rights of others or undermine any provision of the Constitution. This right can only be limited in accordance with the law.[254]

The right to privacy in the employment context has dealt with the following provisions of the Constitution. The Constitutional Court and labour court cases in relation to privacy rights have dealt with the monitoring of employee telephone conversations, use of video cameras and the processes involved in storage of employee personal information.[255] They are as follows:[256]

a) Protection of human dignity.

- Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority.

[251] Ibid 83

[252] Ibid

[253] Ibid

[254] Ibid

[255] Ibid

[256] Ibid 84

b) Rights of liberty.

- In terms of [Article 2(1)], everyone shall have the right to the free development of his personality in so far as it does not violate the rights of others or offend against the constitutional order or the moral code. Everyone shall have the right to life and to inviolability of their person. The liberty of the individual shall be inviolable. These rights may only be encroached upon pursuant to law [Article 2(2)].[257]

c) Restrictions of basic rights.

- Insofar as a basic right may, under this Basic Law, be restricted by or pursuant to a law, such law must apply generally and not solely to an individual case.[258]

Any employer who allows employees the private use of Internet in the workplace will be regarded as someone who "commercially provides or assists in the provision of telecommunications services".[259] In terms of Section 85(2) of the Telecommunications Act of 25 July 1996 (hereafter referred to as the Telecommunications Act), an employer is obliged to maintain telecommunications secrecy. Section 3(16) of the Telecommunications Act defines telecommunications as, "the technical process of sending, transmitting and receiving any kind of message in the form of signs, voice, images or sounds by means of telecommunications systems".[260]

This significance of this definition is that it brings the private use of Internet within the scope of applicability of the Act. In terms of the Act, an employer who grants his employee's access to the Internet is regarded as someone who provides this telecommunication service commercially.[261]

[257] Ibid

[258] Ibid

[259] Ibid

[260] Ibid

[261] Ibid

Where the employer does not allow any private use of Internet by employees the Telecommunications Act will not apply. This is because there is no 'offer' of telecommunications.[262] The processing of personal data will be subject to the Federal Data Protection Act *(Bundesdatenschutzgesetz)*. In terms of the Federal Data Protection Act all the collecting and recording of data that relates to phone calls of employees amounts to the processing of personal data in the sense of section 3 (1).[263] In terms of section 4(1) of that Act, the processing and use of personal data will only be admissible if this Act or any other legal provision permits or prescribes them or if the person concerned has consented. The scope of this section has recently been extended by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 which relates specifically to the protection of individuals personal information.[264]

It has become a popular notion amongst German writers that, technically, e-mailing comes close to telephoning. Due to the similar conditions of electronic transmission in respect of the telephone and e- mails it seems justified in principle for the same arguments to be raised with telephonic information and the use of e- mails.[265] The result of this is that for employees to be able to use e-mails for private purposes the permission of the employer is required. However if there is an existing permission concerning private phoning it can be extended to the use of e-mails.[266] In terms of section 87 (1), no. 6 of the Works Constitution Act the introduction and running of any monitoring equipment is subject to prior consent of the works council. Besides these requirements any monitoring of e- mails has to be brought in line with restrictive case law on informational privacy.[267]

In terms of this approach, monitoring is only permissible when there is a belief that there is

[262] Ibid 88-90

[263] Ibid

[264] Ibid

[265] Ibid 90

[266] Ibid

[267] Ibid

unlawful behavior by employees in the form of sexual harassment through the use of messages, disclosure of trade secrets or a prospect of unlawful competition.[268]

In principle, employees face the same conditions and restrictions with regard to other services of the Internet, especially to the visiting of websites within the "www" facilities.[269]

In terms of German law, if employees make private telephone calls in the workplace when this has been forbidden, then this violation could lead to dismissal which would have been preceded by a warning *(Abmahnung)*.[270] If private calls are to be permitted then the employment contract will stipulate time restrictions for the duration of the calls and whether such calls must be local.[271]

The German Works Constitution Act section 87 (1), no. 6, provides for a compulsory co – determination process. This would apply in cases where there has been an introduction of new technical equipment that is specifically designed to control the behaviour or the performances of employees.[272] This section would apply to telephone monitoring systems. Any monitoring device concerning e- mails will be subject to the same restriction.[273]

In principle, German law regards any monitoring of employee's behaviour in the workplace by hidden video cameras as "an attack on the right to privacy".[274] It is important to note that in certain instance German courts will permit so – called spying on employees. This would normally arise where there is a serious breach of contract, if an unlawful act has been perpetrated or if there are no

[268] Ibid 90- 91

[269] Ibid 91

[270] Ibid 91-92

[271] Ibid

[272] Ibid

[273] Ibid 91-92

[274] Ibid

other means to identify the author of such a crime.[275]

The German model is interpreted as providing extensive protection of workplace privacy. The employer can only lawfully interfere with an employee's personality right if permitted by legislation, collective agreement or the company works council.

4. ITALY

In Italy the most important legal document that governs labour management relationships and regulates the use and monitoring of e-mail in the workplace is the Data Protection Act and the Employees' Statute (Act 30 May 1970 No. 300).[276] This Act contains rules and provisions aimed at protecting the freedom and dignity of employees and the freedom of trade unions and of their activity at the workplace.[277]

Article 4, paragraph 1, states:
"It shall be unlawful to use video cameras and other equipment for the remote monitoring of employees' activity".[278]

The principle that shaped the statute was the view that an employee is a human being whose rights should be protected in the workplace and not the view that an employee is merely someone obliged to perform a job.[279] The right to dignity in the workplace encompasses freedom of expression, autonomy and freedom from control by unidentified, impersonal objects. The statute affirms that all discriminatory practices are unlawful.[280] The statute ensures the equal treatment within the

[275] Ibid 93

[276] Ibid

[277] Ibid 113

[278] Ibid

[279] Ibid 113 -114

[280] Ibid

workplace through the identification of discriminatory practices and other anti discriminatory practices. Article 4, paragraph 2 of the above mentioned Act refers, to "control equipment and appliances required for organizational and productive reasons or for work safety but which could be used for the remote monitoring of employees…". This equipment referred to above "may be installed only after obtaining the agreement of the trade union delegations or, failing this, of one of the works councils".[281] In terms of the nature of this provision it is essential that all employees are involved in the agreements of the particular organization within which they are employed.[282]

In terms of article 26 of Workers' Statute, it is permissible during working hours to promote union activity and to advertise for new membership for a specific for trade union. In doing so, employees must be weary not to interfere with the normal activities and functions of the employer.[283] This has been interpreted to mean that any of the activity of an employee as the one mentioned above, must be carried on only during breaks. In the same sense, Italian courts have permitted the use of a telephone if the workplace is without a public telephone point and if the employee does not abuse the permission.[284]

In light of the above it is plausible to conclude that using computer facilities would be considered legal if it is used for communicating to other colleagues as well as to other people, (provided that the use of the computer facilities does not become excessive) for promoting union activity provided that such takes place during the break period.[285] Conversely, it would be plausible to conclude that it is unlawful to use any electronic communication equipment for leisure or for private business.[286] An exception to the rule would be written or oral permission granted by an employer. An Italian judge has held that, in a case where the unlimited use (of the telephone) by the employees constitutes a deeply rooted practice known by the employer, that has to be

[281] Ibid

[282] Ibid

[283] Ibid 121

[284] Ibid

[285] Ibid

[286] Ibid

considered as a permission per *facta concludentia*.[287]

An infringement of employer property rights by the employee does not give an employer an inalienable right to monitor the activity of the employee, or listen to a conversation, or read the contents of a message.[288] If however, the use of telephone or e- mails is abusive or excessive and when the employer experiences losses or damages because of this, monitoring by the employer may be permissible with subsequent dismissal a real possibility for the guilty employee.[289]

In light of the above, it can be noted that Italian law on surveillance and monitoring of employees involves a human element and must not be as anonymous or inflexible as to prevent independence of the employees' performance. Italian law provides that supervision must be directly related to the tasks required of the employee and must be proportional to the nature and importance of those tasks. The Trade union representatives have an important function in providing assurance that these limits are observed by the employer by playing an active role in the decision – making concerning techniques of monitoring.[290]

5. France

There is no explicit right to privacy mentioned in the French Constitution. The preamble to the Constitution of 1946 does however provide that no employee may be discriminated against because of origin or beliefs.[291] The Civil Code (section 9) does provide for a general right to privacy while the Penal Code provides for the secrecy of letters (section 187) and the confidentiality of speech and pictures (section 368).[292] There is also no references to the Internet

[287] Ibid

[288] Ibid 121-122

[289] Ibid

[290] Ibid 122

[291] ILO, *Conditions of Work Digest,* Vol. 12, 1/1993, p. 15, cited in Colucci op cit note 92, 73

[292] Ibid

and new technologies of information and communication within The French Constitution. However, a statute, called the Computer Science and Freedom Act, was adopted as early as 6 January 1978, whose consent largely inspired the EU directive of 23 November 1995.[293]

Section 1 of the Computer Science and Freedom Act states, "computer science must be in the service of each citizen" and further that "It must not undermine either human identity, human rights, privacy or individual and public freedoms". Section 3 of the Act provides that "every person has the right to know and to challenge information and thought processes used into data processing with which results he can be confronted". Section 25 adds that "data collection carried out by any fraudulent, disloyal or unlawful means is forbidden". A punishment of a maximum of five years in jail and a fine of two million Francs is imposed by section 226- 18 of the new Penal code while eight other sections also penalise "attacks against the rights of the person resulting from computerised data processing". [294]

Since 1970 article 9 of the French Civil Code provides that: "everyone has a right to respect for their private life". This provision is also deemed applicable to an employment relationship.[295] The debate that has emerged in recent times is whether a right to privacy can be effective in the employment relationship since the employee is in a subordinate relationship with the employer.[296]

The French Labour Code has been interpreted to provide for monitoring and surveillance of employees. As general principle, article L. 120- 2 of the Labour Code states that:

"Nobody may limit the rights of the individual unless the limitation in question is justified

[293] Commission Directive 94/46EC of 13 October 1994 amending Directive 88/301/EEC and Directive 90/388/ EEC in particular with regard to satellite communications, O.J.L 268, 19/10/1994, pp. 15-21., cited in Colucci op cit note 92, 73

[294] J.E. Ray and J Rojot, "On line Rights and Obligations of Workers: E- Mail Surfing", *Bulletin of Comparative Labour Law and Industrial Relations,* No. 40, 2001, Kluwer Law International, cited in Colucci op cit note 92, 73

[295] J. Savatier: " Informatique et libertes : Les nouveaux enjeux" (Computer Science and Freedom: The New Concerns), *Droit Social*, No. 1 , January 1990, p. 57; *Alme Rossard v. Ste. Rebuchon et Fils*, Court of Cassation , Social Chamber, 22 January 1992 , in J. Savatier : " La protection de la vie privee des salaries" , *Droit Social* , No .4 , April 1992 , p .334, cited in Colucci op cit note 92, 74

[296] G. Lyon- Caen: Les libertes publiques et l'emploi- Rapport sur le Travail, l' Emploi et sur la Formation Professionnelle (Paris, Documentation Francaise, December 1991), p. 147, cited in Colucci op cit note 92, 74

and proportionate to the desired aim of the measure of practice in question".

In terms of the article, employees must be made aware of the existence of surveillance equipment that is used by their employer.[297] The article makes it unlawful for an employer to implement any method of obtaining information concerning employees without informing the employees of the method to be used to obtain that information.[298] As a result it is illegal for an employer to monitor an employee's online activities whilst at work without first bringing this to their attention. An employer must provide proper justification for an intrusion into the privacy of an employee.[299] In order to be justified, the practice in question must be both relevant to the tasks performed by employees and proportionate to the objective purpose of the measure.[300]

In the case of *Ministre du Travail v. Societe Peintures Corona* [1980] 6 Dr. Soc. 317, the court made it clear that economic considerations alone are not enough to deprive employees of their right to privacy.[301] The question as to whether the employees have consented to such invasive monitoring is irrelevant. In the Noecel case, the *court de Cassation* affirmed that article 9 of the Civil Code prohibits the use of surreptitious surveillance devices in the workplace. Thus employers cannot dismiss employees on the basis of information obtained through unlawful surveillance. [302]

The French Penal Code

The French Penal Code protects employees against video camera surveillance, telephone

[297] Colucci op cit note 109, 75

[298] Ibid

[299] Ibid

[300] Ibid

[301] Ibid

[302] Ibid

monitoring and other types of recording of conversation in the workplace.[303] There is punishment in the form of imprisonment for a period of two months to a year, or a fine of 2000 to 6000 French francs, or both, for anyone who voluntarily causes prejudice to the privacy of someone else by:[304]

a. listening to, recording and / or transmitting , by means of a device , the speech of a person in a private place without the consent of the concerned person;
b. recording and/ or transmitting, by means of a device, the picture of a person who is in a private place without the person's consent (section 369).

Section 368 of the Penal Code has been applied to the employment relationship in cases where there has been recordings of speeches and telephone tapping and monitoring.[305] For example, the Tribunal de Grande Instance of Saint - Etienne applied section 368 to sanction an employer who had installed a device in the canteen to record conversation of employees. On the same topic the Court of Appeals of Paris ruled that private conversations between employees which were recorded on a cassette and disclosed to all employees of the undertaking by the employer was contrary to section 368 of the Penal Code.[306]

The Secrecy of Correspondence with regard to e- mails in the workplace

According to section 226-15 of the Penal Code a maximum jail term of one year and a fine of 300,000 Francs is imposed for: "The fact perpetrated in bad faith to open, suppress, delay or divert correspondence, whether delivered or not, or to read them with fraud". [307] The term correspondence in this context refers to any written relation existing between two identifiable persons, whether it be in the form of letters or messages that were in closed or open envelopes.[308]

[303] Ibid 76

[304] Ibid

[305] Tribunal de Grande Instance of Saint Etienne, case 19 April 1977, mentioned in Savatier, "La liberte dans le travail", p 58, cited in Colucci op cit note 109, 75

[306] Ibid

[307] Ray and Rojot op cit note 203, cited in Colucci op cit note 109, 78

[308] Ibid

The fact that the correspondence are aimed specifically between two people and not the public at large is the reason why French law seeks to protect this relation.[309] In a specific case, a female student working at one of the laboratories of the university had complained of being harassment via e- mail. A Kuwaiti visiting doctoral student whose volume of e- mail was abnormally high was considered the prime suspect. His mailbox was subsequently monitored and messages opened by The Director of the Laboratory, the system engineer and the Webmaster. They subsequently discovered that 90 percent of his e -mails were of a private nature as well as derogatory to the Laboratory. The student was later expelled on these grounds. The student sued the University on the basis of section 226-15. The Court fined the Director of the Laboratory, the system engineer and the Webmaster between 5, 000 and 10,000 FF as well as to 10, 000 damages.[310]

From the above it has become apparent that European countries accord a better measure of protection to the employees' right to privacy in the workplace than the US. The right to workplace privacy is derived from numerous EU directives on data protection and telecommunications. The general rule is that monitoring is only permissible with consent and in circumstances of necessity.[311]

[309] Ibid

[310] Ibid

[311] D Collier "Workplace Privacy in the Cyberage". (2002) 23 *ILJ* 1756

CHAPTER 3

An analysis of South African legislation as it applies to the Monitoring of Electronic Communications in the Workplace

Surveillance and monitoring of communications ('wiretapping' or 'bugging') is conducted in nearly every country in the world by governments and private groups, for a range of reasons. The most common form of surveillance is the wiretap on a standard telephone system. Surveillance and monitoring techniques have no extended beyond the telephone wiretap to more modern and innovative methods of monitoring individuals.[312] Since 11 September 2001, wiretap laws around the world have been amended to expand their scope and applicability.[313]

It is clear that employees do not abandon all privacy rights when they enter the workplace. Employees are vital for the success and sustainability of any organisation, therefore they are entitled to respect, which entails some measure of privacy.

The problems that employers face due to the abuse of their company resources are immense. The overuse of an employer's resources has a negative impact on the working environment. For instance the use of these resources consume employees' working time, and have the potential to pollute and congest computer space not to mention cost the company exorbitant amounts of money.[314] Uncontrolled and irresponsible internet usage also exposes computer systems to the ever present danger of computer viruses that may damage and destroy the company equipment.[315] Employer's also have the legitimate concern of the overloading of network servers and the forwarding of unsavoury messages that may be associated with the employer's brand or domain

[312] T Cohen : The Regulation of Interception of Communications and Provisions of Communication-related Information Act, No. 70 of 2002 *ISPA Advisory 10* February 2003.

[313] Ibid

[314] Ibid

[315] C Mischke "Workplace Privacy, e- mail interception and the law". (2003) 12 (8) *CLL* 72

name. The use of e-mail may also be used to transmit anonymous communications which are offensive or insulting to employees. [316]

The South African law on surveillance was first significantly amended in 1992. This was done to increase individual privacy protections: the *Interception and Monitoring Prohibition Act* (No. 127 of1992) focused primarily on telephonic and postal communications.[317] The South African Law Project (SALC), Project 105, November 1998 sought to review old apartheid security laws decided to prioritize the investigation into interception and monitoring of communications for crime investigation and intelligence gathering purposes, and to extend its ambit from just telephones and postal articles to include all communications networks.[318]

The law reform process was further impacted upon by the Council of Europe Convention on Cybercrime (COE). South Africa is one of four non-member signatories to that convention and as such, is required to develop certain measures in accordance with that agreement.[319]

The COE Convention is the first international treaty on crimes committed using the Internet and other computer networks, dealing particularly with infringements of copyright, computer related fraud, child pornography and violations of network security.[320] The Convention also contains powers and procedures for the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime. This is achieved by adopting appropriate legislation and promoting international co-operation.[321]

---

[316] J Grogan "Workplace Privacy: controlling communications abuse". (2004) 20 (2) *EL* 9

[317] Cohen op cit note 1 , 1-2

[318] Ibid

[319] Ibid 2

[320] Ibid

[321] Ibid 2-3

Two pieces of legislation govern the impact and use of the Internet in the workplace.

The following is a discussion of the relevant sections of the Electronic Communications and Transmissions Act 25 of 2002 (ECTA) and the Regulation of Interception of Communications and Provision of Communication – Related Information Act No 70 of 2002 (RICPCIA).

The Electronic Communications and Transmissions Act 25 of 2002 (hereafter referred to as the ECTA) came into force on 30 August 2002. The purpose of the ECTA is to address issues, such as the formulation of a national electronic communication strategy, the promotion of universal access to electronic communications and the encouragement of e- government services.[322] The are however, a number of provisions that may, directly or indirectly, impact on the use of e- mail and internet communications in the workplace.[323]

The Electronic Communications and Transmissions Act (ECTA) and the law relating to the time of electronic contracting.

The nature of the Internet is such that it enables employers in the form of corporate entities to communicate and transact in ways that were not previously possible. This is so, because electronic contracts improve business efficiency and reduce administrative activities in the form of files of paperwork.[324] The Internet does pose new challenges to employers. The challenges that arise are those that stem from the fact that due to the nature of the medium less information is known about the recipient. This is a considerable risk since there is real possibility that the recipient may be harbouring ulterior motives.[325]

The law of contract was formed for contracts that involved pen and paper. It was never intended to

[322] T Pistorius " From snail to e- mail- a South African perspective on the web of conflicting rules on the time of e-contracting". (2006) 39 (2) *CILSA* 182

[323] Ibid

[324] J Coetzee, "The Electronic Communications and Transaction Act 25 of 2002: facilitating electronic commerce". (2004) 15 (3) *Stell LR* 501

[325] Ibid

cater for contracts that would be concluded in cyberspace.[326] Thus the use of electronic communications for commercial purposes posed complex legal problems for both companies and their clients. This problem was not unique to South Africa but experienced internationally by all those concerned with the digital economy.[327]

The common law rules that were used for paper based contracts, more specifically the law that deals with the time when such contracts were formed cannot be applied to determine the time of electronic contract formation.[328] The normal determination of the time of communication as being either 'instantaneousness' or 'non- instantaneousness' to determine the instance when an electronic contract is formed is outdated. If one is to use the rules of paper based contracts and their formulation then the expediency of electronic commerce transactions is defeated.[329]

The United Nations Commission on International Trade Law established a group to formulate rules with regard to electronic commerce. The result was The UNCITRAL Model Law on Electronic Commerce adopted on 12 June 1996.[330] The UNCITRAL Model Law on Electronic Commerce provided solutions for online contracting and set the foundations for most electronic laws in other jurisdictions.[331] Although the crucial aspect of the time of electronic contract formation remained undecided, the fundamental principles on the legal recognition and validity of data messages and electronic contracts have been adopted.[332]

Despite the fact that The UNCITRAL Model Law on Electronic Commerce has no binding effect on international law. The Model Law has however helped shape the e- commerce legislation

[326] Ibid

[327] Coetzee op cit note 13, 511

[328] Pistorius op cit note 11, 178 -179

[329] Ibid

[330] Ibid

[331] Pistorius op cit note 11, 179

[332] Ibid

adopted in many countries.[333]

South Africa adopted the ECT Act. The overall objective of the ECT Act[334] (hereafter referred to as the Act) is to enable and facilitate electronic transactions and to create public confidence in electronic transacting.[335]

The Act seeks to promote e- commerce in South Africa by formulating practical rules for electronic contracting. The Act also seeks to provide legal certainty by granting recognition to data messages. Another objective of the Act is to provide protection of individuals through consumer protection. The Act provides for measures to be taken against illegal activities and enforcement facilitated by the creation of new cyber offences and provides for functions and powers of cyber inspectors.[336]

Section 4 (2) of the Act provides that the Act must not be construed as requiring any person to generate , communicate, produce, process, send, receive, record, retain, store or display any information , document or signature by or in electronic form.[337] The Act provides for the legal recognition of data messages and the requirements of writing, signature, and contract formation may be met by data messages. Section 3 is important in that it confirms that the Act applies to the common law as well as all legislation except where the application of the Act is specifically excluded. [338]

Electronic communication methods makes the determination of the time and place of transmission and receipt of data messages difficult to determine. Therefore certain rules must be put in place to

[333] Coetzee op cit note 13, 512-513

[334] Electronic Transactions Act 25 of 2002

[335] Pistorius op cit note 11, 182

[336] Ibid

[337] Act 25 of 2002; s 4 (2)

[338] Act 25 of 2002; s 3

determine the time and place of dispatch and receipt of electronic communications.[339] The reason for these rules are simple: whether a contract becomes effective when the acceptance is sent or received, the law must provide certainty as to when a data message may be deemed sent and received in the electronic world.[340]

The Act provides clear rules for the time and place that the dispatch and receipt of data messages becomes effective. The Act makes provision for the time an electronic contract is concluded.[341]

The Act stipulates that a data message enters an information system at the time when it becomes available for processing within that information system.[342] Attention is drawn to the meaning of 'entry' into an information system, which is used to define when dispatch and receipt of a data message becomes effective. In terms of the Act unless the message is complete and intact, receipt of the data message cannot be said to have taken place.[343]

In South Africa the ECT Act[344] adopted the reception theory for electronic contract formation.[345] Section 22 (2) of the ECT Act[346] adopts a specific rule for the formation of an electronic contract. It provides that an agreement concluded between parties by means of data messages is concluded when the acceptance of the offer is received by the offeror.[347] The Act provides that the reception theory offers an effective and realistic solution to the problems that arise due to consensus and long distance contracts. In terms of the reception theory the electronic contract will cone into existence

[339] Ibid 186

[340] Ibid

[341] Ibid 184

[342] Ibid 190

[343] Ibid

[344] Electronic Transactions Act 25 of 2002

[345] Pistorius op cit note 11, 207

[346] Act 25 of 2002; s 22 (2)

[347] Pistorius op cit note 11, 207

at the time the acceptance is deemed to be received by the offeror.[348] This section of the Act removes the factual uncertainties around subjective knowledge of an acceptance. [349]

A criticism raised against the provisions of the ECT Act[350] on the time of contract formation is that the provision is not technically neutral. A data message is deemed to be sent when it enters an information system outside the control of the sender. It is deemed to be received when the complete data message enters an information system designated by the receiver or used for that purpose by the receiver.[351] It is obviously important that the message reach the intended recipient intact and complete. If the message is not received intact, it is thus ineffectual and no contract comes into being. Pistorius[352] submits that the effectiveness of an illegible record, and whether and to what extent it binds any party, should be dealt with by the general principles of law. It is by submitted Pistorius that "It is an established legal principle that the question whether the message is legible is a separate issue from whether the record was received. The intelligibility or usability of a record should be irrelevant , let alone a determining factor , in determining whether a record may have been deemed to have been received or not, or whether a contract was concluded or not".[353]

Section 1 of the ECTA[354] defines 'data' in wide terms as being, "electronic representations of information in any form", and both e- mail messages and other forms of internet information constitute electronic representations of information.[355]

---

[348] Pistorius op cit note 11, 178-213

[349] Ibid

[350] Act 25 of 2002

[351] Pistorius op cit note 11, 178-213

[352] Ibid

[353] Ibid 208

[354] Act 25 of 2002; s 12

[355] Act 25 of 2002

Section 12 of ECTA[356] provides that if there is a legal requirement that a document or information must be in writing, the requirement will be met if the document or the information must be in writing, the requirement will be met if the document or the information is in the form of a data message and it is accessible in a manner usable for subsequent reference.[357] A 'data' message means data generated, sent, received or stored by electronic means and includes voice – data (where the voice is used in an automated transaction) and a stored record.[358]

Section 13 of the ECTA[359] provides that if a signature is required by law and there is no specification of the type of signature, an advanced electronic signature will meet the requirement. Section 13 (2) provides that an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.[360]

Section 15 of the Act relates to the admissibility and evidential weight of data messages[361] – the rules of evidence must not be applied so as to deny the admissibility of a data message only because it is not in its original form.[362]
Section 22 of the Act provides that an agreement is not without legal force and effect solely on the basis that it was concluded partly or wholly by means of data messages. An agreement concluded between parties by means of data messages is concluded at the time when, and place where, the acceptance of the offer was received by the offeror.[363]

[356] Act 25 of 2002

[357] Act 25 of 2002; s12

[358] Mischke op cit note 3, 76

[359] Act 25 of 2002

[360] Act 25 of 2002; s 13 (1) & 13 (2)

[361] Act 25 of 2002; s 15

[362] Mischke op cit note 3, 76

[363] Act 25 of 2002; s 22

The ECTA and Consumer Protection.

The Internet does offer exciting new opportunities. This is achieved by transforming the way companies and other organisations conduct their businesses, it has also provided the means to gather electronic mail and to distribute them expeditiously with little to no cost.[364] Unsolicited e-mail commonly referred to as spam, refers to an e-mail message that is transmitted to a large number of recipients who have not requested those messages, and do want them. Spam is usually some sort of advertising, inappropriately sent to a mailing list or newsgroup.[365] The first major commercial spamming is said to have occurred in 1994, when two lawyers posted a message advertising their services to several thousand newsgroups on USENET, the world's largest online conferencing system. Spam not only wastes the recipient's time, but also misuses the network bandwidth.[366]

Junk e- mail is undesirable to employers for the following reasons:[367]

- Unsolicited messages lead to the users spending a considerable amount of time reading messages, thus, in turn, causing them to stay on line longer and incur further expense.
- The messages may cause the employer's e- mail server to malfunction due to congestion and potentially prevent important business mail from reaching the intended recipients.
- The messages may be sent with a fraudulent purpose. Numerous Internet businesses that send junk e- mail spoof (i.e. forge) their e-mail headings.
- The messages cause great concern to employers because these messages mean a loss of productivity due to the time spent by employees perusing or reading their mail.

Section 45 deals with 'unsolicited communications', which are defined as 'communication by means of data messages'. Section 45 (1) provides that:[368]

---

[364] Pistorius op cit note 11, 178-213

[365] S Gereda "The Truth about Spam". September (2003) De *Rebus* 51[see generally W Jacobs "The Electronic Communications Act: Consumer Protection and Internet Contracts". (2004) 16 *SA Merc LJ*]

[366] Ibid

[367] G Ebersohn "The unfair business practices of spamming and spoofing". July (2003) *De Rebus* 26

[368] Act 25 of 2002; s 45

(1) Any person who sends unsolicited commercial communications to consumers, must provide the consumer:
(a) with the option to cancel his or her subscription to the mailing list of that person; and
(b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.

Section 45 (2) provides that no agreement is concluded where a consumer has failed to respond to an unsolicited communication.
Section 45 (3) and (4) criminalizes the following conduct:[369]
3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89 (1).
(4) Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89 (1).

Gerrie Ebersohn believes with the recent developments in America , Australia and Europe , S.A legislators should seek to amend the Electronic Communications and Transactions Act 25 of 2002 (ECT Act) in order to bring in to line with international best practices.[370]

Spam undermines two of the advantages of e- mail that is, low cost and convenient communication). The reason being is that the recipient of spam incurs costs in downloading, reviewing and deleting unwanted spam.[371] The activating of spoofing on the other hand, Ebersohn, believes impinges on the internet user's trust in the internet because they cannot rely on or trust the sender's e- mail address. Furthermore, the amendment of the ECT Act will help prevent spam becoming the method of choice for those who wish to distribute pornography, perpetuate fraudulent schemes, or introduce malicious viruses onto computer programs.[372]

[369] Act 25 of 2002; s 45 (3) & 45 (4)

[370] G Ebersohn "An analysis of spam legislation". (2004) 12 (3) *JBL* 137

[371] Ibid

[372] Ibid 141- 142

Ebersohn suggests the ECT Act especially s 45 should be amended to provide for the following:[373]

- More attention must be paid on how spammers have obtained the recipients e- mail address. If this is done it will create an environment of transparency and curb the activities of spammers.
- Spammers should be prevented from using false and misleading e- mail headers, referring to both the subject matter as well as the sender's e- mail address and disguising the origin of the e- mail.
- People who send e-mail should be compelled to indicate that their e-mails contain advertisements by using an abbreviation such 'ADV', an abbreviation for an advertisement. Similar practice should be adopted for those who wish to send pornographic material. This would thus enable a recipient of these types of e- mails to activate filtering software to block these e- mails without having to search through them on their own.
- Stiffer penalties should be adopted to for those who contravene the amended provisions of the ECT Act. For instance some American states such as Illinois, North Carolina, Oklahoma, Rhode Island and Virginia provides from criminal penalties of US$ 10 per spam message up to a maximum of US$ 25 000 per day.
- Currently, the ECT Act only protects Internet users against spam, provisions of the ECT Act need to be amended to protect Internet Service Providers (ISP's) because their computer resources are usurped by spam.
- The Australian approach creating civil liability for sending spam and using harvested e-mail addresses is plausible and should be investigated and perhaps adopted in South Africa.
- The South African government should regularly review spam legislation. The Australian and American spam legislation mandate legislatures to regularly review spam legislation.

Failure to curb spam and spoofing undermine consumer confidence and the viability of the Internet as a medium of communication.

[373] Ibid 142

ECTA and Cyber protection

Chapter XIII of the Act is of importance. This chapter relates to the issue of cyber crime. Section 86 of the Act states that, subject to the provisions of the Regulation of Interception of Communications and Provision of Communication related Information Act 70 of 2002 (hereafter referred to as the RICPCIA), a person who intentionally accesses or intercepts any data without the authority or permission to do so, is guilty of an offence.[374] The effect of this provision is such that, unless the employer complies with the RICPCIA[375] or has authority or permission to do so, its interception or accessing of electronic data would constitute a criminal offence.[376]

In terms of section 86 of the ECTA[377], the following also constitutes criminal offences.

- The intentional and unauthorised interference with data resulting in a modification , destruction or rendering ineffective of the data; [378]
- The production , sale, design or adaptation of devices primarily to overcome security measures; [379]
- Unauthorised access (that is, unlawfully overcoming security measures designed to protect data, or hacking into a system); [380] and
- The denial of service offences (that is, committing acts with the intent to interfere with access to a system so as to constitute a denial, including a partial denial, of service legitimate to users).[381]

Section 89 provides that the maximum penalty for a contravention of s 86 of the Act is a fine or

[374] Act 25 of 2002; s 86 (1)

[375] Act 70 of 2002

[376] Mischke op cit note 3, 76

[377] Act 25 of 2002

[378] Act 25 of 2002; s 86 (2)

[379]Act 25 of 2002; s 86(3)

[380] Act 25 of 2002; s 86 (4)

[381]Act 25 of 2002; s 86 (5)

imprisonment for a period of no more than 12 months.[382]

The Interception and Monitoring Prohibition Act 127 of 1992 (The Monitoring Act) is repealed and replaced by the RICPCIA. Before we look at the provisions of the RICPCIA, it is important to provide a brief study of the provisions and application of the Monitoring Act, as this Act sets the framework for the RICPCIA.

The Monitoring Act

In terms of section 2 (1) (a) of the Monitoring Act,

> *"No person shall intentionally and without the knowledge or permission of the dispatcher, intercept a communication which has been or is being or is intended to be transmitted by telephone, or in any other manner over a telecommunications line".*

The term intercept was defined in the Monitoring Act as, 'seize, catch or stop (a person, message, vehicle) from going from one place to another'.[383]

Section 8 (1) (a) of the Monitoring Act makes it an offence to contravene s 2 (1). In the event of a conviction, the penalty is a fine or imprisonment for a period not exceeding two years.

In terms of the provisions of s 2 (1) (a) of the Monitoring Act, person may, with the knowledge or permission, of the dispatcher, intercept a communication. The term dispatcher is not defined in the Act, it therefore bears its ordinary meaning, and would be synonymous with 'sender'.

Section 3 of this Act limited the application for a directive in terms of s 2(2) to be made by certain persons only, including members of the SA Police Service, the SA Defence Force and the Intelligence Services.

---

[382] Act 25 of 2002; s 89 (1)

[383] The *Oxford minireference Dictionary & Thesaurus*. Ed. S Hawker & C Cowly.(1997)

Other than these provisions this Act did not make provision for the interception and monitoring of communications and conversations.

I will look briefly at the application of the Monitoring Act by South African courts.

In the case of *Van Wyk Independent Newspapers Gauteng (Pty) Ltd and others* (2005) 26 ILJ 2433 (LC); the applicant employee, the chief sub-editor of the *Pretoria News* , had a heated argument with her editor, the deputy editor, her superior and a back desk editor while on night duty one evening. The applicant then sent out a series of e- mails to colleagues and managers to which her superiors took exception.

The applicant was dismissed after she was found guilty of the following charges which were levelled against her:[384]

1. *"Gross misconduct in that you on 10 May 2001, sent an e-mail to staff and management containing allegations which are of a malicious nature with the intention of undermining the authority of senior management.*
2. *Gross misconduct in that you in an e-mail dated 11 May 2001 made derogatory statements about the editor and deputy chief editor of the Pretoria News. "*

At the Arbitration proceedings the employee contended that the dismissal had been too harsh a sanction.[385] The arbitrator found that the employee had acted without malice but irrationally and had displayed bad judgment. The arbitrator found that the both the managing director and the editor had every right to feel insulted by the first e-mail.[386] The arbitrator held that the argument that the second e-mail was inadmissible to be without substance as it had been sent to a communal computer which was the property of the first respondent. He found the dismissal to be

[384] *Van Wyk Independent Newspapers Gauteng (Pty) Ltd and others* (2005) 26 ILJ 2433 (LC) at 2435 G-H & 2436 para 5

[385] supra note 73, at 2437 C

[386] supra note 73, at 2437 D

substantively and procedurally fair.[387]

Insofar as the review application was concerned, the applicant relied on the Interception and Monitoring Prohibition Act 127 of 1992 (The Monitoring Act). It was argued on the basis of this Act, that it was prohibited for the arbitrator to have any regard to the e-mail.[388]

The court was unable to accept the employee's reliance on the Interception and Monitoring Prohibition Act. Firstly, because it was not raised before the arbitrator and secondly, the first respondent's information technology usage policy specifically cautioned employees not to assume that e-mails would not be read by other persons.[389]

The court held that very few employers will tolerate this type of behaviour from their subordinates. Therefore the court found that the decision reached by the arbitrator was not irrational and that the decision reached was connected to the evidence before him. The application before the court was dismissed.[390]

In *S v Kidson* 1999 (1) SACR 338 (W) a private individual had been fitted with a tape recorder by the police prior to attending a meeting with a third party . The conversation was recorded and was used as evidence against the third party, who was unaware that the conversation was being recorded. Kidson, the accused, sought to have the recording excluded on the ground that the monitoring contravened the Monitoring Act. The court held that the Monitoring Act was a criminal statue, and must be narrowly interpreted. The court held that the legislature's primary purpose was to 'protect' confidential information from 'illicit eaves- dropping'.[391] The court held what was prohibited is 'the conduct of third person acting in relation to a conversation between others'[392]

[387] supra note 73, at 2437 E-G

[388] supra note 73, a 2437 para 13

[389] supra note 73 , at 2438 para 17

[390] supra note 73, at 2440 A-B

[391] *S v Kidson* 1999 (1) SACR 338 (W), at 344 f.

[392] supra note 80, at 344 H-I

and not that of a person monitoring a conversation in which he or she takes part. It is not necessary the court held, for a person in these circumstances to apply for authority to conduct the recording 'because the monitoring they are most likely to engage in, namely participant monitoring, is not prohibited at all'.[393]

The court in this case also considered whether in such circumstances it could be said that the monitoring was to gather 'confidential' information. The court concluded that confidentiality implies that the information in question is 'confided' to another person, namely that some burden or duty rests on the person to whom the information is communicated. On the facts of the case, the court concluded that the information imparted in the two – way conversation about the communicator's (accused) own criminal conduct , was not ' confidential information' in relation to the other party, and that the participant monitoring was for that reason also prohibited.[394]

In the case of *Tap Wine Trading CC and another v Cape Classic Wines (Western Cape) CC and another* 1999 (4) SA 194 (C), a telephone conversation had been recorded 'at the instance of one of the parties'. The court held that this constituted participant electronic surveillance (that is, the surveillance was consented to by one of the parties to the conversation) which is not in contravention of the Monitoring Act and did not breach any constitutional right to privacy.[395]

In *S v Dube* 2002 (2) SA 586 (N), a private investigator acting on behalf of Toyota SA had arranged a meeting between himself and the accused at which the accused had made certain statements relating to stolen vehicles. The investigator had tape recorded the conversation and had arranged for a photographer surreptitiously to take pictures of the meeting. The court concluded, consistently with *S v Kidson*[396] and *Tap Wine Trading CC*[397] that the investigator's conduct in making the recording amounted to participant monitoring, which is not prohibited by the

[393] supra note 80, at 346 F-G

[394] supra note 80, at 347E- 348D

[395] *Tap Wine Trading CC and another v Cape Classic Wines (Western Cape) CC and another* 1999 (4) SA 194 (C), at 197 A-G

[396] supra note 80

[397] supra note 84

Monitoring Act.[398] The court held further that the information obtained at the meeting did not have the attribute of confidentiality.[399]

The cases above relate to employer – employee cases where the interception and monitoring forms part of an investigation being conducted by the employer into the conduct of the employee. It is clear that the Monitoring Act prohibits third party surveillance but not participant surveillance. [400]

The Regulation of Interception of Communications Related Information Act

It must be noted that the RICPCIA[401] is not just simply an updated version of the 1992 Act. Even though the basic structure of both the Acts are similar, the 2002 Act's provisions are different in a number of respects.[402]

The Interception Act applies to a wide range of issues, including the regulation of the interception of certain communications, the monitoring of signals and radio frequencies /spectrums, the provision of certain communication related information, the issuing of directions authorising the interception of communications and the provision of communication related information, entry warrants by law enforcement officers, reporting loss of SIM cards and cell phones etc.[403]

Important definitions for present purposes include:

The word "intercept" in section 1 of the Act is defined as being:

---

[398] *S v Dube* 2002 (2) SA 586 (N) at, 610 C-E

[399] supra note 87, at 610 H-I

[400] W Beech "The Right of an Employer to Monitor Employees' Electronic Mail, Telephone Calls, Internet Usage and Other Recordings". (2005) 26 *ILJ* 654.

[401] Act 70 of 2002

[402] Mischke op cit note 3, 71

[403] Beech op cit note 89, 654

"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…"[404]

The definition of intercept also refers to an 'interception device'. An interception device is any electronic, mechanical or other instrument, device, equipment or apparatus which is used, or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to intercept any communication.[405] The definition of a 'monitoring device' in the context of interception is important. A 'monitoring device' is thus defined as being any electronic, mechanical or other instrument, device, equipment or apparatus which is used, or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication.[406]

The effect of such a definition of 'intercept' is, in essence, a wide definition – it refers to the acquisition of the contents of any communication by any means: it is not only limited to the use of interception or monitoring devices.[407]

The term 'business' means any business activity conducted by any person, including activates of any private or public body.[408]

---

[404] Act 70 of 2002; s (1).

[405]Act 70 of 2002; s (1)

[406] Act 70 of 2002; s (1)

[407] Mischke op cit note 3, 77

[408]Act 70 of 2002 ; s(1)

The term 'communication' is defined as including both direct and indirect communication. The definition of "direct communication" in section 1 relates this form of communication to actual speech and utterances between two persons who in each other's presence.[409] For present purposes the definition of "indirect communication" is of greater importance:

> *''the transfer of information, including o message or any part of a message, whether—*
> *in the form of-*
> *(ii) speech, music or other sounds;*
> *(ii) data;*
> *(iii) text;*
> *(iv) visual images, whether animated or not;*
> *(v) signals; or*
> *(vi) radio frequency spectrum; or*
> *(b) in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system . . . .'' [410]*

A party to direct communication is a direct participant. It is a person to who the communication is directed or a person who was present when such communication occurred[411]. A party to an indirect communication is the sender, recipient or intended recipient. If it is intended by the sender that such indirect communication received by more than one person, than any of those recipients is a party. It is also a person who, at the time of its occurrence, is in the immediate presence of the sender or the recipient or intended recipient of that indirect communication.[412]

The definition of indirect communication is broad, and includes a number of communications that occur through the media, telephone calls, music, visual images and data or text.[413] The implication

[409] Act 70 of 2002; s (1).

[410] Act 70 of 2002; s (1).

[411] P &K Stassen. " New Legislation" (2005) *De Rebus* 39

[412] Ibid

[413] Mischke op cit note 3, 77

of both data and text included in this form of communication means that electronic mail constitutes a form of indirect communication. In essence, an e- mail message amounts to a transfer of information in the form of data. The term 'data' is not defined in s 1 of the RICPCIA.[414]

A broadcast or transmission for general reception is not considered indirect communication that can be intercepted. Interception takes place in South Africa only if it is affected by conduct within South Africa and the communication is intercepted in the course of its occurrence or transmission by means of a postal service or telecommunication system.[415]

The time of transmission by telecommunication system includes any time when its transmissions are or were used for storing in a manner that enables the intended recipient to collect them or otherwise have access to them. The interception action must be contrary to the Act to be an offence under s 49.[416]

In terms of s 2 of the RICPCIA, it is clear that no person may intentionally acquire the contents, that is, intercept, any e- mail message in the course of that e-mail message's occurrence or transmission by using an interception or monitoring device. This also refers to indirect communication in the form of data or text.[417]

The RICPCIA does not define 'transmission' for the purposes of s 2 of the Act. It is safe to assume that the entire transmission process, from the point where a computer user clicks the send button in respect of a single e- mail message to the point where the e- mail message appears on the computer screen of the recipient is intended. There is no indication in the Act to suggest a narrower definition should be adopted.[418]

The use of the word "occurrence" is important to note. The question that arises is, does the e-mail

[414] Ibid

[415] Ibid

[416] Stassen & Stassen op cit note 100, 39

[417] Mischke op cite note 3, 77

[418] Ibid

message "occur" on the employee's individual computer or on the employer's network server? In many cases, an e- mail message is not transmitted to an individual employee's computer or stored on the hard drive of the employee's computer; the message is stored (and often remains) on the central mail- server of the employer, where that e- mail message may be accessed by any user server with access privileges to the server.[419] Any employee therefore seated at his own desk, may use Interactive Mail Access Protocol (IMAP)[420] to access the messages stored on the central mail server. In doing, so- the employee is accessing "remote" information. Using IMAP, this employee can view, delete and otherwise manipulate the e-mail messages that have been appended to his or her inbox on the shared mail server. completion of the transfer, deletes the message from the server.[421]

From the wording of s 2, it does not appear that much emphasis is placed on the word 'occur'. The scope and purport of s 2 is wide, and seeks to protect communications from interception regardless of how, when and where they are transmitted, and irrespective of where, the e- mail message is stored on the computer network.[422] It would according to Mischke[423] be safer to assume that s 2 prohibition encompasses the entire transmission process and protects the contents of the e- mail message no matter where it is situated. Where the information is located is still important with respect to who exercises control over the information, as well as for the purposes of tracking the source of information as well as their intended destination.[424]

The RICPCIA does provide for a number of ways in which the s 2 prohibition can be avoided. In terms of s 3 of the Act, an authorised person may execute an interception. An authorised person in terms of the Act is a law enforcement officer from the South African Police Service (SAPS), the

---

[419] Ibid 78

[420] Ibid

[421] Ibid

[422] Ibid

[423] Ibid

[424] Ibid

Defence Force, the Independent Communications Authority of South Africa (ICASA), the National Prosecuting authority or the National Intelligence Agency (NIA), or other person in terms of s 26.[425]

The question that subsequently arises is when an employer can intercept a communication in terms of the Interception Act. Subject to the provisions of the Interception Act, no person may intentionally intercept or attempt to intercept or authorise or procure any person to intercept or attempt to intercept any communication.[426]
This means that unless the interception is authorised in terms of the Interception Act, it is prohibited. The Interception Act authorised interception or attempted interception in a number of circumstances. Within the employment context, there are three important provisions of the Interception Act which permit the employer to intercept or attempt to intercept any communication.[427] These provisions are as follows:

Section 4 of the Act states that a party to the communication may intercept, unless such communication is intercepted to commit an offence.[428] This means that any person who is a party to the communication may intercept such communication. The term 'party' is not defined. It will therefore have its ordinary meaning, and would include the sender, the recipient, and any person to whom the communication is copied. There is also potential argument that the employer, by providing the relevant systems, is a party to any communications which are sent or received on the system.[429]

A law enforcement officer may intercept if he is a party to a communication and satisfied that reasonable grounds are present that permits such an interception. Unless such communication is intercepted to commit an offence. Section 16 (5) sets out these reasonable grounds.[430]

---

[425] Stassen & Stassen op cit note 100, 39

[426] Ibid

[427] Beech op cit note 89, 656

[428] Act 70 of 2002; s (4)

[429] Beech op cit note 89, 656

[430] Ibid

With regard to the issue of workplace privacy and the interception of communications by employers, section 5 is the most important. Section 5 of the RICPCIA relates to the interception of communications with the consent of the one of the parties to the communication. This section provides that any person may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception.[431] This may be the route that an employer will take, to secure the written prior consent of employees for the purposes of intercepting their e- mail messages and reading the contents of those messages.[432] It is important to note that the consent must be prior consent, i.e. it must be given before the interception occurs (it may of course be argued that the person may ratify the interception, after the interception has occurred, in which event any objection to the interception will fall away).[433] Secondly, the consent must be in writing. Employers will argue that, if a general consent is contained in the terms and conditions of employment (either in the contract of employment, applicable policies, practices and procedures, or some other document), this would amount to consent which complies with the provisions of s 5(1). An argument may however be raised that the words 'consent in writing to such interception' may imply consent on a case by case basis. It has been suggested, that consent given freely and voluntarily in the terms and conditions of employment would address interceptions contemplated in the consent, i.e the scope of the consent and the manner in which it is drafted require careful consideration.[434]

Unless the employer carefully sets out the scope of the consent, it may result in an argument being raised by employees that consent is not enforceable because the employee, when giving consent, could not contemplate the scope and therefore, the consent is not proper consent.[435]
It may be interesting to note that s 5 (1) provides that the communication may be intercepted 'if one of the parties to the communication has given prior consent'. This, Beech[436] believes could

---

[431] Act 70 of 2002; s (5)

[432] Mischke op cit note 3 , 78

[433] Beech op cit note 89, 656

[434] Ibid

[435] Ibid

[436] Ibid

lead to a situation that where there is multi - party communication, provided that one party gives its consent, the provisions of s 5 (1) would be complied with.[437]

Section 6 of the RICPCIA provides that any person may, in the course of the carrying on any business, intercept any indirect communication:[438]

- by means of which a transaction is entered into in course of that business;
- which otherwise relates, to that business; or
- which otherwise takes place in the course of the carrying on or that business.

Section 6 (1) appears according to Beech[439] to address the situation where for example, the transaction is recorded for the purposes of recording the terms and conditions of the transaction, protection of the parties. Section 6 (1) essentially provides for the recording of transactions which take place in the course of carrying on the business of the employer.

Such interception may take place only if: [440]

- effected by, or with the express or implied consent of, the system controller;
- the system concerned is provided for use in connection with that business; and
- the system controller has made all reasonable efforts to inform in advance a person, who intends to use the system, that indirect communications may be intercepted or if such indirect communication is intercepted with the express or implied consent of the person who uses it.

Also, such interception must be for purposes of monitoring or keeping a record of indirect communications: [441]

---

[437] Ibid

[438] Act 70 of 2002; s 6 (1) a-c

[439] Beech op cit note 89, 656

[440] Act 70 of 2002; s 6 (2)

[441] Act 70 of 2002; s 6 (2)

- in order to establish the existence of facts;
- to, investigate or detect unauthorised use of that system; or
- To secure, or as an inherent part of the effective operation of the system.

Such interception will also be allowed for: [442]

- monitoring indirect communications made to a confidential voice-telephony counselling or support service:
- which is free of charge, other than the cost of making a telephone call; and
- operated in a way that users thereof may remain anonymous if they so choose.

The purpose of the monitoring must therefore fall within one of three defined purposes. The first of these purposes would be to establish the existence of facts.[443] The interception could also be for the purpose of investigating or detecting the unauthorized use of the telecommunication system. (This would include monitoring and intercepting for the purpose of detecting unauthorized use of the internet system. In this context, unauthorized use would be any use which is not authorized by the company. Any access to, for example, pornography, transmission of racist jokes, etc, would constitute unauthorized use, and would trigger the application of the provisions of s 6).[444]

The third purpose would be to secure or to ensure the effective operation of the system.[445] Fourthly, the system controller must make all reasonable efforts to inform, in advance, the person who intends to use the telecommunication system that indirect communications transmitted may be intercepted, alternatively, the indirect communication must be intercepted with the express or implied consent of the person who uses that telecommunication system.[446]

The provisions referred to above mean that an employer can continue to monitor and intercept

[442] Act 70 of 2002; s 6 (2) (ii)

[443] Beech op cit note 89, 656
[444] Ibid 658

[445] Ibid

[446] Ibid

communications in the workplace provided that, where it seeks to rely on a particular provision, it complies with the provisions contained in that section.[447]

Section 6(2) would therefore authorize the employer to intercept and monitor for these purposes. The reference to detection of unauthorized use is extremely wide, and would include interception to determine whether pornography is being sent and received, racist jokes etc are being sent and received[448]

In addition to interception for one of the listed purposes, it is however essential for an employer to obtain the express or implied consent of the person who uses the telecommunication system. It must be kept in mid that reference to express or implied consent does not necessarily require written consent.[449] For example, if a person is advised that communications may be intercepted oil a particular telecommunication system, and the employee nevertheless makes use of that telecommunication system, this would be implied consent. In order to avoid any possible arguments, written consent should be obtained. If all reasonable efforts have been made to inform a person who intends to use the telecommunication system concerned that indirect communications may be intercepted, there would be compliance with the provisions of s 6(2), and it would not be necessary to obtain the consent of the person.[450]

The requirement of prior written consent has been controversial. On the one hand it has been argued that it is absolutely essential for an employer to obtain the prior consent of its employee in writing before such employer may intercept the electronic communications such as e- mail or short messages (SMS's) of an employee.[451] On the other hand, it is argued that the only time such prior written consent is required, is in section 5 where the employee as a party to the communication has to give such consent. As result of this requirement in section 5, it has been an adopted practice by

[447] Ibid

[448] Ibid 658- 659

[449] Ibid

[450] Ibid 659

[451] VA Lawack Davids & A van der Walt. "Interception of Electronic Communications in the Workplace" (2005) 26 (1) *Obiter* 133- 139

some, to read prior written consent into s 6. Section 6 however does not expressly require prior written consent.[452] If the employee, has consented in advance, it can be taken that the system controller has made all reasonable efforts to inform in advance that indirect communications transmitted by means of a telecommunication system may be intercepted. Therefore if written consent should be obtained, it will be viewed as interception with the express consent of the employee who uses the system (s 6 (2) (d)).[453]

As a result of the uncertainty, van der Walt and Davids[454] believe, that from a practical point of view, it would be advisable for an employer to obtain the prior written consent of all its employees who use its telecommunication system that their communications may be intercepted in accordance with an electronic communications or office communications policy.[455] Due to the fact that prior written consent is not required in terms of s 6, it may occur in certain instances that an employee will refuse to give his or her consent. In cases where this occurs, an employer must have alternative methods of ensuring that its system controller has made all reasonable efforts to inform in advance a person who intends to use that system that indirect communications may be intercepted.[456]

Section 51 of the RICPCIA sets out offences and penalties. It provides that any person guilty of an offence or behaves contrary to the provisions of the Act will be liable to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.[457]

[452] Ibid

[453] Ibid

[454] Ibid

[455] Ibid

[456] Ibid

[457] Act 70 of 2002; s 51 (b)

CHAPTER 4

1. Reasons for monitoring Electronic Communications in the Workplace

The use of computers in the workplace is now a normal occurrence and is often taken for granted. It has become impossible for employees to ensure proper performance of their tasks without the use of increasingly sophisticated electronic communication tools.[458] The use of computer networking, e-mail facilities and the Internet have greatly increased an employees' access to information. A company's computer network, and the Internet has allowed employees virtually unrestricted access to the World Wide Web from their desktops. In light of this it has become difficult for employers to police the information which employees either access or disseminate in the business environment.[459]

The term "electronic communication tools" is said to include the following: [460]

- telephones, mobile phones and voice-mail facilities
- e-mail facilities
- fax machines, modems and servers
- computers
- network tools (for example, Internet browsers and Internet access facilities)

These above mentioned tools have been made available to employees by their employers and are intended to provide and promote business communications as well as to enhance the productivity of company employees. The employer as the owners of these tools, gives them the inalienable right to decide the manner in which they should be used as well as to regulate their use.[461]

---

[458] V Etsebeth "The growing expansion of vicarious liability in the information age (part 1)". (2006) 3 *TSAR* 564

[459] Ibid

[460] L Michalson "The use of the e- mail and the Internet in the Workplace" *Cyberlaw S.A: the internet and the law*. CD-ROM (1999) 196

[461] Ibid

These 'electronic communication tools' can be utilized to access and distribute confidential information with ease and on an anonymous basis. If the electronic tools are used in this way it poses a high risk to their employers because of the potential loss and litigation that may occur. [462] The abuse of these 'electronic communication tools' by employers, will, in most instances compromise the employer. The difficulty in differentiating between business and private usage as well as the methods to be adopted when monitoring raises a number of complex legal issues.[463]

There are inherent dangers to employers due to the unauthorised and inappropriate use of corporate computer systems and resources by employees. [464] Employers may find themselves exposed to legal liability in cases of inappropriate use of corporate Internet and email facilities. There may even be potential liability for employers on grounds of harassment, discrimination, defamation, copyright infringement (where the employee carelessly downloads and disseminates copyright material and software), and criminal liability (if child pornography is downloaded).[465]

This places a greater responsibility on employers not only to guard against attacks being launched against them in the cyber world but also to ensure that they are not used as a vehicle to launch a similar an attack on another company.

Employers must therefore be vigilant as they may be faced with liability on grounds of harassment and defamation resulting from an email which one of their employees sends, they could also be faced with claims based on discrimination and the creation of an unacceptable workplace environment if employees, for instance, view pornographic or sexually explicit or offending material on their computers.[466]

---

[462] Ibid 193

[463] Ibid

[464] Ibid 196- 197

[465] Etsebeth op cit note 1, 565

[466] Ibid 566

1. Vicarious liability

The general rule with regard to the commission of unlawful or delictual acts is that a person is liable only for acts committed personally.[467] In contrast to this rule, our law recognises the doctrine of vicarious liability in terms of which one person can be held liable to a third party for the delictual acts performed by another which caused loss to that third party.[468]

Vicarious liability is a doctrine of liability without fault in terms of which one person is held liable for the unlawful acts of another. It is a strict liability, or liability without fault, on the part of the defendant and is additional to that of the other person's delict.[469] The decision to treat a class of persons differently and to impose vicarious liability is based on social policy regarding what is fair and reasonable and amounts to an expression of a society's legal convictions that victims of a delictual conduct should be able to recover damages from someone who has the ability to pay.[470]

Vicarious liability will be incurred if there is a special relationship between the two persons. For purposes of this discussion, one such important relationship is the employer-employee relationship. In terms of the doctrine of vicarious liability as applied in the employment context, an employer may be held liable to a third party for the delictual acts performed by employees.[471]

The reasons advanced for the existence of the doctrine is that the victim should enjoy fair and just compensation (out of the deeper pocket of the employer), this is so because the employer is better equipped to spread the cost of compensating victims by taking out insurance and by price increases and that employers will take measures to prevent employees from causing damage to third persons if they will be held liable for the acts of their employees.[472]

---

[467] *Feldman (Pty) Ltd v Mall* 1945 AD 733 at 779

[468] JC van der Walt & JR Midgley. *Principles of Delict*. 3ed. (2005). 36

[469] Ibid

[470] Ibid

[471] ME Manamela "Vicarious liability: 'paying for the sins of others' ": case comments. (2004) 16 (1) SA *Merc LJ* 126.

[472] K Calitz "Vicarious liability of employers: reconsidering risk as the basis for liability". (2005) 2 *TSAR* 215

Despite the fact that vicarious liability has its origin in the law of delict it has developed as a general labour law principle that the employer will be liable for the delicts committed by its employees.[473]

The requirements for vicarious liability are: [474]

(a) A relationship of employment must exist;
(b) Commission of a delict;
(c) The employee must have acted in the course and scope of his employment. This phrase refers to acts committed by the employee in the exercise of the functions to which he/she was appointed, including such acts as are reasonably necessary to carry out the employer's instructions.

A) Relationship of employment

There must be some form of employer – employee relationship between the parties in that one person makes his working skills available to another person for some form of numeration. The employer will usually employ people to do his work, and takes interest in their capacity to work.[475] The risk of damage arising from the employee's actions increases if the employer does not do the work on his own. Therefore where the employer trusts the employee to execute the work for third parties on his behalf, then it seems just for the employer to bear the burden of damage should it occur.[476] In an employment relationship there must be some form of control over the employees by the employer. A person will be vicariously liable for the actions of another if the person has control over the actions of the one who committed the delict.[477]

B) Commission of a Delict

---

[473] SP van Zyl "An employer's vicarious liability with reference to the internet and e- mail". 2006 39 (1) *De Jure* 131

[474] van der Walt & Midgley op cit note 11, 37

[475] Ibid 37-38

[476] Ibid

[477] Ibid

This requirement entails that during the course of the employment, the employee fails to perform his duties adequately or at all and consequently causes damage, the employer could be held liable for the damage.[478] The action committed must be wrongful and the employee must have acted negligently or with intent. There must also be a causal link (factually and legally) between the damage suffered and the employee's action.[479]

(C) The employee must have acted in the course and scope of his employment

The test to determine whether or not an employee was acting in the course and scope of his employment was laid down by the court in the case of *Minister of Law and Order v Ngobo 1992 4 SA 822 (A*), where Scott JA described the test as:

> *"The standard test for vicarious liability of a master for the delict of a servant is whether the delict was committed by the employee while acting in the course and scope of his employment. The enquiry is frequently said to be whether at the relevant time the employee was about the affairs, or business, or doing the work of the employer…"*[480]

There is no general rule for establishing the liability of an employer that can be applied to all South African cases involving vicarious liability. The question whether the act falls within or outside the scope of employment is not without problems and the answer has been described as a question of law, but it has also been said that each case will depend on its own facts.[481]

In determining whether an employee's actions fall within the scope of his or her employment and therefore renders the employer vicariously liable, both a subjective test and an objective test may be applied.[482]

---

[478] Ibid

[479] Manamela op cit note 14, 126

[480] *Minister of Law and Order v Ngobo* 1992 4 SA 822 (A) see also *Minister of Safety & Security v Jordaan t/a Adre Jordaan Transport 2000* (4) SA 21 (SCA) at 24H-25E.

[481] Calitz op cit note 15, 218

[482] see *Division in Minister of Police v Rabie* (1986 (1) SA 117 (A); and see also *Witham v Minister of Home Affairs 1989* (1) SA 116 (ZH) at 126) in the following terms (at134C±E): [`It seems clear that an act done by a servant solely for his own interests and purposes ,although occasioned by his employment, may fall outside the course or scope of his

The consequence of these tests is that an employer will be able to escape liability only if the employer can prove that the employee's intention was to solely promote his or her own interests (the subjective test) and that the employee had completely disengaged himself or herself from the affairs of the employer when committing the delict (the objective test).[483] For the employer to escape liability, the actions of the employee must be completely 'unconnected with those of his master'.[484]

Certain sub-rules have been developed by the courts for different types of actions of employees. This is what has become known as cases of deviation and cases of digression.[485]

The application of these rules are discussed below.

In *Viljoen v Smith* 1977 (1) SA 309 (A) the employee, although prohibited by his employer, climbed through a fence and walked some 70 metres onto the third party's farm to relieve himself. While doing so, he lit a cigarette and caused a fire. The Court held that the employee had not abandoned his place of work and that he was still acting within the course and scope of his employment. This indicates that the mere existence of a digression does not automatically result in the employer not being found vicariously liable for the delict of an employee. The employee may still be engaged in the business of the employer whose instructions for the conduct of that business he has disobeyed. Whether the employer will be vicariously liable will depend on the nature of the digression and the surrounding circumstances.[486]

In *South African Railways & Harbours v Marais* (1950) (4) SA 610 (A), the third party was a passenger in the guard van of a mixed passenger and goods train. In contravention of standing

---

employment, and that in deciding whether an act by the servant does so fall, some reference is to be made to the servant's intention. . . . The test is in this regard subjective .On the other hand, if there is nevertheless a sufficiently close link between the servant's acts for his own interests and purposes and the business of his master, the master may yet be liable. This is an objective test. And it may be useful to add that . . . "a master . . . is liable even for acts which he has not authorised provided that they are so connected with acts which he has authorised that they may rightly be regarded as modes ± although improper modes ± of doing them"].

[483] supra note 10, at 742

[484] supra note 10, at 742

[485] Calitz op cit note 15, 218

[486] *Viljoen v Smith* 1977 (1) SA 309 (A) at 317 H-J and 318 E-F

orders, the engine driver invited the third party to join him on the engine's footplate. The two of them and a fireman drank brandy. On route, the engine left the rails due to the driver's negligence and all three died of burns sustained in the accident. In a claim for damages by the third party's wife against the driver's employer, the Court ruled that the transportation of the third party on the engine was entirely the driver's own action and fell outside the scope of his employment. The employer was therefore not vicariously liable.[487]

These cases indicate that an employees act must have had something to do with the carrying on of his or her employment in order to conclude that the act fell within the scope of that employment; if not, the employee will be deemed to be on a 'frolic of his or her own'. The employer will not be vicariously liable if the act of the employee is not performed to accomplish an object for which the employee was employed, but in the furtherance of a personal act, motivated solely by personal reasons.[488] A possible distinction between the cases referred to above may be that, on the one hand, if there is a deviation by the employee which does not amount to a complete abandonment of the employer's business, the employer will be held liable; but, on the other hand, if the deviation by the employee is so great that it cannot be said that the employee is still performing his or her duties, the employee will not be deemed to be acting in the course of his or her employment so that the employer will not be held liable.[489]

An employer may still be held vicariously liable for the conduct of employees even though an employee is not conducting the exact duties imposed on him by the employer. This is illustrated in the case of *Estate Van der Byl v Swanepoel* 1927 AD 141 at 146 where Wessels JA held that there are situations where the employee acted outside the scope of employment but where those actions are reasonably considered to complete his duties. The court held that an employer will definitely be liable for the negligence of the employee where the employee followed his employer's instructions exactly and a stricter approach is to hold the employer liable for the employee's negligence in cases where the employee contravenes the exact instructions of the employer and

[487] *South African Railways & Harbours v Marais* (1950) (4) SA 610 (A), at 613- 614

[488] Manamela op cit note 14, 129

[489] Ibid 129-130

commits actions which are not necessary to complete his duties but still commits these actions whilst engaged in the affairs of the employer. In such cases the court held public policy will dictate whether the employer will be held vicariously liable or not.[490]

The circumstances in which an employer must guard against being vicariously liable are discussed below.

2. Defamation

Shakespeare stated:[491]

''Good name in man and woman, my dear lord,
Is the immediate jewel of their souls;
Who steals my purse steals trash; 'tis something, nothing;
'Twas mine, 'tis his, and has been slave to thousands;
But he that filches of me my good name
Robs me that which not enriches him
And makes me poor indeed.''

Defamation is the 'unlawful, intentional, publication of defamatory matter (by word or conduct) referring to the plaintiff which causes his reputation to be impaired'.[492]

In order to determine whether the contents of an e- mail is defamatory, it must first be ascertained whether a reasonable person of ordinary intelligence may reasonably understand the e- mail to contain a defamatory meaning as regards the plaintiff.[493]

---

[490] van Zyl op cit note 16, 134

[491] Othello Act III Scene 3.

[492] C Mischke ''Disciplinary action and the internet: responding to employee abuse of e-mail, network access and internet access''. (1999) 12 *CLL* 46.

[493] JM Burchell *The Law of Defamation in South Africa* (1985) 35. The meaning of the words published , allegedly defamatory material is determined by establishing whether:
" a reasonable person of ordinary intelligence might reasonably understand the words to convey a meaning defamatory to the plaintiff … The test is an objective one … the reasonable person of ordinary intelligence is taken to understand the words alleged to be defamatory in their natural and ordinary meaning… the Court must take account not only of what the words expressly say , but also of what they imply" (see Corbett CJ in *Argus Printing and Publishing Co Ltd v Esselen's Estate* 1994 (2) SA 1 (A), at 20 E-G later followed in *Delta Motor Corporation (Pty) Ltd v Van der Merwe* 2004 (6) SA 185 (SCA), at 370C *; Dendy v University of Witwatersrand* 2005 (2) All SA 490 (WLD) , at 514 F earlier on in *Channing v South African Financial Gazette Ltd* 1966 (3) SA 470 (W) 474 A-C), where Colman J referring to *Johnson v Randy Daily Mails* (1928 AD 190) where an ordinary reader was defined as :

Publication can be defined as an ‘‘act of making known a defamatory statement or the act of conveying an imputation by conduct, to a person or persons other than the person who is the subject of the defamatory imputation”.[494] The requirement of publication is met when a defamatory statement that impairs the reputation of a third party is spread and read through by others using the employer’s electronic communications’ system as a medium.[495]

An employer can be liable for defamatory e- mail sent by an employee in the course of his or her employment, provided that the requirement of ‘publication’ was met. The question that subsequently arises is, what exactly constitutes publication on the Internet.

In *National Media v Bogoshi* 1998 4 SA 1195 (SCA); it was stated that ‘‘publication is the act of making known a defamatory statement or the act of conveying an imputation by conduct, to a person or persons other than the person who is the subject of the defamatory statement or conduct’’.[496]

It can be inferred from this statement that the following acts will amount to publication: postings to a newsgroup, sending an email, making a website available on the internet, internet relay chat and file transfer by file transfer protocol.[497]

In terms of the South African law of delict, no publication has taken place if the person to whom the statement was made did not understand the meaning thereof. Consequently, if a defamatory statement is encrypted, it will be published only once it has been decrypted.[498]

“A reasonable, right thinking person of average education and normal intelligence; he is not a man of ‘morbid and suspicious mind,’ nor is he ‘super critical’ or abnormally sensitive; and he must be assumed to have read the articles as article are usually read” (474 A-C).

[494] Mischke op cit note 35, 46

[495] Ibid

[496] *National Media v Bogoshi* 1998 4 SA 1195 (SCA)

[497] V Etsebeth “The growing expansion of vicarious liability in the information age (part 2)”. (2006) 4 *TSAR* 755

[498] Ibid

Publication will take place on the internet where the defamatory statement is read, seen or heard and when the receiver understands its contents. Therefore, it is not sufficient for a subject merely to read, see or hear the defamatory statement. He/she must actually understand the content thereof.[499]

In the case of *CWU v Mobile Telephone Networks (Pty) Ltd* 2003 8 BLLR 741 (LC) it is evident that liability for defamation can result in vicarious liability for a company. This case concerned a derogatory e- mail sent by one of the employees of MTN. The e- mail contained allegations that MTN's management was corrupt and that they show favouritism to a certain temporary employment agency.

MTN charged the employee with: (i) intentional circulation of an email insinuating that MTN management was corrupt; (ii) intentionally and disrespectfully engaging in abusive and insulting language in that he insinuated that management were ''fat cats''; (iii) making unfounded allegations against management by insinuating in the email that management was benefiting from recruitment processes; (iv) bringing the company's image into disrepute in
that he circulated the email to MTN employees; and (v) intentionally conducting himself in an insubordinate manner in that the email contained derogatory remarks against MTN management and clients.[500]

The court found that the employee had failed to comply with the procedure established by MTN for reporting allegations of fraud, and that he was seeking a wider audience in the form of MTN management and employees.[501] His email therefore increased the damage to the reputation of MTN and his actions therefore justified a defamation suit against him. The court held that in addition, there were grounds on which the clients of MTN could institute a vicarious liability suit against MTN.[502]

---

[499] Ibid

[500] *CWU v Mobile Telephone Networks (Pty) Ltd* 2003 8 BLLR 741 (LC) at 743G-744B.

[501] supra note 43, at 748F
[502] supra note 43, at 748F.

A court can find that in providing an employee with ‘‘tools’’ to access the internet and email facilities, the employer is directly liable as a publisher or disseminator of the offending statement.[503]

Employers that decide not to regulate publication of material on the internet by their employees could be potentially exposing themselves to a possible claim for negligence on grounds that they owed a duty of care to their employees and third parties to impose some restrictions.[504]

From the above therefore it is accurate to conclude that if a defamatory statement is posted on a Usenet newsgroup or where the email is sent to a person other than the person who is defamed in the message, the requirements of publication would have been met.[505]

Where an e- mail or e- mails are used as the medium for defamatory remarks in the workplace it is important to remember that the defamation will probably occur at the place where the offending material is accessed. This might impact on a defamatory e-mail received from a foreign jurisdiction, as a South African court will only have jurisdiction in South Africa if the words were published (accessed) in South Africa.[506]

This could pose even further problems for employers as practically every country in the world has access to a specific company’s web site, which in turn means that the company is exposing itself to the possibility of being sued in every country where that specific e- mail has been accessed as a result of the behaviour in certain instances of a single employee.[507]

---

[503] Etsebeth op cit note 31, 757 , see also[An international example of online defamation is found in the Australian case of *Dow Jones &Co INC v Gutnick* 2002 HCA 56. This case represents the first Australian case by a final court of appeal on transnational online defamation. Gutnick, the plaintiff (AU), brought an action against the defendant, an American publisher of Barron’s magazine and Barron’s Online. The action was based on an article containing a large photograph of the plaintiff and a statement that he did business with convicted money launderers. This article appeared in printed form and on the web site. Gutnick succeeded in his claim.]

[504] Michalson op cit note 3, 199

[505] Etsebeth op cit note 40, 757-758

[506] Michalson op cit note 3, 199

[507] Ibid

3. Sexual Harassment and Discrimination

Sexual harassment can occur through electronic means.[508] The sexual harassment may take the form of coarse jokes sent via e-mail, pornographic screen-savers and crude graphics. Racial and religious discrimination cases can also be based on offensive electronic content, regardless of the sender's intentions.[509]

Sexual harassment has become a major problem in the workplace. Parliament and our courts have sought to protect employees who are victims of sexual harassment by imposing certain obligations that may render the employers liable.[510]

Employers are under a legal duty to prevent discriminatory acts being perpetrated against their employees. This was illustrated in the case of *Media 24 v Grobler* 2005 JDR 738 (SCA) at 741, where Farlem JA held that an employer has a legal duty that is dictated by public policy to prevent harm such as sexual harassment to its employees.

In terms of section 5 of The Employment Equity Act 55 of 1998 (EEA) an employer is under an obligation to combat unfair discrimination in the workplace:

"Every employer must take steps to promote equal opportunity in the workplace by eliminating unfair discrimination in any employment policy or practice".
Harassment can generally be defined as ''any humiliating or degrading treatment
of a person because of their personal characteristics''. [511]

Harassment is a form of unfair discrimination and is prohibited in the workplace.[512] The reference

---

[508] Ibid

[509] Etsebeth op cit note 40, 758

[510] S Gule "Employers' vicarious liability for sexual harassment". (2005) 13 (2) *JBL* 66

[511] Ibid

[512] Section 6 (3) of the Employment Equity Act 55 of 1998

to harassment includes sexual harassment. Harassment in any form is treated in the EEA as a form of unfair discrimination. The most prevalent form of harassment in the workplace is sexual harassment.[513] An employer who fails to prevent or put an end a case or cases of sexual harassment may be held liable.[514]

Sexual and racial harassment are two forms of harassment that occur most frequently in the workplace. In terms of section 203 of the Labour Relations Act 66 of 1995, sexual harassment amounts to ‘‘unwanted conduct of a sexual nature’’.

A Code of Good Practice on the Handling of Sexual Harassment Cases[515] was issued with the purpose to combat sexual harassment in the workplace. The Code of Good Practice on the Handling of Sexual Harassment Cases states that sexual attention will become harassment if it is ‘‘(a) persistent, although a single incident of harassment can constitute sexual harassment; and/or (b) the recipient has made it clear that the behaviour is considered offensive; and/or (c) the perpetrator should have known that the behaviour is regarded as unacceptable’’.[516]

The Code defines sexual harassment as including various types of conduct, such as, physical, verbal, and non-verbal conduct.[517]

---

[513] M van Jaarsveld “Forewarned is Forearmed: Some Thoughts on the Inappropriate Use of Computers in the Workplace”. (2004) 16 (4*) SA Merc LJ* 661

[514] Section 60 of the EEA 55 of 1998 - which regulates the liability of employers for the conduct of their employees committed while the employees are at work. If the conduct complained of is brought to the employer’s attention, the employer is obliged to take the necessary steps to eliminate the alleged conduct and to comply with the EEA. Section 60(3) renders the employer vicariously liable for the conduct of an employee who contravenes the provisions of the EEA. It states: ‘If the employer fails to take the necessary steps referred to in sub-section (2), and it is proved that the employee has contravened the relevant provisions, the employer must be deemed to have contravened that provision.’ Section 60(3) deems the employer to have contravened the provisions of the applicable section if it “fails to take the necessary steps referred to in subsection (2), and if it is proved that the employee has contravened the relevant provision”.
An employer is not liable for the conduct of an employee “if that employer is able to prove that it did all that was reasonably practicable to ensure that the employee would not act in contravention of this Act” (section 60(4)). Steps that may be taken are set out in sub-section (2) – that is, the relevant parties must be consulted and the “necessary steps” taken.

[515] Promulgated by notice 1367 in GG 19049 of 17 July 1998

[516] Code of Good Practice on the Handling of Sexual Harassment Cases , section 3 (2) (a- c)

[517] Code of Good Practice on the Handling of Sexual Harassment Cases , Item 4

In the case of *Ntsabo v Real Security CC* [2004] 1 BLLR 58 (LC); Ms Ntsabo was employed as a guard with Real Security CC. Ms Ntsabo, a single mother, found herself stationed at Khayelitsha Day Hospital. She reported to a supervisor who turned out to be worse than a mere groper. On one occasion the supervisor all but raped her, then threatened to shoot her if she told anybody about the incident. The matter was 'sorted out' by transferring Ms Ntsabo to another site, where she was required to work at night. When she complained, Ms Ntsabo was told that if she did not like night work she could resign. She did so. After resigning, she approached the Labour Court for relief, claiming compensation for an automatically unfair dismissal and damages for future medical costs and humiliation, impairment of dignity, pain, suffering, emotional trauma and the loss of the normal amenities of life. All this relief was sought against her former employer. [518]

The court had to consider whether the employer Real Security was liable for making the continued employment of Ms Ntsabo intolerable, even though the cause of the intolerable situation was due to the conduct of an employee of Real Security (the supervisor), who, while he may have harassed the employee during working hours, could hardly be said to have been acting in the course and scope of his duties.[519]

The court held that an employer can only be held liable for the conduct of one of the employees if the employer created an intolerable situation by failing to prevent one of its employees from creating and perpetuating an intolerable situation for another an further that an employer can only be held to have failed to prevent an employee from creating and maintaining an intolerable situation for another if it (or its management) was aware of the situation and did nothing about it. [520]

Pillay AJ held that Ms Ntsabo had done all that could reasonably be expected of her "to attempt to hold onto her employment and avoid being sexually harassed". The employer had "brushed aside her complaint". This inaction was unfair and had created an intolerable working environment for

---

[518] *Ntsabo v Real Security CC* [2004] 1 BLLR 58 (LC); at I- J

[519] supra note 61, at 93 A-B see also [*Pretoria Society for the care of the Retarded v Loots* (1997) 18 ILJ 981 (LAC) at par 985 A-B]

[520] supra note 61, at 98 H-I

Ms Ntsabo. Her resignation accordingly constituted a constructive dismissal.[521]

The EEA now gives the Labour Court power to grant compensation and/or damages to employees who are victims of discrimination on various grounds cited in the Act[522]

The court found that Ntsabo had been constructively dismissed and awarded her
R12 000 as compensation. On the sexual harassment issue, the court found that the senior employee of the corporation had contravened section 6(3) of the EEA and that the corporation was liable for the conduct of such employee in contravening the Act.[523]
The Labour Court exercised its power in terms of section 50 to award compensation and damages in respect of unfair discrimination. It awarded Ntsabo R20 000 for future medical costs, and R50 000 as general damages.[524]

If the traditional test[525] of vicarious liability is applied to sexual harassment cases, the employee would have to prove that, when the harassment took place, the perpetrator was acting within the course and scope of employment. It was thought that an aggrieved employee would be unlikely to prove this, as there is no employee who can be said to be acting within the course and scope of employment when he or she sexually harasses co-employees.[526] Instead in this instance, the harassment will be regarded as a 'frolic' of the employee, which has traditionally been a defence to a claim based on vicarious liability.[527]

---

[521] supra note 61, at 93 A-C

[522] Employment Equity Act 55 of 1998 (see sections 50(1) (d) and (e), read with sections 50(2) (a) and (b)), which specifically includes "harassment" (section 6(3)).

[523] supra note 61, at 102 A-D

[524] supra note 61, at 102 A-D

[525] *Canadian Pacific Railways C v Lockhart* 1942 AC 591 599 –formulated the so-called ''Salmond test'': ''. . . an employee's wrongful conduct is said to fall within the course and scope of his employment where it consists of either (i) acts authorized by the employer; or (ii) unauthorized acts that are so connected with the acts that the employer has authorized that they can be regarded as modes – although improper modes – of doing what has been authorized''.]

[526] Gule op cit note 53, 67

[527] Gule op cit note 53, 67

The High Court had to consider the common law doctrine of vicarious liability in sexual harassment cases in *Grobler v Naspers* 2004 (4) SA 220 (C).

In *Grobler v Naspers*[528] a trainee manager (Samuels) sexually harassed his secretary (Sonja) who suffered severe trauma. She claimed damages from Naspers on the ground that they were on common law principles vicariously liable for the manager's conduct. The victim did not claim from the employer in terms of section 60 of the Employment Equity Act 55 of 1998, since this Act requires that the perpetrator and victim should be employed by the same employer. She was employed by Naspers Tydskrifte, while the perpetrator was employed by Naspers Ltd.

The court referred to *ABSA Bank Ltd v Born Equipment (Pretoria) (Pty) Ltd* 2001 (1) SA 372(SCA) at 378, where the following was stated:

> *"The standard test for vicarious liability of a master for the delict of a servant is whether the delict was committed by the employee while acting in the course and scope of his employment. The enquiry is frequently said to be whether at the relevant time, the employee was about the affairs, or business, or doing the work of the employer. . . . A master is not responsible for the private and personal acts of his servant, unconnected with the latter's employment, even if done during the time of his employment, and with the permission of the employer".*

The court had to consider whether the actions of Samuels took place within the scope of his employment. The court referred to *Costa da Ouro Restaurant (Pty) Ltd t/a Umdloti Bush Tavern v Reddy* 2003 4 SA 34 (SCA). In this case the Supreme Court of Appeal had to decide whether a barman acted inside or outside his scope of employment when he assaulted a patron outside the bar. The reason for the assault was that the patron (Reddy) made remarks about the barman (Goldie)'s efficiency. Reddy afterwards tipped another barman excessively in front of Goldie. Goldie was provoked and followed Reddy when he left the restaurant. He attacked Reddy outside the restaurant. Reddy claimed damages from the restaurant on the ground of vicarious liability. The court *a quo* also applied the degree of deviation test and held that Goldie's act was committed within the scope of employment for the following reasons:

---

[528] *Grobler v Naspers* 2004 (4) SA 220 (C)

"It was not a grudge which Goldie harboured against the plaintiff independently of his work situation. It was a grudge which arose directly out of his work situation. The digression or deviation, if any from what Goldie was employed to do, and what he in fact did was so close in terms of space and time that it can reasonably be held that he was still acting within the courseand scope of his employment". [529]

This is an example of the degree of digression used as test in order to establish the vicarious liability of the employer. The court a quo was in fact prepared to hold the employer liable for the intentional wrongdoing of the employee. This decision was, however, overturned on appeal. The Supreme Court of Appeal held that the restaurant was not vicariously liable because the assault occurred after the barman had abandoned his duties. The court stated the following:
"It was a personal act of aggression done neither in furtherance of his employer's interests, nor under his express or implied authority, not as an incident to or in consequence of anything Goldie was employed to do. The reasons for and the circumstances leading up to the assault may have arisen from the fact that Goldie was employed by the restaurant as a barman, but personal vindictiveness leading to the assaults on patrons does not render the employer liable"[530].

Should the court apply the rule as interpreted in that case, the acts of Samuels would also fall outside the scope of employment. The reason this is that the acts of Samuels could be similar to the acts of Goldie the barman, that is, classified as acts of personal aggression and passion, not done in furtherance of his employer's business and not authorised by the employer.
South African cases on vicarious liability do not provide guidelines. Since sexual harassment would always be against the employer's instructions, it could not be described as being done in furtherance of the employer's business and therefore will not fall within the scope of the employee's appointment.[531] The court in Naspers[532] therefore considered foreign cases in this regard:

---

[529] *Costa da Ouro Restaurant (Pty) Ltd t/a Umdloti Bush Tavern v Reddy* 2003 4 SA 34 (SCA) - The court of appeal quoted from the decision of the court a quo at 41B.

[530] supra note 72, at 41H.

[531] Calitz op cit note 15, 225

[532] supra note 71

The leading American case is *Faragher v City of Boca Raton* 524 US 775 (1998), where the court held that an employer may be held vicariously liable "for conduct that may be fairly regarded as foreseeable risks of his business".[533]

In a Canadian case of *Boothman v Canada* [1993] 3 FC 381 (TD), the court held that an employer will be liable in sexual harassment cases because an "employer must ensure that every person employed in a position of trust is capable of curbing his or her sexual urges".

The court in *Boothman v Canada,* stressed the importance of "finding a sufficient connection between the act of the employees and the employment''.[534]

In the case of *Proceedings Commissioner v Ali Hatem* 1999 1 NZLR 30, the court held that although sexual harassment cannot be regarded as part of the ordinary course of the firm's business, the perpetrator was acting in the ordinary course of such business when he committed the act.[535]

---

[533] *Faragher v City Boca Raton* 524 US 775 (1998), 524 US 775 (1998), - ["It is quite unlikely that these cases would escape efforts to render them obsolete if we were to hold that supervisors who engage in discriminatory harassment are necessarily acting within the scope of their employment. The rationale for placing harassment within the scope of supervisory authority would be the fairness of requiring the employer to bear the burden of foreseeable social behaviour, and the same rationale would apply when the behaviour was that of co-employees. The employer generally benefits just as obviously from the work of common employees as from the work of supervisors; they simply have different jobs to do, all aimed at the success of the enterprise. As between an innocent employer and an innocent employee, if we use the scope of employment reasoning to require the employer to bear the cost of an actionably hostile workplace created by one class of employees (ie supervisors) it could appear just as appropriate to do the same when the environment was created by another class of employees (ie co-workers)."]

[534] *Boothman v Canada* [1993] 3 FC 381 (TD 22 par 20 ["The fundamental question is whether the wrongful act is sufficiently related to the conduct authorised by the employer to justify the imposition of vicarious liability. Vicarious liability is usually appropriate where there is a significant connection between the creation or enhancement of a risk and the wrong that accrues therefrom, even if unrelated to the employer's desires. Where this is so, vicarious liability will serve the policy considerations of provision of an adequate and just remedy and deterrence. Incidental conditions to the employment enterprise, like time and place (without more), will not suffice. Once engaged in a particular business, it is fair that an employer be made to pay the generally foreseeable costs of that business. In contrast, to impose liability for costs unrelated to the risk would effectively make the employer an involuntary insurer."]

[535] *Proceedings Commissioner v Ali Hatem* 1999 1 NZLR 30 par 24- `` [E]mployers have the authority to deal with staff in the work environment to the extent necessary. If they deal with them badly, rather than well, they are nevertheless doing something within the ordinary course of the business of the firm. They are doing something generally authorized, albeit they are doing the acts in a tortuous manner".

The court in Naspers[536] stated that even if the supervisor test could not be used, the courts in Canada, New Zealand and the United Kingdom would have held Naspers liable on the ground that the work relationship created a risk of harassment or enhanced such a risk and that the harassment took place in that employment relationship.

The court applied factors suggested in *Bazley v Curry* (1999)174 DLR (4th), to establish whether there was a sufficient connection between the creation of risk by Naspers and the wrong complained of.[537]

The court investigated the employment relationship between the trainee manager and secretary and found that the intense and personal relationship created an inherent risk of sexual harassment and that the acts of Samuels were sufficiently connected to and fell within the risk that was created. The court held that because there is a sufficiently close connection between the enterprise risk and the wrongful acts, policy purposes (adequate compensation of the victim and deterrence) will be served if Naspers is held vicariously liable for the sexual harassment of the secretary by her manager.

Nel J stated that section 173 of the Constitution Act 108 of 1996 allows the court to develop

[536] supra note 71

[537] *Bazley v Curry* (1999)174 DLR (4th (1999)174 DLR (4th) at para 41 –[McLachlin J concluded that in determining whether an employer is vicariously liable for an employee's unauthorised intentional wrongdoing in cases where precedent is inconclusive, courts should apply the following principles:
(1) ``They should openly confront the question of whether liability should lie against the employer, rather than obscuring the decision beneath semantic discussions of 'scope of employment' and 'mode of conduct'.
(2) The fundamental question is whether the wrongful act is sufficiently related to conduct authorized by the employer to the imposition of vicarious liability. Vicarious liability is generally appropriate where there is a significant connection between the creation or enhancement of a risk and the wrong that accrues there from . . . . Where this is so, vicarious liability will serve the policy considerations of provision of an adequate and just remedy and deterrence. Incidental connections like time and place will not suffice. Once engaged in a particular business it is fair that an employer be made to pay the generally foreseeable costs of that business. In contrast, to impose liability for costs unrelated to the risk would effectively make the employer an involuntary insurer.
(3) In determining the sufficiency of the connection between the employer's creation or enhancement of the risk and the wrong complained of subsidiary factors may be considered:
(a) the opportunity that the enterprise afforded the employee to abuse his or her power;
(b) the extent to which the wrongful act may have furthered the employer's aims;
(c) the extent to which the wrongful act was related to friction, confrontation or intimacy inherent in the employer's enterprise;
(d) the extent of power conferred on the employee in relation to the victim;
(e) the vulnerability of potential victims].

common law to promote justice.[538]

In light of the above Nel J held that the employer was vicariously liable for the actions of its employees even though the said delict, in this case sexual harassment of a fellow employee, might have been "a frolic of its own".[539]

The cases of *Ntsabo*[540] and *Naspers*[541] demonstrate two different approaches that have been adopted by the courts in seeking to grant relief to victims of sexual harassment. *Ntsabo* is based on the provisions of the EEA, which incorporates the doctrine of employer liability.[542] The employer has a defence if it can show that it took reasonable steps to guard against actual harassment taking place, by implementing policies related to it, and, when an incident was reported, by taking steps to redress the wrong.[543]

As things stand, however, Naspers[544] is a landmark judgment not only for cases of sexual harassment in the workplace, but also for the law of vicarious liability in general. It reveals that the courts will not hesitate to break the shackles of the common law where that law is perceived as no longer satisfying the requirements of modern society and the values enshrined in the Constitution. The judgment therefore sounds a clear warning to employers: If employees harass their colleagues to the extent that they suffer physical or psychological harm, employers will have to cough up.[545]

---

[538] supra note 71, at 299

[539] supra note 71 , at 299

[540] supra note 61

[541] supra note 71

[542] J Grogan "Vicarious harassment: Employers become reluctant insurers". (2004) 20 (4) *EL* 3

[543] Ibid

[544] supra note 71

[545] Grogan op cit note 85, see also *Grobler v Naspers* supra note 71 at (277D - F and 278H - I) - where Nel J stated that :
-the test for vicarious liability is not a strict and unchangeable rule
-the application of the rule must be determined with reference to public policy.
-the most important rule of public policy is that a fair right of recourse will be awarded which can double as a deterrent
-the risk created by the employer to do his work is an important factor.

In the interests of public policy, courts tend to rule in favour of the existence of vicarious liability.[546] In order to grant some form of relief to the victim, the courts sometimes make a ruling against the employer. The policy objective supporting these rulings is the creation of a balance in society.[547]

Since misconduct in the workplace such as sexual harassment is not unforeceable, an employer cannot escape liability merely because the actions of the employee was the frolic of his own. Therefore it is necessary for employers to put preventative measures in place that prevents such conduct from occurring.[548]

The case of *Cronje v Toyota Manufacturing* 2001 3 BALR 213 (CCMA) dealt with discrimination through racially offensive material.

The commissioner remarked that the email sent by the applicant was "crude, offensive and had a racist stereotype developed over centuries by white people that associates black people with primates; beings of lesser intelligence and low morality''. The commissioner decided that Cronje's dismissal was substantially fair.[549]

The reason for the increase in the popularity of emails as the chosen form of harassment and discrimination can be explained as follows:

> *''. . .because it appears to be anonymous and transitory, and is thought of as being akin to the spoken rather than the written word, the tone utilised in e-mail is generally more informal and discursive than in formal written correspondence. Written words lack vocal and visual intimations, and offence may easily be caused where none was actually intended as the informal culture surrounding e-mails often result in accuracy, implications and consequences of the content of the message being overlooked. This increases the risk that*

---

[546] van Zyl op cit note 16, 133

[547] Ibid

[548] Ibid

[549] *Cronje v Toyota Manufacturing* 2001 3 BALR 213 (CCMA) at 222F-G.

messages may be sent in anger or jest without consideration of the consequences of releasing the message into an uncontrolled external environment, thereby also increasing the danger of occurrence of harassment . . . In addition the scope of causing offence is increased as a single email may reach a wider and more diverse audience than originally envisaged given the ability to forward
messages".[550]

Harassment can also occur through racially offensive material as illustrated in the case of *Bamford v Energizer (SA) Limited* 2000 12 BALR 1251 (P) and the case of *Morse v Future Reality Ltd* (ET case number 54571/95).

The arbitrator in the *Bamford*[551] case held that:

''[t]o suggest that they thought that it was permissible to use company resources to entertain themselves with images which would have been regarded generally speaking as socially unacceptable is not credible. Their claim that they thought there was nothing offensive with it, is of course, in part, undermined by Oosthuizen's evidence that she was indeed offended by the bouquet of penises sent to her, and untenable on the basis that the material is so obvious contrary to what would circulate amongst self-respecting people. . . . those jokes which have a racial connotation, are typical of what one would strive to avoid in contemporary South African society. Although it is probable that such humour is enjoyed in private, it can hardly be said that in the work place an employer would and should condone such exchanges."[552]

In the case of *Morse v Future Reality Ltd* (ET case number 54571/95); an English tribunal found the employers vicariously liable as they had failed to take the necessary steps to prevent sexual discrimination in the workplace. Morse had been forced to share an office with men who spent large amounts of the working day viewing pornographic material, even though circulation and

[550] Etsebeth op cit note 40, 759

[551] *Bamford v Energizer (SA) Limited* 2000 12 BALR 1251 (P) 2000 12 BALR 1251 (P)

[552] supra note 94, at 1268 C-F

discussion was not directed at her, the tribunal found that the employer had created an uncomfortable working environment by allowing the employees to download sexually explicit material.

In light of the above it is clear that an employer can be held vicariously liable for the discriminatory conduct of its employees.

4. Viewing of Pornography

The introduction of the internet to South Africa in 1993 ensured the country's irrevocable entry into the information age. A flood of information, some good and others not so good, were suddenly easily accessible.[553] The introduction of the internet coincided with a period of major political transformation in South Africa. With the adoption of the Interim Constitution of South Africa Act 200 of 1993 and its successor, the Constitution of South Africa Act 108 of 1996 saw the introduction of the Bill of Rights, including the rights to privacy and freedom of expression.[554] Although these rights are not absolute, they need to be jealously guarded. These rights become relevant especially when closer attention is paid to the nature of information, such as pornography available on the Internet.[555]

Pornography is easily accessible on the Internet. Certain forms of on- line pornography (also referred to as cyber porn) constitute cyber crime and may be prosecuted in terms of the Films and Publications Act 65 of 1996 (hereafter referred to as the ACT). The Act is the principal statute governing online pornography in South Africa.[556]
Section 2 of the Act outlines the objects of the Act as follows:[557]

[553] M Watney. "Regulation of Internet pornography in South Africa (1)". 2006 (69) *THRHR* 227-228

[554] Ibid

[555] Ibid

[556] Ibid 232

[557] Films and Publications Act 65 of 1996; s 2

(a) to regulate the creation, production, possession and distribution of certain publications and certain films by means of classification, the imposition of age restrictions and the giving of consumer advice, due regard being had in particular to the protection of children against sexual exploitation or degradation in publications, films and on the Internet; and
(b) to make the exploitative use of children in pornographic publications, films or on the Internet punishable.

Section 1 of the Act defines publication as inter alia (i) computer software which is not a film; and (ii) any message or communication, including a visual presentation, placed on any distributed network including but not confined to the Internet. Most forms of pornography on the Internet will be classified as 'publications', with the exception of a pornographic video clip, which could rather be classified as a 'film' due to the fact that the definition of film includes "images (that) will be capable of being seen as a moving picture".[558]

Section 27 of the Act deals specifically deals with child pornography[559] and in this regard the following three categories of offences were created:[560]
(a) Offences dealing with the actual perpetrator;
(b) failure to report knowledge of the commission of an offence referred to in paragraph (a); and
(c) failure to prevent access to certain materials.

Section 27 (1) makes it an offence for any person to be in possession of, create, distribute, import or knowingly export or takes steps to export a film or publication which contains child pornography or which advocates, advertises or promotes child pornography or the sexual

[558] Film and Publications Act 65 of 1996; s1[the first amendment was brought by the Films and Amendment Act 34 of 1999 to make specific provision for material on the Internet, this was followed by the second Films and Amendment Act 18 of 2004 to give further effect to the provisions of the Convention on Cybercrime.]

[559] Act 65 of 1996 - Section 1 defines child pornography : " It includes any image, however created , or in any description of a person , real, or simulated , who is, or who is depicted or described as being , under the age of 18 years: (i) engaged in sexual conduct; (ii) participating in, or assisting another person to participate in , sexual conduct ; or (iii) showing or describing the body , or parts of the body , of such person in a manner or in circumstances which, within context , amounts to sexual exploitation , or in such a manner that is capable of being used for the purposes of sexual exploitation".

[560] Act 65 of 1996; s 27 (a) – (c)

exploitation of children.[561]

In terms of s 30 (1A) contravention of s 27 (1) is punishable with a fine or imprisonment for a period not exceeding 10 years or both such fine and imprisonment.[562]

Section 27 (2) (b) places a duty upon any person who has knowledge of an offence under section 27 (1) or has reason to suspect that such an offence has been or being committed to report that offence or suspicion of that offence to the South African Police Service. Section 30 (1) provides for a sentence of a fine or imprisonment for a period not exceeding five years or both in respect of a contravention of s 27 (2).[563]

Internet Service Providers (ISP's) have a vital role to play with regards to the accessibility of the Internet. Thus such formal regulation of the industry is to be expected. Ignorance will no longer be a defence to the ISP whose services are used for the hosting or distribution of child pornography. [564] Section 27 A is specifically aimed at the duties and responsibilities of ISPs in relation to child pornography and was placed in the statue book by the second Films and Amendment Act 18 of 2004. Every ISP is required to take all reasonable steps to prevent the use of its services for the hosting or distribution of child pornography.[565]
The steps to be taken are not outlined, but the provision that "all reasonable steps" must be taken places a substantial burden on ISP's in this regard.[566]

Section 30B (1) contains two presumptions to assist the State in the prosecution of child pornography offences in particular. The first presumption entails that, if in any prosecution in

[561] Act 65 of 1996; s 27

[562] Act 65 of 1996; s 30 (1A) & s 27 (1)

[563] Act 65 of 1996 ; s 27 (2)

[564] Watney op cit note 96, at 232

[565] Act 65 of 1996 ; s 27 A (2) (a) – (c)

[566] Watney op cit note 96, at 232

terms of the Act it is proved that any message or communication, including a visual presentation, was placed on a distributed network, including the Internet, by means of the access provided or granted to a registered subscriber or user, it shall be presumed, in the absence of evidence to the contrary which raises reasonable doubt, that it was so placed by the registered subscriber or user.[567] Section 30B (l) (b) further provides that if in any prosecution in terms of the Act access was gained or attempted to be gained to child pornography on a distributed network, including the Internet, by means of access provided or granted to a registered subscriber or user, it shall be presumed, in the absence of evidence to the contrary which raises reasonable doubt, that such access was gained or attempted to be gained by the registered subscriber or user.[568]

In light of the above, it is clear that employers must ensure that their employees are not engaged in the creation, production, distribution and possession of pornographic material. In instances where the employees are engaged in this conduct, ISP's will be brought to account, with the result that the ISP's will report the company as the wrongdoer as the company is responsible for the material on company computers and e- mail systems(s 27 A).[569] It is submitted that the implications of s 30 B (1) and S 30 B (1) (b) is that the brand of the company that is ultimately tarnished even if the employees are engaged in the creation and distribution of the conduct.[570]

Further reasons why employers need to monitor their employees.

5. Intellectual Property

Electronic content is subject to copyright. In terms of South African copyright law, copyright is the right given to the owner of certain types of works not to have his/her work copied without

---

[567] Inserted by the second Films and Publications Act 18 of 2004

[568] Inserted by the second Films and Publications Act 18 of 2004

[569] M Watney. "Regulation of Internet pornography in South Africa (2)". 2006 (69) *THRHR* 385-386

[570] Ibid

authorisation.[571] A work is copyrighted when it has been created by the author's original skill and effort and has been reduced to a material form and is therefore not merely an idea.[572]

Copyright is protected in South Africa in terms of the Copyright Act 98 of 1978 (hereafter referred to as the 'Act'). Copyright gives the owner the right to prevent the unauthorised reproduction of his/her work as well as protection against the commercial exploitation thereof.[573] In terms of the Act, two forms of copyright infringement can take place, namely direct and indirect infringement.[574] Direct infringement consists of an act ''done or caused to be done, in the Republic, without the licence of the copyright owner, which the copyright owner has the exclusive right to do or to authorise''. Indirect infringement will take place where there is the ''importation, sale or distribution of unauthorised copies, provided the defendant had knowledge that the making of the article concerned constituted an infringement of that copyright or would have constituted such an infringement if the article had been made in the Republic''.[575] In order to be successful, the plaintiff must first of all indicate to the court that he/she has copyright in the work concerned.[576]

In South Africa, one does not have to register copyright (as is the case with other forms of intellectual property, such as patents or trademarks). A copyright situation will arise automatically as soon as something tangible is produced as a result of the author's original skill and effort.[577] Once an expression is entered into a computer in a form that can be read on a screen, it is considered fixed in a material medium even if it is never printed out or saved to a disk. Therefore employees surfing web sites are not entitled to freely copy and distribute content obtained from those web sites owned by companies without obtaining prior permission. This extends to copying

[571] GJ Lidovho " The internet and the piracy of copyrightable computer software in South Africa : some comparative perspectives" .(2006) 123 (2) *SALJ* 339

[572] Ibid

[573] Etsebeth op cit note 40, 761

[574] Ibid

[575] Ibid

[576] Ibid

[577] Lidovho op cit note 114 , 339- 340

images and text found on the web site.[578]

The World Wide Web now makes it possible to download magazine articles, reports, song titles, videos and photographs, all of which are protected by copyright. A computer software program placed on the Internet can also be downloaded at sites around the world and re-posted.[579] All this is possible without it never leaving the computer of its designer. It is also possible to download copyrighted graphic and textual material posted to a web site where it can be changed, merged with other material, returned to cyberspace and perhaps even sold as a different product altogether.[580]

This has obviously created numerous problems for publishers and a potential nightmare for the creators of articles, songs, software and films, as the owners will want to protect their materials. While there are steps and measures being put in place by operators and or creators to protect the content of their web sites against indiscriminate copying, there is a large amount of online content that is not technically protected against copying.[581] This being the case, there is a serious potential of loss that could arise for corporate employers where such copying is conducted by their employees.[582]

If an employee ignores these stipulations, he/she will expose the company to vicarious liability for copyright infringement.

6. Personal use

It is an implicit term of an agreement between employer and employee that: "An honest day's

---

[578] Ibid

[579] Etsebeth op cit note 40 , 762

[580] Ibid

[581] Michalson op cit note 3, 207

[582] Ibid

work will result in an honest day's pay".[583] This agreement between employer and employee has been established over centuries. The overwhelmingly popular reason advanced by employers for the electronic monitoring of employees is the need to maintain or improve productivity.[584]

The challenge that many companies face is that with the introduction of technological innovations in the workplace there has emerged the increased risk of wasted time and resources by employees.

The first of these technological innovations was the introduction of the telephone.[585] The telephone does provide the employer with the benefit of having employees to do more work in a shorter period of time. This new technological tool added something not typically found in formal office communication, that is, the emergence of idle office conversation, commonly referred to as chitchat. Employers do have a vested interest in promoting good communication and strong relationships between employees. Thus, employers are willing to compromise and are of the view that as long as the number or length of personal calls is not excessive, attempts to ban them will have a negative effect for employee morale and ultimately the employer suffers as a result.[586]

Due to the Internet being an increasingly important part of the workplace, game playing is no longer the chief time wasting tool by employees. Employees who have Internet access are presented with the equivalent of a television set that has a million or more channels.[587] As a result employees are finding it difficult to resist the temptation to engage in on- line shopping, monitor sport scores, buy shares, keep in touch with colleagues, buy movie and concert tickets and so on.[588]

E-mail software is now able to convert voice recordings and even full motion video into one e-mail message.[589] If employees use the multimedia e-mail capabilities excessively this will

[583] Ibid 198

[584] Ibid

[585] Ibid

[586] Ibid

[587] Ibid

[588] Ibid

[589] Ibid 198- 199

consume significant portions of the company's bandwidth, leading to network performance problems and increased operation costs.[590] A great concern for employers is that the time spent by employees on the internet and reading e- mails will inevitably be time wasted. The effect of this is ultimately felt by the employer in the form of loss of productivity.[591]

7. Electronic Fraud

In an electronic environment, it is possible to impersonate another person's identity. [592]

In almost all cases the true identity of the sender will not be determined. The reliance on e-mail headers which would normally reveal the name and e-mail address of the sender will not be a true indicator as from whom the e- mail originates.[593] These headers may have been changed by the sender and it would be incorrect to assume in such circumstances that the sender must be the source of the e-mail simply because he/she appears to be working from these otherwise trustworthy and reliable electronic addresses.[594]

8. Computer Viruses

A computer virus may be defined as an unauthorised software program or portion of a program that is introduced into a computer or network.[595] The purpose of a virus whether formed intentionally or not is to damage data files, delete data or perform other harmful actions. In most instances where a virus has been detected the only method of dealing with that particular virus would be to reformat the infected removable storage device or hard drive. When a removable storage device or hard drive is reformatted all the data on that removable storage device or hard

---

[590] Ibid

[591] Ibid

[592] Ibid

[593] Ibid 206

[594] Ibid 206-207

[595] Ibid 206

drive is lost forever.[596] This would obviously result in major losses for an employer should crucial and irreplaceable company information be lost in the process.

Computer viruses are becoming increasingly common and the number of viruses being detected has increased. The downloading or copying of unauthorised software onto employees' computers is one of the most common and simple ways for these viruses to invade a computer or network.[597] Networks may also contract viruses. The Melissa virus, for example, has been estimated to have cost North American businesses about $80 million. Viruses result in great costs for employers.[598]

9. Disclosure

On a daily basis companies make use of the World Wide Web to manage and distribute proprietary and confidential information. A company's e-mail messages to other businesses can contain information on business plans, and can carry as attachments detailed spreadsheets, drawings, charts and supporting documentation. Besides e-mail, the company may place equipment design and important formulae on the company's intranet to be accessed by employees. [599]

Employers also have an vested interest in preventing the premature and unauthorised disclosure of information by employees which is likely to have a detrimental effect on the financial results, the financial position or cash flow of a public company listed on the Stock Exchange, or any information pertaining to new developments in its area of activity which has not been disclosed publicly or intended for public knowledge. The unauthorised disclosure of such information may have an effect on a public company's assets and liabilities or financial position.[600]

As a result and as discussed above companies are exposed to an increased risk of exposure of

[596] Ibid 208

[597] Ibid

[598] Ibid

[599] Ibid 206

[600] Ibid 208-209

confidential information. This disclosure can occur in a variety of ways: [601]

- an e-mail to a distribution list that includes a non-employee (or even co-employees who do not have a need to know, in the case of some particularly sensitive information)
- posting information to a bulletin board or newsgroup that contains non-employee members
- placing information on a company-controlled intranet that has been configured and allows access by non-employees
- the temporary collapse of an intranet firewall, permitting temporary access by outsiders (whether or not such access actually occurs)
- posting information to a password-controlled, externally accessible web page (where the password is compromised)
- loss of the computer on which the information has been stored (e.g. loss through theft of a notebook computer)
- sale of a used computer (and disk), from which confidential information has not been thoroughly removed
- loss, theft, or improper destruction of computer media (for example a CD ROM) containing the confidential information.

10. Excessive use

The time spent by employees on the Internet may give rise to a tendency not to do assigned work. Overuse may also overload the workplace network. This will cause delays and unwanted congestion in the distribution and dispatch of incoming and outgoing business information. All these difficulties increase costs for employers. [602]

In light of the above, employers believe they have adequate reasons to monitor the activities of their employees during working hours.

[601] Ibid

CHAPTER 5

Employers arguments in favour of monitoring – An Examination of case law

There are legitimate reasons why employers wish to monitor the activities of their employees during working hours. For instance, employees waste time by sending and forwarding e- mail messages that are not concerned with aspects of work, there is the possibility of confidential information being communicated to someone outside the employer's organisation, the possibility of sexual harassment or racial discrimination arsing from an employee's downloading and displaying images or material that is offensive to others.[603] Frivolous communications can also cost money and pollute and congest computer space. The uncontrolled usage of the Internet has the possibility of exposing computer systems to the ever present menace of computer viruses, and unsavory messages sent by employees through official company channels may damage the employer's brand or domain name.[604] Employer's also have the legitimate concern of the overloading of network servers and the infiltration of computer viruses that may damage and destroy the company equipment and information.[605]

The extent to which companies in South Africa are experiencing internet abuse practices has been surveyed and the results are presented below. The prevalence and content of internet acceptable usage policies has also been surveyed.

The survey described below was conducted through questionnaires. The survey was conducted with 644 companies listed on the Johannesburg Stock Exchange. The response rate was 25, 4 percent, which was high and possibly an indication of the relevance and importance of the topic to South African business at present.[606]

---

[602] M McGregor "The use of Internet and E- mail at work" (2003) 11 (3) *JBL* 190.
[603] J Grogan "Workplace Privacy: controlling communications abuse". (2004) 20 (2) *EL* 9

[604] Ibid

[605] C Mischke "Workplace Privacy, e- mail interception and the law". (2003) 12 (8) *CLL* 72

[606] L Dancaster "Internet Abuse: A Survey of South African Companies". (2001) 22 *ILJ* 862

The responses to different types of internet abuse in the workplace are listed below:

	Yes	No	No response
Loafing on the internet	68,63%	30,07%	1,3%
Accessing, downloading or sending through e-mail discriminatory or sexually offensive jokes or pictures	69,93%	29,41%	0,66%
Clogged bandwidth or degraded system performance through abuse of the internet system	64,71%	34,64%	0,65%
Violating copyright laws or posting information in the name of your company that defames other companies or individuals	15,69%	81,7%	2,61%

Sufficient cases have surfaced in the law reports to indicate that abuse of electronic communications facilities has become something of a problem for employers.

The case of *Bamford & Others / Energizer (SA) Limited* [2001] 12 BALR 1251 (P) dealt with the illicit use of the internet by employees.

The respondent's South African manager discovered thousands of e-mails of a pornographic, racist and sexist nature, some of which parodied the brand names of other companies and had been stored by the grievants on the company computer system. The company contended that the use of company computers for this purpose affected the efficiency of its computer system and that the storing of such material in the international network potentially compromised its brand name. The grievants were charged with "repeated receipt of and onward forwarding to other staff of obscene pornographic material and jokes" and "with repeated violations of company policies and procedures regarding the use of the electronic mail system and work environment policies". After a disciplinary hearing presided over by the company's attorney, the grievants were summarily dismissed. The grievants then referred a dispute to the CCMA. The grievants did not dispute sending or receiving the material. They claimed, however, that: there was no clear rule against the receipt or transmission of such material, that the company had acted inconsistently in singling

them out for dismissal, and that the penalty of dismissal was inappropriate.[607]

The arbitrator noted that the company had issued several directives concerning the use of the e-mail facility, including one issued in response to the discovery of a chain letter forwarded by one of the grievants. While none of these dealt expressly with pornographic or racist material, they left no room for doubt that the circulation of such material was forbidden. Employees had also been warned against the down-loading of foreign material into the company system, and had been told that office computers were for business use only.[608]

The company exercised a 'margin of tolerance' in regard to the use of computers for conveying messages of a 'social' nature.[609] All the grievants, save one, had admitted knowledge of the policy documents on which the company relied, but they claimed that they had not been under the impression that there was an absolute prohibition on the use of their office computers for the receipt and transmission of private material. The grievants also claimed that they did not regard the material as pornographic or offensive.[610]

The arbitrator rejected the grievants' claims that they were unaware that it was impermissible to traffic in socially unacceptable material. The arbitrator held that the grievants should have realised this even if the company had no rules at all. Apart from the fact that the material was offensive, it damaged the business of the company by clogging the computer system and carried the risk of the company's domain name becoming associated with the messages in its system. The abuse of trade names constituted a trademark violation, and demonstrated how frivolous use of office computers by untrustworthy employees exposed businesses to risk. Furthermore, there was a distinct likelihood that the material might have offended other employees if they had chanced upon it.[611]

The arbitrator rejected the grievants' claim that the company had invaded their privacy because the messages concerned were personal or private, as they claimed. The messages had all been

---

[607] *Bamford & Others / Energizer (SA) Limited* [2001] 12 BALR 1251 (P), at 1251 E-J

[608] supra note 5, at 1258 par a 26 B-H

[609] supra note 5, at 1260 para 31 C-E

[610] supra note 5, at 1252 A

generated by anonymous third parties for the consumption of any member of the general public who wished to read or view them. Moreover, all the information used against the grievants had been retrieved from the company's own e-mail system. Individuals have no right to deposit private material in an employer's storage facility and then prevent the employer from examining it to determine whether there is any point to it being preserved.[612]
The commissioner thus held that the dismissal was of the three applicants was procedurally and substantively fair.[613]

Another case which involved the use or rather abuse of the internet by employees while at work is the case of *Smuts v Backup Storage Facilities* [2003] 2 BALR 219 (CCMA).
The applicant in this case was a branch manager. He was dismissed for viewing pornographic material on the company computer during working hours. He faced other charges of failing to account for company money that was allocated to him for business purposes and a further charge of using the company vehicle for his private use. The applicant argued that all the charges was a fabrication in attempt by the employer to get rid of him.[614]

The commissioner found that all charges were proved, including with regard to the viewing of pornographic material on the company computer during working hours. The commissioner found that the applicant had spent significant time during working hours on the internet. Furthermore, the commissioner held, that, Mr Smuts (the applicant) should not have been engaging in this type of activity in the workplace. Mr Smuts as the most senior person in the office, who was thus required to ensure discipline and the smooth running of operations should have known better. It was held by the commissioner that Mr Smuts had failed to set an example, abused the facility and had failed to act in the best interests of the company. Dismissal according to the commissioner was the appropriate penalty.[615]

---

[611] supra note 5, at 1268 para 45.2, 45.6.45.7 B-D
[612] supra note 5, at 1270 par 47,48 H-J & 1271 A-B

[613] supra note 5, at 1272 par 55 G

[614] *Smuts v Backup Storage Facilities* [2003] 2 BALR 219 (CCMA*)* at 220 A-F

[615] supra note 12 , at 224 A-G

In the case of *Kalam / Bevcap (Nampak)* [2006] 6 BALR 565 (MEIBC); the applicant was dismissed after the respondent established that over a period of five months he had visited thousands of internet sites, mostly pornographic, and spent about a quarter of each working week on this activity. He was dismissed for contravening the respondent's (Nampak) Internet and Information Technology (IT) policy and abusing his position of trust. The applicant denied knowledge of the company's IT policy, and claimed that he did not consider his conduct wrong.[616]

Mr Peter Brown (the HR Manager) testified that on 26 September he received an e-mail alerting him about the breach of the IT policy by the applicant. This e-mail report alerted him to the fact that the applicant was monitored for a period of five months and it is an established fact that he visited 14 802 sites and spent 285 hours per week on the Internet. This meant that 25 percent of the time in each working day was spent on the Internet. The majority of the sites visited were pornographic sites.[617]

The applicant was well informed about the company's IT policy. All employees including the applicant are consistently alerted each time they log onto the Internet that all internet browsing are monitored and if non-conformance to the company's IT policy is detected, the details will be passed to the responsible line and HR management for investigation and possible action.[618]

The commissioner held that the respondent must prove on a balance of probabilities that the applicant is guilty of misconduct.[619]

The commissioner held that according to the evidence presented to him the applicant had violated the respondent's IT policy. The fact the respondent did not read it was not an acceptable excuse. The commissioner held that the fact that the respondent spent approximately 285 hours per week

[616] *Kalam / Bevcap (Nampak)* [2006] 6 BALR 565 (MEIBC) at 565 E-G

[617] supra note 14, at 566 B-C

[618] supra note 14, at 566 C-D

[619] supra note 14, at 567 F- (Schedule 8 of The Labour Relations Act 66 of 1995 provides guidelines in cases of dismissal for misconduct).

and visited 14 802 sites on the Internet on non work related activities was deplorable.[620]

The commissioner held that the applicant visited and downloaded pornographic pictures on many occasions. The commissioner held further that, the respondent did this even though he was alerted via pop up messages showed that his actions were orchestrated. The commissioner held that the applicant had failed to exercise common sense in realising that his conduct was inappropriate. The commissioner held further that this posed a serious concern about the applicant's lifestyle, particularly as a manager and or leader. Thus inevitably, this resulted in the trust relationship between the applicant and respondent having been destroyed.[621]

The commissioner held that the respondent had an obligation to take strict action against abuse of the Internet facility. Therefore the dismissal was justified.[622]

In the case of *Latchmiah / Billiton Aluminium SA (Pty) Ltd t/a Bayside Aluminium* [2006] 6 BALR 569 (MEIBC); the applicant, a senior employee, was dismissed for repeatedly accessing undesirable and pornographic internet sites via his company computer.[623]

The applicant was charged as follows:
"Gross misconduct in that you allegedly committed the following transgression(s):
Improper use of company resources by repeatedly using the company's time and/or computer system to access pornographic material."
In doing the above you also contravened the company's Internet Access Policy and/or the Business Ethics policy and/or the BHP Billiton Guide to Business Conduct and/or the BHP Billiton Logon Notice to Users.[624]

Page 5 of the Business Ethics Policy particularly paragraph 4 stated that:

---

[620] supra note 14, at 567 G-I
[621] supra note 14 , at 567 H-J

[622] supra note 14, at 568 A-C

[623] *Latchmiah / Billiton Aluminium SA (Pty) Ltd t/a Bayside Aluminium* [2006] 6 BALR 569 (MEIBC), at 569 E

[624] supra note 21, at 572 E-F

"The company's electronic communications systems are company resources and all electronic communications are regarded as company records. Offensive material (for example, pornography or material of a sexist or racist nature) is not permitted in any form.[625]

The problem according to the respondent with accessing pornographic sites was that viruses are distributed on them. Viruses are also prevalent on gambling sites. These viruses load themselves onto the computer and gather information from a user's computer and which then can be distributed onto the Internet. There are also viruses, which can destroy one's computer. The respondent company has specific computers which are dedicated to monitoring computers for viruses. In addition virus protection software is updated on a weekly basis.
The respondent prohibits the viewing of pornographic material as graphics take up space and slows the computer systems.[626]

The applicant signed acknowledging having received a copy of the company's business ethics policy. In addition to the business ethics policy employees are given a Guide to Business conduct; page 26 states that:–
"The company's electronic communications systems are company resources and all electronic communications are regarded as company records. Material such as pornography is not permitted on BHP Billiton systems in any form."
The applicant received copies of all the company's policies. New employees are given a handbook titled Business Ethics at Bayside which states that:–
"Offensive material such as pornography is not permitted in any form."
Furthermore a warning appears on the computer warning users that they are being monitored. An employee has an option to log off.[627]

The commissioner noted that by the applicant misusing his company computer in the manner he had done, the applicant had contravened several company policies and prescripts of which he was

---

[625] supra note 21, at 571 B
[626] supra note 21, at 571 B-E

[627] supra note 21 ,at 571 E-H

well aware and having regard to the excessive nature of the viewing of pornographic sites by the applicant, on one occasion more than 3000 pages of the same, the commissioner held that dismissal was the appropriate sanction.[628]

Racial harassment through the inappropriate use of the company computer e- mail systems has also surfaced in the workplace. In the case of *Cronje / Toyota Manufacturing* [2001] 3 BALR 213 (CCMA); the applicant, a Senior Manager and National President of the Staff Association of the Motor & Related Industries (SAMRI), was dismissed for circulating a cartoon he had received via company e-mail. The cartoon depicted the Prime Minister of Zimbabwe as a gorilla. The cartoon version of Mugabe was holding another smaller gorilla, and was captioned: "*Mugabe and his right hand man. We want the farms to grow more bananas"*. The applicant claimed that he was unaware at the time of the respondent's e-mail policy, and that he had received the cartoon as an attachment to a petition to President Mbeki, requesting him to intervene in the Zimbabwe crisis. The applicant said he had added his name to the petition, and had sent the message and its attachment on to a number of colleagues. Although he was aware of the racial stereotype that associated black people with monkeys, baboons and gorillas, he did not regard the cartoon as racist, and did not regard himself as a racist. The respondent contended that it was obliged to take strict action against racism and e-mail abuse in the workplace, and that it had done so on a number of occasions in the past.[629]

The commissioner rejected the applicant's claim that he had only made one paper copy of the cartoon, and that somebody else had made another copy, and handed it to the shop stewards who had reported him to management. The applicant's assertion that he was "framed" was disingenuous. There was no doubt that the cartoon was racist and inflammatory. It fell into crude, offensive and racist stereotyping developed over centuries that associated black people with primates, that is, beings of lesser intelligence and low morality. The cartoon had to be evaluated in the context in which it was published, i.e. a factory that employs 3 500 black workers in a newly independent South Africa, in the year 2000. The fact that stereotyping exists is a matter of deep moral, cultural and social sensitivity to blacks. Stereotyping cartoons offend people's cultural or

[628] supra note 21, at 574 A-C
[629] *Cronje / Toyota Manufacturing* [2001] 3 BALR 213 (CCMA), at 213 E-G and 215 I-J

racial self-image. The commissioner held that the depiction of a black person as an ape is inherently wrong. The commissioner rejected the applicant's 'belated' claim that he regarded the cartoon as a depiction of Mugabe as the leader of a 'banana republic'. The use of the word 'we' in the caption indicated that not only Mugabe, but others like him, also wanted the farms to grow more bananas. The overwhelming probability was that the applicant knew that the cartoon was racist.[630]

The evidence indicated that the respondent had a rule against the circulation of offensive e-mail material, and that the applicant was aware of it. There was no compelling evidence to indicate that the rule had been inconsistently applied. The courts had made it clear that an arbitrator may not, at whim substitute his or her views on what may be an appropriate sanction for that of the employer. Employers cannot be expected to tolerate racism in the workplace. There was accordingly fair reason for the dismissal of the applicant.[631]

The applicant in the case *of Dauth / Brown and Weir's Cash and Carry* [2002] 8 BALR 837 (CCMA) was dismissed for distributing an offensive e-mail to more than 100 people, including the respondent's senior management. He admitted that he had done so, but claimed that dismissal was too harsh a sanction because he was acting under stress caused by his impending retrenchment and while under the influence of prescription drugs.[632] The applicant also claimed that, as the respondent's business had since been transferred to another company, a continued employment relationship between himself and his new employer was neither untenable nor intolerable.[633]

The applicant had insisted that, apart from derogatory and racist remarks contained in the e-mail, the contents were true. Even though a colleague on whose computer the e-mail was written had been suspended, the applicant had not disclosed that he was author of the e-mail until he failed a voluntary polygraph test. The contents of the e-mail and the manner in which it had been

[630] supra note 27, at 222 F- J and 224 E-F

[631] supra note 27, at 224 F-G

[632] *Dauth / Brown and Weir's Cash and Carry* [2002] 8 BALR 837 (CCMA) at, 842 D-E

[633] supra note 30, at 842 G-J

distributed indicated that the applicant was fully in control of himself when he composed the message.[634]

As to the applicant's attempt to downplay anti-Semitic remarks in the e-mail, the commissioner rejected the applicant's claim that no weight could be given to these remarks unless the person about whom they were made testified. This approach, and the applicant's plea for reinstatement, indicated that the applicant was either unaware of the shocking nature of the comments in the e-mail, or was totally without remorse.[635]

The dismissal of an employee is justified if his or her conduct was of such a gravity that it makes continuing the employment relationship intolerable.[636]

In *Philander / CSC Computer Sciences* [2002] 3 BALR 304 (CCMA); the applicant was charged with a contravention of the respondent's electronic communications policy in that he had intentionally and knowingly accessed sexual and/or pornographic material of an offensive nature and forwarded it via CSC's electronic communication system to Old Mutual staff as well as other external clients on specified dates and times.[637] He acknowledged knowing that the e-mail content was not allowed according to CSC policy and that he had seen and was aware of the policy document.[638] When confronted with the charge, the applicant had initially admitted to sending e-mails in contravention of the respondent's policy. The applicant claimed later, however, that he had admitted only to transgressing the e-mail policy of his former employer.[639]

The applicant was dismissed for forwarding pornographic material on the respondent's e-mail system.

---

[634] supra note 30, at 842 G-J

[635] supra note 30, at 846 A-J

[636] Schedule 8 Code of Good Practice on Dismissal, section 3(4)

[637] *Philander / CSC Computer Sciences* [2002] 3 BALR 304 (CCMA) at 311 I-J

[638] supra note 35, at 312 A-B

[639] supra note 35, at 312 A-B

In an appeal, the commissioner held that the choice of an appropriate sanction did not only depend on its nature. The sanction depended also on the particular facts of the case, and on the reasons that may justify a more severe penalty.[640]

The applicant had neither shown repentance for his conduct, nor had he apparently appreciated the harm that could have resulted from his conduct. This attitude indicated that the employment relationship had been destroyed. The commissioner held that the attitude of the applicant towards his employer was the main reason why the maximum penalty of dismissal was justified: [641]

> *"I have great difficulty in finding a reason why an employer should tolerate such attitude from an employee and how an employee can expect the employer to tolerate a continuation of the relationship in such circumstances".*[642]

In *Jardine / Tongaat Hulett Sugar Ltd* [2002] 4 BALR 426 (CCMA); the applicant, a middle manager, was dismissed for 'incompatibility' after he lodged a grievance against a senior manager. The grievance was caused by an incident in which the senior manager reminded the applicant of the time he was required to start work. The applicant alleged that the senior manager had rebuked him in the presence of other members of management. The senior manager denied having done so. The respondent found that there was no substance to the applicant's complaint. A disciplinary hearing was convened, and the applicant was dismissed. The respondent contended that the dismissal was the culmination of a series of unsuccessful counselling sessions.[643]

At the CCMA hearing, the commissioner held that the respondent's case against the applicant is essentially this: the manner in which he framed his grievance against the General Manager was

[640] supra note 35, at 316 B

[641] supra note 35 , at 316 C

[642] supra note 35, at 316 D

[643] *Jardine / Tongaat Hulett Sugar Ltd* [2002] 4 BALR 426 (CCMA) at 426 E-G

dramatic evidence of a pattern of behaviour that had been manifested for years.[644] The applicant's entries in the Process Manual and the way in which he used e-mail are two significant illustrations of this pattern. The review meetings are evidence of a consistent attempt by the Respondent to warn and counsel the applicant. The warning letter, plus other verbal warnings, signalled to the applicant that his behaviour was regarded as misconduct. The commissioner held that the pattern of incompatibility justified dismissal.[645]

Due the fact that the e- mails resulted in the working relationship between the applicant and the respondent becoming intolerable the commissioner held that the dismissal of the applicant was unfair, but did not order reinstatement or re-employment. The respondent was to pay compensation to the applicant in the sum of R121 920 (One hundred and twenty one thousand, nine hundred and twenty rand).[646]

In the case of *Volkwyn / Truworths Ltd* [2002] 4 BALR 455 (CCMA); the applicant, who worked as an assistant in the corporate management dining room of the respondent's headquarters, had a steamy relationship with the manager of the dining room, one DT (not her real name), who was employed by a catering company. The relationship included the exchange of suggestive and indecent SMS (text) messages, clandestine meetings, suggestive remarks and physical contact during and outside working hours. When the catering company learned of the affair, the manager was dismissed.[647]

---

[644] supra note 41 , at 439 B-D

[645] supra note 41 , at 439 B-D

[646] supra note 41 , at 444 B-H – ("Both the tone and appearance of the article, which goes out of its way to soil the respondent's public image indicates an active and willing participation by the applicant. Hence I would have been persuaded by it that, by participating in it, the applicant had made continued employment intolerable and denied her re-instatement or re-employment. While employees have a right to freely express their grievances against their employers in the press, they do so at the risk of forfeiting their right to re-instatement or re-employment because high profile mud slinging – particularly when the employer's business depends on a positive public image – makes a continued employment relationship intolerable.")

[647] *Volkwyn / Truworths Ltd* [2002] 4 BALR 455 (CCMA) at 456 E-I

The applicant claimed that he had been sexually harassed by the manager, and denied any relationship with her. He also claimed that because the SMS messages had been sent outside working hours, the respondent lacked authority to discipline him for this conduct. The respondent claimed that the applicant had willingly consorted with DT, and that his behaviour, which was known to other employees ; with the exception of his girlfriend, who also worked in the dining room ; had the potential to disrupt the workplace.[648]

The respondent's employee relations manager, Ms Helen Drabbe argued that it was highly unlikely that the SMS messages were only sent from Volkwyn's residence after hours. The nature and content of some of the messages referred to issues only known at the workplace and related to certain incidents. She argued that even if the SMS messages were only sent after hours, they had a profound effect on morale and relationships in the workplace and exacerbated an already bad situation.[649]

The commissioner held that the impression left by the evidence was of two people blatantly flaunting social, ethical and workplace rules and conventions. The SMS messages had become common knowledge and had had a disruptive effect on discipline and relationships in the workplace.[650]

The commissioner held that although most of the SMS messages had been sent after hours from home, they were received and read during working hours and had led to gossip, breakdowns of relations, improper behaviour, and had had a host of other unacceptable effects which the respondent could not be expected to tolerate. The applicant's record indicated that he had difficulty conforming to acceptable standards of behaviour, and he had displayed a total lack of judgement. The commissioner held further that such behaviour is generally unacceptable and the average

---

[648] supra note 45 , at 457 F-H and 460 A-E

[649] supra note 45, at 457 I-J

[650] supra note 45, at 460 G-H

employer would certainly have taken the same steps that respondent did.[651]

The commissioner held that the employer had proven on a balance of probabilities that it had sufficient reason to discipline Volkwyn for sending SMS messages and for the effect those messages had on the working environment and staff involved.

Thus the dismissal was justified.[652]

In the case of *Sylvester / Neil Muller Constructions* [2002] 1 BALR 113 (CCMA); the applicant was dismissed after forwarding a crude sexual 'sms' (text) message to a female colleague's cellular telephone. The woman claimed later that she had been sexually harassed. The applicant stated that he was not aware that the messages offended his colleague as he has shared jokes and innuendoes of a sexual nature with her in the past. The commissioner held that sexual harassment consists of unwanted and persistent sexual advances and or suggestions. The court held that the person who claims that he or she was offended by the said conduct must make it clear to the offender that he or she objects to the that conduct. The offender must thus be aware that his conduct is unwanted and unappreciated.[653]

The commissioner found that in this case, the applicant's conduct amounted to just a single act. Thus he had no reason to think that his colleague will take exception to it.
The applicant was thus awarded an amount that was equivalent to 12 months' salary.[654]

In the case of *Sugreen / Standard Bank of SA* [2002] 7 BALR 769 (CCMA); the applicant, a managerial employee (Ms Sugreen), was dismissed for alleged corruption. The main evidence against her was a tape recording of a telephone conversation with one of the respondent's service

[651] supra note 45, at 461 B-D

[652] supra note 45, at 461 G-H

[653] *Sylvester / Neil Muller Constructions* [2002] 1 BALR 113 (CCMA) at 113 E-G
[654] supra note 51, at 113 E-G

providers (Mr Singh). The recording was made by Mr Singh, the person who allegedly offered the applicant a bribe. Apparently Mr Singh paid R 30 000 to Ms Sugreen to keep his company on her employer's panel of service providers. Mr Singh later reported the matter to the respondent.[655] The applicant was dismissed on the basis of the information on the tape. The applicant denied that she had received a bribe, and claimed that the tape was a compilation of a series of actual telephone conversations, and that they were inadmissible because the recording of her conversation had *inter alia* breached her right to privacy.[656]

Mr Vahed (for the applicant) argued that the tape recorded conversation is inadmissible for the following reasons: [657]

a) It constitutes an invasion of the applicant's rights;

b) While it is conceded that there are times when such evidence may be admitted, the role of the employer itself in recording is crucial. In the present case the employer had made it clear that it did not want to get involved with entrapment and this was then done by a third party;

c) It is appropriate to take into account the credibility and calibre of the witness before deciding on the admissibility of the recording. In this case on his own admission the witness had been prepared to pay a R30 000 bribe, and had previously been convicted of theft.

---

[655] *Sugreen / Standard Bank of SA* [2002] 7 BALR 769 (CCMA) at, 770 G-J and 771 A-I

[656] supra note 53, at 772 A-B

[657] supra note 53, at 772A-B and C-F – ((Mr Vahed argued there is authority to support a finding of inadmissibility. The commissioner referred to *Cape Town City Council v South African Municipal Workers Union obo Beukes and Dollie* (2000) 21 *ILJ* 2409 (LAC) where Stelzner AJ held that the dismissals were unfair because he was "satisfied that there were (and still are) adequate remedies available to the Council as employer to protect its interests without unfairly prejudicing its employees. The Council could have conducted itself differently (or directed the operations of, or mandate it supplied to, its agents) in a manner that would not have caused this Court to conclude that the interests of justice had been unduly affected." The court did however add that it could not be said that a system of trapping could never be fair in the employment context. I was also referred to *Moonsamy v The Mailhouse* (1999) 20 *ILJ* 464 (CCMA), a case where evidence had been obtained by bugging a telephone conversation of an employee at the premises of the employer. The Commissioner said "If the employer could show that the telephone interception was, in the circumstances, the only method available of securing evidence against the employee, in circumstances where the employee was clearly causing harm to the employer, then perhaps the use of telephone tapping could be justified" (at 472D). In this case it was held that there were other more conventional means for the employer to have gathered its evidence. The evidence was ruled inadmissible on that basis.)

Mr Pillimer (for the respondent) argued that the tape was admissible for the following reasons:[658]

a) The conversation between the applicant and the witness was not a fabrication; it had been admitted by the applicant.

b) There was strong authority in both criminal and civil court decisions that such evidence did not constitute a violation of the privacy right.

c) Section 138 of the LRA obliges the Commissioner to determine the manner in which the arbitration should be conducted, that is, 'fairly and quickly', dealing with the substantial merits of the dispute with the minimum of legal formalities'. In light of the above, Mr Pillimer submitted that the Commissioner has discretion to admit such evidence.

The commissioner held that use by employees of their employer's telephone and e-mail facilities are of legitimate interest to the employer if there is reason to suspect that the employee is guilty of misconduct. The commissioner held further that it was also necessary to evaluate the fairness of the employer's actions. The following considerations were relevant in this regard:[659]

- the recording was not aimed at enticing the applicant to commit a crime;
- because the alleged crime had already been committed, there were few other methods of securing evidence against the employee;
- the recording was not part of an on-going monitoring of all the applicant's calls;
- the recording was not undertaken by the employer itself;
- the recording was made during working hours, using the employer's telephone. The tape

---

[658] supra note 53, at 772G- J and 773 A-B- (In *S v Kidson* 1999 (1) SACR 338 (W) it was held that participant monitoring was not prohibited by statute, and the tape recording of a conversation constituted no violation of any discernible privacy interest. Cameron J placed emphasis on the fact that the conversation was with someone to whom no confidentiality was owed, and the speaker ran the risk that what was said could be imparted to someone else. In these circumstances there was no constitutionally cognisable breach of privacy. So to in *TAP Wine Trading & Another v Cape Classic Wines (WC) CC* 1994 (4) SA 194 and in *S v Dube* 2000 (2) SA 583 (N) was it held that participant monitoring and surveillance was neither illegal nor a breach of the right to privacy).

recordings were accordingly admissible.

Based on these grounds the commissioner was prepared to accept that there has been no constitutionally cognisable breach of privacy in this case.[660]

The commissioner held that the tape was believable in that it reflects a normal conversation with interjections and interruptions, with the participants reacting to each other's comments and questions.[661] The court confirmed that an employee's privacy rights were not infringed by telephone monitoring.

The commissioner held that the implication of the bribe by means of the taped conversation, is that it shifted the burden to Ms Sugreen, to prove that she had been framed.[662]

The commissioner held that the applicant had not shifted the onus placed on her when she raised the defence of a fabricated tape. With the result the commissioner held that he was left with a coherent and plausible tape recording with many aspects that are damaging to the applicant.[663] The respondent, the commissioner held, had adduced sufficient evidence to establish, on a balance of probabilities, that the applicant accepted a bribe of R30 000.[664]

---

[659] supra note 53, at 773 A-B

[660] supra note 53, at 773 A-B (It is sufficient to recognise that the use by the employee of the employer's telephone and e-mail are legitimate areas of interest to the employer where it suspects that the employee is guilty of misconduct).

[661] supra note 53, at 777 C-D and E-J

[662] supra note 53, at 777 C-D and E-J (With this defence, the onus shifted to her to establish the probabilities of this, by showing (a) that Singh had a motivation to frame her; (b) that a fabrication of a tape is possible; (c) Singh had the ability to fabricate a tape and (d) that there are adequate explanations to her own words on the tape. Of these three factors, only the first was suggested with any reasonable explanation, but the respondent offered an equally plausible motivation, namely anger. No expert evidence was led as to the ease with which an apparently normal-sounding conversation can be created from several other conversations, nor that Singh had the equipment or know-how to fabricate a tape).

[663] supra note 53, at 778 D-H

[664] supra note 53, at 778 D-H [Section 192(2) of the LRA requires the employer to prove that the dismissal is fair; this

The applicant had not discharged the burden, and so her dismissal was confirmed.

Similarly in the case of *Allied Workers Union of South Africa obo Ncube v Northern Crime Security CC* (1999) 20 ILJ 1954 (CCMA); this case concerned an abusive employee Ncube, who used abusive language towards another employee (Koekemoer) and threatened to kill him and assault his wife. Ncube was dismissed on the basis of the threats made. The arbitrator allowed the tapes on the basis that the recorded conversations did not show evidence of private conversations between Ncube and third parties, but between the two employees involved. The CCMA held that Koekemoer had a legitimate interest in recording the conversation because of the threats made towards him, and the conversations did not reveal any personal or confidential information about Ncube. The tapes were confirmatory evidence of communication in the course of the employment relationship, and the recording was made to support the oral evidence. The evidence the commissioner held could also have been submitted as hand -written notes.[665]

The cases discussed above not only serve as a reminder for employers to keep a 'watchful eye' on their employees but also provides strong argument in their favour for a need to monitor the activities of their employees. Failure to do so may potentially result in the employer suffering huge losses.

---

must be done on a balance of probabilities (See *Cycad Construction (Pty) Ltd v CCMA & Others* (1999) 20 *ILJ* 2340 (LC) 2344A–E)]. In elaboration of the employer's onus, John Grogan in *Workplace Law* (5 ed 2000) 111 states**:** "The primary significance of the onus is that when the evidence on a point is evenly balanced or indecisive, the balance will tip against the party upon whom it rests. It must be noted, however, that the burden of proving a particular point may shift to the party not bearing the onus, on the basis of the principle that 'he who alleges must prove'. So for example, if an employee accused of theft pleads an alibi, the burden rests on him or her to prove that he or she was elsewhere at the time of the commission of the offence. If he or she fails to discharge the evidentiary burden, it may be that the employer will be held to have discharged its overall onus."

[665] Case extract from: A Dekker. "Vice or Devices: Employee Monitoring in the Workplace". (2004) 16 *SA Merc LJ*

CHAPTER 6

Responding to potential abuse.

Employers may seek to reduce abuse of electronic tools by resorting to disciplinary solutions and procedures.

The size of the task, the number of users, their use patterns, their usual tasks and the scope, size and power of network facilities and resources may all play a role in determining what kind of response the employer is going to take in order to restrict or rather terminate abuse.[666]

It must be noted that any disciplinary action arising in the context of computer network abuse, Internet, text messaging, telephone calls and even e- mails must comply with the requirements contained in Schedule 8 of the Labour Relations Act 66 of 1995.[667] The Act provides that disciplinary action must be fair and consistent and that disciplinary rules must be clearly communicated to all employees.[668]

It is not necessary for an employer to deal with electronic abuse separately but, the abuse may be processed and dealt with in terms of an existing schedule of offences.[669] For instance, Internet abuse or abuse through the telephone may fall into the category of sexual harassment or creating a hostile working environment, (which may occur through the display of sexually explicit material on the computer screen or through a text message).[670] Bad conduct like insolence and insubordination expressed in an e- mail message retains its character as a disciplinary offence. Such offences does not require the formulation of a new disciplinary code to deal specifically with the abuse that may occur through the electronic equipment that is made available to an employee in

---

634-635

[666] C Mischke "Disciplinary action and the Internet". (1999) 9 (5) *CLL* 43

[667] J Grogan. *Workplace Law*. 8ed. (2005) 105-106

[668] Ibid

[669] Mischke op cit note 1, 43

[670] Ibid

the workplace.[671]

Another method by which it could be possible to respond to other forms of abuse with respect to the electronic communication tools in the workplace by employees is by relating that abuse to misuse of employer's property and the inadvertent downloading of viruses and failing to use anti virus – protection software.[672]

There are however certain limitations that arise by simply relating an offence to be categorised into one of the abovementioned offences and thus may call for specific measures to be formulated and communicated to employees.[673] In determining whether or not the employer prefers to specifically address the problem will depend on a variety of factors, such as, the number of employees regularly using the network, the computer resources available , cost implications and abuse , and the future possibilities of abuse by employees.[674]

The punishment handed down for the abuse of electronic tools[675] in the workplace should involve both progressive and corrective discipline, and as a last resort dismissal should be contemplated (for cases such as those involving sexual harassment of co -workers using e- mail, and text messages). Counselling is also a viable option for less serious abuses for instance the viewing of pornographic material by an individual employee.[676]

As stated above dismissal for the abuse of employer's electronic tools must be the last resort. An employer therefore in order to alleviate the abusive conduct of the employee or employees before

---

[671] Ibid

[672] Ibid

[673] Ibid

[674] Ibid

[675] L Michalson "The use of the e- mail and the Internet in the Workplace" *Cyberlaw S.A: the internet and the law*. CD-ROM (1999) 196 defines electronic tools as :

- telephones, mobile phones and voice-mail facilities
- e-mail facilities
- fax machines, modems and servers
- computers
- network tools (e.g. Internet browsers and Internet access facilities)

actual dismissal may proceed in the following manner.

The employer may issue:

a) General warnings

Warnings may be general or specific.[677] General warnings are normally issued to employees informing them of the rules that the employer has put in place and that are instituted to regulate the workplace. These types of warnings are frequently used to signal to all employees that the employer intends to take action against specific forms of misconduct. These rules are not sanctions in themselves but their purpose is to ensure that employees cannot later claim that they were unfairly or inconsistently treated if the employer acts on the general warning.[678] If employees are not given a general warning the conduct on which they have embarked may lead to dismissal, their dismissal may be ruled unfair.[679]

b) Informal warnings

Informal warnings are those given to individual employees for particular acts of misconduct. These warnings act as reminders that should the conduct continue, more serious action will follow.[680] The purpose of specific warnings is to inform and advise the employee concerned of defective standards of performance or behaviour, to remind him or her of the existence of the rule that has been breached or overlooked.[681] If the employees are not informed after committing an offence, then when disciplinary action is taken they would argue that they had a right to believe that their actions did not deserve any disciplinary action. The purpose of the warning is to correct the defective conduct in whatever form that conduct may have taken. Informal warnings may also

---

[676] C Mischke. "Dismissal for abuse of e- mail". (2002) 11 (6). *CLL* 51

[677] Grogan op cit note 2, 98, see also *SA Polymer Holding t/a Magpak* (1996) 8 BALR 978 (LAC), in which the dismissal of the employees was ruled unfair because they had not been warned that failure to obey a particular instruction would lead to dismissal).

[678] Ibid

[679] Ibid

[680] Ibid

[681] Ibid 99

be in the form of an oral warning.[682]

c) Written warnings

A written warning is more formal than an oral warning.[683] The purpose of a written warning is that it enables the employer to prove that the warning was given subsequent to a disciplinary action. This is important should disciplinary action prove necessary against that employee. An employee is normally required to sign a written warning. However a refusal by an employee to sign a written warning does not affect its validity.[684]

d) Final written warning

A final written warning is the last warning an employee can expect before dismissal. The purpose of a final written warning is to give employees a final chance to correct their behaviour. Such warnings must not be issued lightly or prematurely.[685]

e) Denial of privileges

The Code of Good Practice on Dismissal (item 3 (3)) states that infringement of workplace rules may call for a final warning 'or other action short of dismissal'. This leaves open a wide range of options, such as deprivation of a portion of discretionary bonuses, or other special privileges which the employer may grant (for example, special leave, or other privileges attached to long service).[686] Employer's may not however impose fines on employees, or make any deductions from their salaries for disciplinary offences without their consent in writing.[687]

---

[682] Ibid

[683] Ibid

[684] Ibid, see also case of *Chemical Workers Industrial Union & another v AECI Paints (Natal) (Pty) Ltd* (1988) 9 ILJ 1046 (IC), the court ruled a dismissal unfair because the employer had not given consideration to the circumstances in which the earlier warnings had been given.

[685] Ibid, see also the case of *Changula v Bell Equipment* (1992) 13 ILJ 101 (LAC) , where the court found that the final written warning that had been issued to the employee before his dismissal was unjustified , and that the dismissal was therefore vitiated (at 109f)

[686] Ibid 101

[687] Section 34 of the Basic Conditions of Employment Act 75 of 1997.

f) Suspension

Employers may suspend employees by dismissing them and re- engaging them after a suitable interval.[688]

g) Demotion

At common law and under the Basic Conditions of Employment Act 75 of 1997, demotion raises problems similar to suspension because it constitutes a unilateral variation of the employee's contract of service.[689] Unfair suspension, unfair demotion constitutes unfair labour practice. However, demotion is considered acceptable if it is provided for in a disciplinary code.[690]

h) Dismissal

The Code of Good Practice: Dismissal advises all employees to adopt disciplinary rules that establish a standard of conduct required for their employees. As to the contents of workplace rules, the Code states:[691]

> *"The form and content of disciplinary rules will obviously vary according to the size and nature of the employer's business. In general, a larger business will require a more formal approach to discipline. An employer's rules must create certainty and consistency in the application of discipline. This requires that the standards of conduct are clear and made available to employees in a manner that is easily understood. Some rules may be so well established and known that it is not necessary to communicate them".*

Although workplace rules emanate form different sources, they generally give rise to legally

[688] Grogan op cit note 2, 102 [It is also implicit in the Labour Relations Act 66 of 1996, [s 186 (2) (b)] – the prohibition therein of unfair suspension necessarily implies that legislature accepts that in certain circumstances suspension will be fair and hence permissible].

[689] See s 186 (2) (a) of the LRA 66 of 1996

[690] Grogan op cit note 2, 103

[691] Schedule 8 Item 3 (1)

enforceable rights.[692] An infringement of one of these rules entitles the employer to institute disciplinary action against the offender. The nature of a permissible sanction depends on the importance of the rule and how many instances has that rule been contravened by an employee.[693]

Both the Labour Relations Act 66 of 1996 and the common law state that employees have a duty to abide by rules that are reasonable. The employer's right to formulate disciplinary rules does not give them the inalienable right to frame and enforce rules that are unreasonable.[694]

A reasonable rule is said not enjoin the impossible or illegal, does not discriminate unnecessarily between different classes of workers, and is not 'sprung' on workers out of the blue.[695] The broad principle is that a disciplinary rule must be designed to promote the efficiency of the enterprise, in other words it must have some kind of economic rationale.[696]

Grogan provides the following check list to asses the validity of a workplace rule and the legality of sanctions for infringements of such a rule:[697]

- Did the employer have the authority to make the rule in terms of the employment contract.
- Does the rule comply with applicable statutes or regulations.
- Is the rule reasonably required for the efficient, orderly and safe conduct of the employer's business?
- Was the existence of the rule known to the employee, or could/ should the employee reasonably have been expected to have known of its existence.
- Has the rule been consistently applied in similar cases in the past?

[692] Grogan op cit note 2, 93- 94

[693] Ibid

[694] Ibid 94- 95

[695] Ibid

[696] Ibid 95

[697] Ibid

Only if the answer to each of these questions is in the affirmative will the rule be enforceable, if the answer is "no" to any of the above questions the employee may not be fairly disciplined for breaching it.[698]

An employer is not required to spell out every workplace rule in meticulous detail; the test is whether the employees concerned were actually aware, or should have been aware, of the rule and the consequences of non- compliance.[699]

The Code of Good Practice on Dismissal provides that any person who is determining whether a dismissal for misconduct is unfair should consider:[700]

(a) whether or not the employee contravened a rule or standard regulating conduct in, or of relevance to, the workplace; and
(b) if a rule or standard was contravened , whether or not
    (i) the rule was a valid or reasonable rule or standard;
    (ii) the employee was aware , or could reasonably have been expected to be aware , of the rule or standard;
    (iii) the rule or standard has been consistently applied by the employer;
    (iv) dismissal was an appropriate sanction for the contravention of the rule or standard.

In the case of *Bamford & Others/ Energiser (SA) Ltd* (2001) 12 BALR 1251 (P), the arbitrator's findings are insightful for employer's who rely on computer driven workstations and workflows and lays the foundation for successful workplace disciplinary measures to be taken against employees who abuse e-mail.

In this case the facts of which were discussed earlier, the arbitrator held that the employer at the time of the disciplinary infractions did have a comprehensive policy with regard to e- mail and

[698] Ibid 95- 96

[699] Ibid 96

Internet abuse. Relevant in this regard was the message the managing director sent to all users in response to the political message received from the employee. The director regarded that response as an instruction to all e- mail users. The company also had in place a "Business Practices and Standards of Conduct" policy which was pinned on the notice board. This policy document which is referred to in the letters of appointment, prohibits actions that lead to a hostile working environment and instructs employees not to engage in harassment. Furthermore , an e- mail message had been sent out to all users setting out the rules of computer use, the message clearly instructed and affirmed that these computers were business tools intended for business use, and indicated that employees did not have the time to engage in non business related e- mail and internet activities. This e- mailed message also indicated that the Business Practices and Standards of Conduct Policy was applicable in respect of electronic information. The arbitrator also mentioned the importance of what he called 'the common sense implications of the employment relationship'.[701]

The most fundamental and important questions that remained in the present case was whether or not there was a clearly communicated workplace rule in terms of which employees were given to understand that they were not permitted to send chain letters, or to engage in exchanges in pornography or trademark infringements. According to the arbitrator there was:

> *"As to the socially unacceptable material, the text of the standard policy document, of course, does not in as many words spell out prohibitions in respect of e-mail usage. There is however quite enough in the text of that policy, had any of the individuals bothered to pay attention to it, to indicate to them that the 'tone' of the workplace was expressly regulated by the employer. The individuals in question are all middle class articulate young women who are not bereft of education. To suggest that they thought that it was permissible to use company resources to entertain themselves with images which would have been regarded generally speaking as socially unacceptable is not credible. Their claim that they thought there was nothing offensive with it, is of course, in part, undermined by Oosthuizen's evidence that she was indeed offended by the bouquet of penises sent to her, and untenable on the basis that the material is so obviously contrary to*

[700] Code of Good Practice on Dismissal , Item 7
[701] *Bamford & Others/ Energiser (SA) Ltd* (2001) 12 BALR 1251 (P),at 1260 C

what would circulate amongst self-respecting people. In my view, it cannot lie in the mouth of well educated white-collar workers like Wollenschlaeger and Gibson to say that they were unaware that it was impermissible for them to traffic in what was socially unacceptable material. Those jokes which have a racial connotation, are typical of what one would strive to avoid in contemporary South African society. Although it is probable that such humour is enjoyed in private, it can hardly be said that in the work place an employer would and should condone such exchanges.

In my view, even if the facts were to demonstrate a deafening silence in regard to any express regulatory regime concerning the tone of material which could be trafficked on the company e-mail system, it would follow from an application of common sense that images as grotesque as those which I have described do not belong in the work place and the applicants must have realised this fact".[702]

The employees argued that they were not aware of the fact that they could be dismissed because of sending the e- mail. The arbitrator dismissed this argument, stating that whilst there was, indeed, nothing in the documentation that linked the abuse of the e- mail facility to dismissal, there was sufficient grounds to dismiss the employees. The employees' actions had damaged the employer, most obviously, said the arbitrator, by clogging up the system and running up costs. There was also significant risk that the domain name of the employer would be associated with obscene, degrading or offensive transmissions, and the trademark violations could also contain a risk for the company. The arbitrator held that some things could not be denied:

"The axiomatic risk upon commission of a serious transgression, calculated to embarrass one's employer, is dismissal. The applicants' denial of an appreciation of that fact is not credible".[703]

In the case of *Cronje/ Toyota Manufacturing* (2001) 3 BALR 213 (CCMA*)* the arbitrator was guided by Schedule 8 of the LRA (item7) as well as (section 188 (2) of the LRA) which lays down

[702] supra note 36, at 1268 B-H

[703] supra note 36, at 169 E-F

the guidelines to be taken into account by any person who is called upon to decide whether a dismissal was fair.[704]

The arbitrator held that Mr Cronje had contravened the rule prohibiting the distribution of racist and inflammatory material. The arbitrator held that Mugabe appearing as a gorilla, and calling for more bananas, commonly fits into the historical racist white stereotype that still lives in the minds of white people in this country and elsewhere, that associates black people with gorillas, monkeys and the like. It was found that the applicant knew the cartoon was racist was thus was sufficiently moved to pass on to colleagues.[705]

The arbitrator had to consider whether the employer's rules or policies against the distribution of racist and inflammatory material were valid and reasonable.

The arbitrator held that the company's code states that breach of this rule may result in severe disciplinary action. Severe disciplinary action was defined as including dismissal.[706] With regard to the reasonableness of the code, in this case regard was made to the context of the workplace. In the arbitrator's view, the fact that the company employed 3 500 black workers, it was eminently reasonable to include a rule prohibiting the distribution of racist and inflammatory material.[707]

The applicant in this case conceded that he knew that the distributing of pornographic and racist material was wrong.[708]

The arbitrator held that with regard as to how the employer had dealt with previous cases the rule

---

[704] *Cronje/ Toyota Manufacturing* (2001) 3 BALR 213 (CCMA*)* at 221 H-J

[705] supra note 39, at 223 F-J

[706] supra note 39, at 224 A-C

[707] supra note 39, at 224 A-C

[708] supra note 39, at 224 D-E

was consistently applied.[709]

In deciding whether dismissal was the appropriate sanction for contravening the rule, the arbitrator stated that dismissal is justified where:

> *"Where the disciplinary offence has "the effect of seriously damaging or destroying the relationship between employer and employee so that the continuance of that relationship could be regarded as intolerable"; where the relationship of "trust, mutual confidence and respect cannot continue, where the relationship is irreparably harmed and where continuation of the relationship would be futile".*[710]

The Code adopts a similar approach. It provides that if the misconduct is serious and of such a gravity that it makes a continued employment relationship intolerable, then dismissal is the appropriate sanction.[711] The Code of Good Practice in schedule 8 of the LRA provides that if the misconduct is of such gravity that it makes a continued employment relationship intolerable, then dismissal is an appropriate sanction.[712]

The dismissal of the applicant was held to be fair.

In the case of *Philander/ CSC Computer Sciences* (2002) 3 BALR 304 (CCMA) (a case involving an employee forwarding pornographic material on e-mail); the applicant acknowledged that he knew that specific e- mail content was not allowed according to CSC policy and that he had been aware of the policy document.[713]

The arbitrator held that it is trite law that before an employee can be disciplined there must be a

---

[709] supra note 39, at 224 F-G

[710] supra note 39, at 224 I-J

[711] supra note 39, at 225 A-B

[712] Schedule 8 Item 3 (4)

[713] *Philander/ CSC Computer Sciences* (2002) 3 BALR 304 (CCMA) at 312 B

rule, that the rule must be reasonable and that the employee must have been aware of it before he can be held responsible.[714]

The arbitrator held that the sanction to be imposed depends largely on the specific facts of the particular matter.[715] There may be other reasons why a more severe penalty may be appropriate.

In this case the arbitrator held that the applicant had shown no appreciation of the potential harm of his transgression but also no repentance for what he done, seeking rather to feign lack of knowledge.[716] The arbitrator held further that he could find no reason why an employer should tolerate such behaviour from an employee an also tolerate a continuation of the employment relationship.[717] The dismissal of the applicant was found to be fair.

In the case of *Volkwyn/ Truworths LTD* (2002) 4 BALR 455 (CCMA) (a case that involved the exchange of indecent text messages by an employee); the arbitrator held that text messages that had only become evident in the workplace, had led to gossip, breakdown of relations, improper behaviour and a host of unacceptable issues which the respondent employer could not be expected to tolerate. It was further held that the text messages affected the general morale and atmosphere in the work place and that such behaviour is generally unacceptable and that the average employer would be justified in taking the same steps the employer had taken.[718] The arbitrator held that there was sufficient reason to dismiss the applicant and thus the dismissal was justified.[719]

In the case of *Kalam/ Bevcap (Nampak)* (2006) 6 BALR 565 (MEIBC); the arbitrator held that employer must prove on a balance of probabilities that an employee is guilty of misconduct.[720]

---

[714] supra note 48, at 314 B

[715] supra note 48, at 314 B

[716] supra note 48, at 316 C-E

[717] supra note 48, at 316 C-E

[718] *Volkwyn/ Truworths LTD* (2002) 4 BALR 455 (CCMA) at 461 C-D & F-G

[719] supra note 53, at 461 G-H

[720] *Kalam/ Bevcap (Nampak)* (2006) 6 BALR 565 (MEIBC); at 567 F

The applicant committed an offence by contravening the company's Information Technology (IT) policy (all employees including the applicant are consistently alerted each time they log onto the Internet that all internet browsing are monitored and if non- performance to the company's IT policy is detected, the details will be passed to the responsible line and Human Resource (HR) management for investigation or possible action).[721] In terms of the company's code of conduct the unacceptable conduct and excessive use of the internet is viewed as serious and dismissible offence.[722] The applicant did not dispute the existence of the policy but alleged that he did not read it. According to the arbitrator this did not constitute an acceptable excuse. The fact that the applicant spent 285 hours per week and visited 14 802 sites on the Internet on non work related activities was in the eyes of the arbitrator deplorable. The applicant down loaded pornographic pictures on many occasions even though he was warned via pop up messages that these sites were restricted for use through his computer, this according to the arbitrator showed that his actions were well orchestrated.[723]

The arbitrator held that in viewing the pornographic material and sexually explicit images the applicant's behaviour poses serious concerns about his lifestyle.[724]

Thus it was held that the respondent had an obligation to take strict action against abuse of the company's Internet facility. The arbitrator found that the IT Policy was both valid and reasonable. [725] It terms of the company's disciplinary code the failure to adhere to the rule above is a dismissible offence. The fact that the respondent held a managerial position, the arbitrator was convinced that the trust relationship had been severely destroyed. Thus the dismissal was held to be fair.[726]

---

[721] supra note 55, at 566 B – D

[722] supra note 55, at 566 E

[723] supra note 55, at 567 G-I

[724] supra note 55, at 567 J

[725] supra note 55, at 568 A-B

[726] supra note 55, at 568 A-B

In the case of *Latchmiah/Billiton Aluminium SA (PTY) LTD T/A Bayside Aluminium* (2006) 6 BALR 569 (MEIBC) (a case that involved a senior employee viewing undesirable material on the internet); page 5 of the respondent's Business Ethics Policy paragraph 4 states that;
"The company's electronic communications systems are company resources and all electronic communications are regarded as company records. Offensive material (for example, pornography or material of a sexist nature or racist nature) is not permitted in any form".[727]

The applicant signed acknowledging having received a copy of the company's business ethics policy. In addition to the business ethics policy employees are given a guide to Business conduct.[728]

In addition to the business policy employees are given a guide to Business Conduct.
The Guide to Business states that:
"The company's electronic communications systems are company resources and all electronic communications are regarded as company records. Thus the viewing of material, such as pornography is not permitted on BHP Billiton systems in any form".[729]

The applicant received copies of all the company's policies. New employees are given a handbook titled Business Ethics at Bayside which states that:
"Offensive material such as pornography is not permitted in any form".[730]

Furthermore, a warning appears on the computer warning users that they are being monitored. An employee also has an option of logging off.[731]

The arbitrator applied the criteria set out in terms of the LRA.

---

[727] *Latchmiah/Billiton Aluminium SA (PTY) LTD T/A Bayside Aluminium* (2006) 6 BALR 569 (MEIBC) at 571 B

[728]supra note 62, at 571 E

[729] supra note 62, at 571 F

[730] supra note 62, at 571 G

[731] supra note 62, at 571 H

There was overwhelming evidence indicating that the rule was well established. The applicant admitted being aware of the rule against the prohibition of viewing pornographic material on the respondent's Internet.[732]

The rule was found to be reasonable as the company considered this offence as being ethically unacceptable at the workplace during work hours.[733] The rule is seen further as being reasonable as it discourages sexual harassment, offensive material and negates the possibility of hackers infiltrating the company computer systems with viruses which could lead to a loss of information and damage to computer systems.[734] The graphics from pornographic sites also causes an increase of traffic on the business network that slows down the ability of other users on the network to communicate effectively.[735]

The arbitrator was satisfied that the rule was consistently applied. He therefore had to consider whether dismissal was the appropriate sanction.[736]

The arbitrator referred to the case of *County Fair Foods (Pty) Ltd v CCMA & others* (1999) 11 BALR 1117 (LAC) at 112 E-F where Kroon JA held the following:

> *"It remains part of our law that it lies in the first place within the province of the employer to set the standard of conduct to be observed by its employees and to determine the sanction with which non-compliance will be visited, interference therewith is only justified in the case of unreasonableness and unfairness".*

The arbitrator held that due to the excessive nature of the viewing of the pornographic material a

[732] supra note 62, at 572 G-H

[733] supra note 62, at 572 J – 573 A-B

[734] supra note 62, at 572 J – 573 A-B

[735] supra note 62, at 572 J – 573 A-B

[736] supra note 62, at 573 F

policy as such as the one adopted by the employer is necessary.[737] The arbitrator held further the there is a duty on the employer to set standards with regard to employee conduct.[738]

The arbitrator found that the dismissal of the applicant did not produce a sense of shock and that dismissal in this case was necessary to curb such conduct.[739]

Most employees caught (red handed or otherwise) abusing the electronic tools in the workplace should expect get a written warning, and in more serious cases a final written warning. The option of suspension or even possible demotion remains an option for the employer.

An employer may even take disciplinary action against the employee in the form of a dismissal. Where this occurs the employer often has a policy in place that prohibits and discourages the conduct or action in question. The courts have accepted the dismissal provided the requirements in the LRA were met.[740]

[737] supra note 62, at 574 A

[738]supra note 62, at 574 A

[739] supra note 62, at 574 B-C

[740] Mischke op cit note 11 , 55 [In the case of *Bamford (supra)* it was clear that a court may still take disciplinary

CHAPTER 7

Practical steps to prevent the abuse of 'electronic tools' in the workplace

An employer seeking methods to put an end to abuse of company equipment may institute or implement the following:

1. Encryption

It can be made more difficult for an employee to find useful data if the employer somehow scrambles data so that interpretation is meaningless without the intruder knowing how the scrambling was done. The most powerful tool in providing computer security is scrambling or encoding.[741]

Encryption is the formal name for the scrambling process.[742] In this process normal, unscrambled data called clear text is transformed so that they are in unintelligible to the outside observer. The transformed data are called enciphered text or cipher text. Using encryption employers can nullify the value of an interception and the possibility of effective modification and fabrication.[743]

Encryption stresses the need for confidentiality of data. Although encryption is an important tool in any computer security tool kit, other tools must be used to complement its use.[744] If encryption is not used properly, it may have no effect on security and could even degrade performance of the entire system. Therefore it is important that if encryption is implemented it must be used in a manner that it can function effectively.[745]

---

action that is valid and fair even if there was no policy in place].

[741] C P Pfleeger and S L Pfleeger. *Security in Computing*. 4 ed. (2007). 25 see also [R Safavi- Naini & M Young. *Digital Rights Management – Technologies, Issues, Challenges and Systems.* (2006) 228- 277].

[742] Ibid

[743] Ibid

[744] Ibid

[745] Ibid 26

2. Software controls

Programs themselves can be used to protect computer security and thus improve the security for the employer.

Program controls include the following;[746]

- Internal program controls: parts of the program that enforce security restrictions, such as access limitations in a database management program.
- Operating system and network system controls: limitations enforced by the operating system or network to protect each user from all other users.
- Independent control programs: application programs, such as password checkers, intrusion detection utilities, or viruses scanners, that protect against certain types of vulnerabilities.
- Development controls: quality standards under which a program is designed, coded tested, and manipulated to prevent software faults from becoming exploitable vulnerabilities.

3. Hardware controls

Hardware controls devices have been created to assist in providing computer security. These devices include a variety of means:[747]

- Hardware or smart card implementations of encryption
- Locks or cables limiting access or deterring theft
- Firewalls
- Intrusion detection systems
- Circuit boards that control access to storage media

[746] Ibid

[747] Ibid 27

4. Physical controls

In most cases the most effective and least expensive are physical controls. Physical controls include locks on doors, guards at entry points, backup copies of important software and data, and physical site planning that reduces the risk of loss and damage.[748]

5. A User Policy

Upon due consideration the best method to be adopted by the employer to deal with a technology based problem is to formulate an Electronic User Policy.[749] A policy for using e-mail and Internet is generally seen as part of the employer's prerogative to control the workplace. The employer may take the first step and set up a committee involving information technology, industrial relations, human resources, and legal advisors to write a draft and then negotiate in the formulation of this policy.[750]

The purpose, scope, administration, and terminology of the user policy must be assessed against the background of the needs of the business, on the one hand, and the reasonable expectations of employees that the employer will respect their privacy, on the other.[751] It may be open for the employer to identify specific employees such as the system controller and the system administrator to take responsibility for certain issues. Some attention may be given to defining terminology used in the policy as not all employers and employees are familiar with computers.[752]

---

[748] Ibid

[749] M McGregor "The use of e- mail and Internet at Work." (2003) 11 (3) *JBL*191

[750] Ibid

[751] Ibid

[752] Ibid

The User Policy must be centred generally around the following considerations:[753]

- A provision that makes some of the employees aware and reminds others that all electronic resources provided by the employer at the workplace (including the desk top, workstation , hard drives , monitor , printers , networking facilities, telephone, fax machines,) and which are provided for the purposes of the employees work remain , at all times , the property of the employer. [754]
- The electronic resources are intended to be used for work related activities. These works related activities must be consistent with the conduct that can be normally expected from employees.[755]
- The policy must clearly indicate without any ambiguity whether the employer strictly prohibits the personal use of electronic tools by employees entirely or allows them to use it within certain limits.[756]
- Where the policy does allow employees permission to use facilities for personal purposes such use must be regulated. The policy must encompass guidelines for personal use that provides for use that is conducted :[757]
    - responsibly, ethically, and lawfully;
    - that employees must consider and respect the rights of others;
    - they must not overuse the facilities: their use of email for private purposes, for example, must not disrupt network services for business purposes;
    - that in their use employees must not expose the employer to any liability;
    - employees must make it clear that statements outside the scope of their employment represent only their personal opinion and should not be construed as official opinion.

[753] C Mischke. "Disciplinary action and the Internet". (1999) 9 (5) *CLL* 43- 45 [see also M McGregor. "The use of e-mail and Internet at Work." (2003) 11 (3) *JBL* at 191-192

[754] Ibid

[755] Ibid

[756] Ibid

[757] Ibid

- Employees must be informed that they should have no expectation of privacy in relation to information (files, messages, web access information) stored on computers provided by the employer. The employer must convey a clear intention or the real possibility that there will be the monitoring of online traffic, including electronic mail messages sent to other networks, users on the same network, and all access to pages on the World Wide Web. [758]
- An important provision in the user policy must be a clause that informs employees that their messages would be intercepted by the employer, provided that the sender of the message or information is aware of such interception.[759]
- A provision in the policy that informs employees that access to the Internet and other electronic resources is not an absolute right and depends on the nature of the work that the employer is charged to do will go a long way towards the effort by employers to restrict or discontinue access to electronic source at any time.[760]
- The user policy must prohibit certain practices. These would include but are not limited to the following:

  viewing, storing, downloading or forwarding sexually explicit material (or sexually suggestive) or material that is, racist, harassing, intimidating or defamatory. This provision can extend also to attempts to gain access to restricted resources either inside or outside the computer network of the employer, impersonating another user, damaging or deleting files of another user, obtaining, without authorisation, the access codes and /or passwords of another user. The downloading, installing or using unlicensed software or software that the employee is not authorized to use, install or download may also be prohibited in terms of such a provision.[761]

- The employer in order to provide for an effective a policy must be sure to provide for specific forms of abuse or types of behaviour that may be problematic. This may include providing a list of e- mail practices that are prohibited (sending unauthorized unsolicited

[758] Ibid

[759] Ibid

[760] Ibid

[761] Ibid

mail, commercial advertising of other businesses, mail flooding), or even excessive cross postings on Usenet newsgroups.[762]

- In this policy , an employer can seek to address and regulate the computer conduct of the employee by including:[763]
  a) A blanket prohibition on using any computer resource to promote any business or enterprise except the business or enterprise of the employer
  b) A ban on any attempt to send an electronic message to indicate or gain support for any political party or religious party.
  c) A prohibition on any form of violation of network security, including unauthorized access to, or the use of, data, systems or network, unauthorized interference with network services or equipment.
  d) A restriction on any activity where the employee seeks to gain access to the Internet without running anti- virus software.

- It is not unusual for an employer to include a provision that restricts access to a specific lists of websites due to content that may for instance contain sexually explicit, sexist or defamatory material.[764]

The drafting of a well thought out policy for the use of electronic tools in the workplace will prove to be of immense help to employers especially with regard to issues of privacy and discipline in the work place.

The policy will inform employees of what they may and may not do in relation to their workstation. It is important for the employer to communicate the provisions of this policy to the employee and in certain circumstances where necessary implement provisions through training that focuses on acceptable as well as unacceptable use of electronic tools in the workplace.[765]

[762] Ibid

[763] Ibid

[764] Ibid

[765] Ibid

The policy may be reviewed annually or at shorter intervals to adapt it to the changing needs of the business.[766]

This route of action would not only cut down on the risks relating to e mail, telephone and Internet abuse , but it may also result in a computer system significantly more efficient than ever before.[767]

[766] McGregor op cit note 9 , 192

[767] C Mischke. "Dismissal for abuse of e- mail". (2002) 11 (6). *CLL* 56

CHAPTER 8

Monitoring Devices.

Throughout the years and especially over the last century, improvements in technology have dramatically changed our expectation of privacy in the workplace.

The installation of what has become know as advanced switching technology have made it possible to dial numbers directly anywhere in the country without the assistance of an operator, who might be tempted to listen in.[768] In addition to this, as the cost of telephone lines and equipment steadily dropped, the number of single – user lines increased, and consumers proved increasingly willing to pay for them. Thus, over the course of a generation, we came to expect that a telephone conversation was a private as a face- to face chat in our living room.[769]

To a large degree and without surprise, this expectation of privacy, with regard to phone calls has extended to the workplace. It has become a natural occurrence for any employee to pick up a telephone, and assume that no one is secretly listening in to that conversation.[770] In its 2001 Annual Survey of workplace monitoring and surveillance, the American Management Association estimated that twelve percent of the major North American corporations periodically record and review telephone calls, while eight percent more monitor the amount of time that employees spend on the telephone, and check the phone numbers that have been called.[771]

The exercise of tracing the dialled numbers that an employee calls can be as simple as reading the monthly phone bill. A slightly more aggressive step that may be adopted is the installation of a pen register, which records every number dialled from a particular phone.[772] However due to the fact

[768] F S Lane. *The Naked Employee*. (2003). 106- 108.

[769] Ibid

[770] Ibid

[771] Ibid

[772] Ibid

that use of computers and telephones are closely linked, it is possible to use personal computers and software to track employee phone usage and produce detailed reports of all telephone activity.[773]

According to Telemate.Net, a manufacturer of telephone monitoring software, over twenty percent of all workplace calls are personal.[774] The company has created a software product called Telemate (TM) Call Accounting. This product enables an employer to track all the data generated by the company's telecom resources. The software allows management to identify "the calls and call patterns placed by individuals, teams, departments, and the organisation". [775]

This software is capable of reporting on the following:[776]

- Identify call volume, topics, destinations, sources, length, frequency and peak calling times.
- Track account activity and build a marketing prospect or customer database.
- Classify phone numbers to identify potential productivity distractions.
- Identify inbound callers.

1. Employer Bugs

The use of 'interception devices' such as 'employer bugs' have become increasingly popular with employers.[777] Employers will often use these 'employer bugs' and secret wiretaps to effectively eavesdrop on the conversations of their employees. These 'employer bugs' go unnoticed as they are often hidden in electrical wall plates, smoke detectors, clocks, lamps, radios, frames or even in the ceiling. The result is that the employers may be able to know their employee activities even

[773] Ibid

[774] Ibid 107

[775] Ibid

[776] Ibid

[777] Ibid

when it is not permissible.[778]

2. Magstripe Cards

Currently, the most popular and widely implemented technology for monitoring employee movement is the same familiar magnetic strip (or 'magstripe') found on the back of billions of credit cards in use by people around the world.[779]

This typical magstripe is a thin strip of plastic film containing thousands of small magnetic particles.[780] With the use of a magnetic field, the particles in various sections of a magnetic strip can be oriented to the North or South Pole. Once this information has been recorded on the strip, it can be deciphered by a magstripe reader.[781]

To put this type of monitoring in place, the employer will issue identification cards to their employees. These identification cards contain encoded information on the magstripe, such as an employee's name, Identification number, security access, etc.[782] The employees will thus be required to swipe these identification cards in order to gain access to the company's various facilities.[783]

The magstripe readers are normally wired into a network.[784] In effect, when an employee swipes her card, the information in the strip can be verified by a central database. Most of these systems are specifically designed to record the date, time, and identity of each person who goes through a

[778] Ibid

[779] Ibid 108- 109

[780] Ibid

[781] Ibid

[782] Ibid

[783] Ibid 109 - 110

[784] Ibid

business's checkpoints.[785]

The main concern for employers who use this type of surveillance to monitor access and movement is the phenomenon of 'tailgating'.[786] Tailgating occurs when one employee swipes his card and other employees pass through without swiping theirs. To prevent this, some companies insist that such practice is strictly forbidden. In so doing, companies install an alarm device, which triggers if more than one employee enters a facility with only a single card swipe.[787]

A possible problem area for employers may arise due the consistent swiping of the card which will eventually and inevitably result in the magnetic strip being worn out, which means that the magnetic strip will have to be replaced. This will result in extra expenses for the employer and inconvenience.[788]

3. The Active Badge System

The basic concept of the Active Badge is without many complications. Employees are given a special identification card equipped with an infrared transmitter. This card then sends out a unique code approximately every fifteen seconds.[789] If the card is within six meters of an infrared sensor (mounted on a wall or ceiling), the code is read by the sensor. The sensor is connected to a network of other senses, all of which are linked to a central station. The central station then retrieves data from each of the sensors and uses the information to compile a map of each badge's current location.[790]

---

[785] Ibid

[786] Ibid

[787] Ibid

[788] Ibid

[789] Ibid 111- 113

[790] Ibid

The most obvious benefit of this system is the ability to locate staff more quickly. The aim of this method of surveillance is to improve staff efficiency and enhances quality of service to customers.[791] Employers will utilize this additional information to help them evaluate internal processes, and that such a system reduces ambient noise (since employees can be located quickly without having to be paged).[792]

The Active Badge System is normally designed with the following features: [793]

- WITH- a list of the other badges in the same area as the target badge.
- LOOK- a list of badges currently located in a particular area.
- NOTIFY- an alarm that goes off when a particular badge is picked up by the sensor system.
- HISTORY- a record of the badge's location over a period of time.

4. Cameras

Closed Circuit Television (CCTV) remains the most public and discussed form of surveillance.

In the mid- 1990s, Conservative John Major based his campaign for re- election as British Prime Minister in part on a promise to install more video cameras in public spaces.[794] Major promoted his proposal with a highly successful slogan: "If you've got nothing to hide, you've got nothing to fear". After his appointment as Prime Minister Major kept his promise and began a programme (which was aggressively continued by Tony Blair's government) that has made the British people the most heavily watched and supervised people in the western hemisphere, if not the world.[795] There is an estimate of more than 2.5 million surveillance cameras in Britain, and the average Englishman is photographed by over three hundred different cameras each day.[796] It is also

[791] Ibid
[792] Ibid

[793] Ibid

[794] J E Mcgrath. *Loving Big Brother*. (2004) 19-23 [see also C Norris & G Armstrong. "CCTV and the Social Structuring of Surveillance". In *Surveillance, Crime and Social Control*. Ed. C Norris & D Wilson. (2006) 81-102]

[795] Ibid

[796] Ibid

estimated that in 2002, 5.7 billion cameras were sold in the United States to industries.[797]

Security in corporate entities that are centred around camera systems pose a greater privacy threat to society as a whole but an even greater threat to employees due to the fact that they are more consistently monitored, notwithstanding the fact that employers have both the resources and financial motivation to do so, are more widely implemented, and more frequently hidden.[798]

The main obstacle to the widespread implementation of video surveillance systems has been cost, with the most expensive item being the cameras themselves. This includes the monitors into which the cameras are hardwired, and the personnel required to operate and monitor the cameras.[799] However this obstacle is slowly diminishing. The costs of cameras are falling steadily, and more importantly, the images the cameras produce can now be fed directly into an office network or even onto the Internet.[800] Thus, it is now possible for a single individual to monitor hundreds of people using any computer as a monitor.[801] Images can even be stored on a hard drive for later review, further minimising the need for someone to do real time surveillance.[802]

5. The "PC Monitor"

The Personal Computer Monitor ("PC Monitor") is a small device, approximately two inches long and one and a half inch in diameter, containing a micro- controller and a fixed amount of non-volatile memory.[803] The installation of the PC Monitor is a painless exercise: all that's

---

[797] Ibid

[798] Ibid

[799] Ibid

[800] Ibid

[801] Ibid

[802] Ibid

[803] Lane op cit note 1, 146- 147

required is to unplug the key- board cable from the back of the computer, plug the PC Monitor into the keyboard port, and then plug the keyboard cable into the PC Monitor.[804]

The PC Monitor once installed records every keystroke made on the keyboard port, up to the limits of its memory, which is 8Kb, 32Kb or 64Kb. Since each stroke takes up one byte, the largest PC Monitor can store roughly 64 000 keystrokes.[805]

The PC Monitor is easy to use without the employee's knowledge. Since all of the monitor's electronics and monitoring are self contained, it does not cause any unusual hard drive or Central Processing Unit (CPU) activity, and only a few employees would ever think to check the back of their computer every time they sit down to use it. [806]

6. Computer Monitoring Software

The nature of the office environment over the last decade has dramatically changed and conduct of employees is not monitored by an uncompromising manager or supervisor but by a relentless observer, that is, software that takes monitoring and surveillance to a brand new level.
The following are three examples of such software. There are however, hundreds of similar types of software that are available to an employer:

A. *Investigator*: this software not only records every keystroke made on the computer , it also maintains a record of dialogue boxes and takes periodic screen shots of what is displayed on the computer. The software can be configurated to take secret photographs of the computer user if the computer user is equipped with a Web cam. By recording every keystroke made by the computer user, *Investigator* can effectively record every e- mail

[804] Ibid

[805] Ibid

[806] Ibid

made and sent by a computer user, Internet relay chat, or instant messenger session that takes place on the computer.[807]

B. *The Survey Suite:* this software details the time employees spend using Windows applications, e- mail, and the Internet, and provides the employee with easy to understand reports so that he or she can better manage their time. The focus of *The Survey Suite* is on the amount of time you spend actually interacting with the programs on the computer rather than what you are actually typing. This type of software can be particularly useful for keeping an eye on an employee's computer and then transmit the results of its observations to a central database. *The Survey Suite* gathers the information during the course of the day and then transmits it to the central server whenever a network or Internet connection is opened.[808]

C. *Computer Monitoring Software for Corporate Networks* or what is commonly referred to as *Spector CNE*: this type of software automatically captures and lets the employer review e- mails sent and received, chat conversations and instant messages, files downloaded, web sites visited, applications launched and keystrokes typed. In addition to this, *Spector CNE* creates the equivalent of a digital surveillance tape so that the employer can see the exact sequence of everything the employees are doing on the computer. The software provides e-mail alerts that notify the employer when certain specified words determined by the employer are contained in the e- mail, chat, instant message or web site. *Spector CNE* can be remotely configured and installed from any computer on the network and the recordings can be viewed from any computer on the network, which is ideal for the employer.[809]

7. Emerging monitoring devices

Employers are now beginning to adopt more sophisticated monitoring technologies to help track

[807] Ibid 128

[808] Ibid 129

[809] www.spectorsoft.com. Accessed: 03 October 2007

employee productivity and movement, including Radio Frequency Identification Systems ("RFID") and Global Positioning Systems ("GPS").[810] The uses of RFID and GPS vary widely and can range from simple key-card electronic access employed in many workplaces to more advanced systems that can track an employee's precise location nearly anywhere on the planet. The majority of companies using RFID employ Smartcard technology to control physical security and access to buildings and data centers.[811]

This technology now makes it possible for employees to track the location of most employees who carry modern mobile telephones.[812] CityWachter.com, an American surveillance company, based in the State of Ohio, caused an uproar when it announced that it embedded RFID tags in two of its employees. RFID chips are being used increasingly to track everything from product shipment to pets. Veri-Chip, the company that makes the devices, said the implants were created primarily for medical purposes. According to the company, approximately seventy people have had the implants at the end of 2006.[813] RFID and GPS raise somewhat unique monitoring issues as they are more likely than other technologies to capture off-duty conduct. [814]

Besides the present technological viability for RFID and GPS monitoring, there is current experimentation and development of biometric identification tools (such as facial recognition equipment).[815] Biometric tools in contrast to the RFID and GPS which are widespread are not currently in use. Contrary to representations in movies and television, biometric tools in particular facial recognition technology is unreliable. It is more than likely that in the near future employers

---

[810] V Schachter & S M Swanson "Workplace Privacy and Monitoring: New Developments affecting the Rights of Employers and Employees" (2006) Order No. 8966 Practising *Law Institute* 152-153. *Westlaw* Accessed: 20 February 2007.

[811] Ibid

[812] Ibid 153

[813] Ibid

[814] Ibid

[815] Ibid

may look forward to implementing such an advanced employee recognition and monitoring device.[816]

[816] Ibid 154

CHAPTER 9

Entrapment

Despite the arguments raised by employers that they have legitimate grounds to monitor their employees so as to ensure that they are not exposed to litigation on grounds of vicarious liability (through defamation or sexual harassment), electronic fraud, copyright infringement and costs such as those incurred in the excessive use and time wastage by employees due to employees surfing the Internet or even sending e- mails to colleagues during working hours, this monitoring must not progress further into the dangerous territory where the employer monitors the employee , and at the same time the employee is lured into committing a crime for the specific purpose of securing a conviction against that employee or even to dismiss that employee.

Entrapment is where a person is lured into committing a crime for the specific purpose of securing a conviction against him or her.[817]

The Concise Oxford Dictionary (10 ed) defines the word 'entrap' to mean 'catch in or as in a trap (of a police officer), or to deceive a person into committing a crime in order to secure their prosecution.' *The Oxford Dictionary of Law* (6 ed 2006) defines the noun 'entrapment' to mean 'deliberately trapping a person into committing a crime in order to secure his conviction, as by offering to buy drugs.' From the dictionary definitions alone it is apparent that central to the concept of entrapment or trapping is the premise that a person is lured into committing a crime for the specific purpose of securing a conviction against that person.[818]

In *S v Malinga* 1963 (1) SA 692 (A), at 693 G Holmes JA, defined a trap as "a person who with a view to securing the conviction of another, proposes certain criminal conduct to him, and himself ostensibly takes part therein". In other words, he creates the occasion for someone else to commit the offence.

[817] CR Snyman. *Criminal Law*. 4ed. (2002) 139 see also J Burchell. *Principles of Criminal law*. 3ed. (2005). 348-349

[818] EA Martin and J Law. *Oxford Dictionary of Law*. 6 ed (2006).

An American judge has described entrapment as "the conception and planning of an offence by an officer, and his procurement of its commission by one who would not have perpetrated it except for the trickery, persuasion of that officer".[819]

It is generally considered to be a controversial form of procuring evidence, because there is always the risk that an otherwise innocent person might have been induced to commit the crime on account of the persuasive conduct of, or the methods employed by the trap.[820]

The primary objection to 'entrapment,' expressed by Squires[821], is that it is wrong for the 'trap' to 'cause' individuals to commit crime in order to punish them.[822]

It has been recognized as deeply offensive to ordinary notions of fairness' stated Lord Bingham in *Nottingham City Council* v *Amin* [2000] 1 WLR 1071, at 1076–7 "if a defendant were to be convicted and punished for committing a crime which he only committed because he had been incited, instigated, persuaded, pressurized or wheedled into committing it by a law enforcement officer".

Even though it is regarded as somewhat unfair, if not unethical, to catch someone out by means of a trap and the *modus operandi* involving a trap is considered somewhat devious, many believe that the use of a trap is necessary only as a measure of last resort in order to deal with elusive criminals who cannot otherwise be brought to book.[823]

Not many employers have the confidence to say that their employees will not engage in conduct that will bring the employer into disrepute or behaviour that will cause their employer damages in

[819] Roberts J in *Sorrels v United States* 287 US 435 at 454 (1932)

[820] PJ Schwikkard and SE van der Merwe. *Principles of Evidence.* 2ed. (2002). 246 [In *S v Chesane* 1975 (3) SA 172 (T) McEwan J pointed out, at 173G, that "persons used as traps may have a motive in giving evidence which may outweigh their regard for truth", and that "such motives may include the earning of a monetary reward"].

[821] D Squires "The Problem with Entrapment". (2006) 26 (2). *Oxford Journal of Legal Studies*. 351- 376

[822] Ibid 355

[823] Schwikkard & van der Merwe op cit note 4, 246

some way, either in monetary terms (as is the situation of an employer being found vicariously liable for defamation where the employees distributed untrue remarks about a certain person) or result in the damage of reputation for the employer (where for instance employees who are engaged in the viewing and distribution of pornographic material).[824]

Employers therefore are frequently driven to 'trapping'. The use of a trap involves appointing people, often outside 'agents', whose job it is to try to conclude 'deals' with employees, usually as purported receivers of stolen goods. This practice of appointing traps is not unique to the workplace. The police sometimes try it when conventional detective work fails. The practice is known as 'entrapment'.[825]

The courts have allowed entrapment in many cases for the sake of justice, provided that it takes place with regulation and careful scrutiny by the courts.[826]

With regards to the entrapment and labour law, it was the case of *Cape Town City Council v SA Municipal Workers Union & others* (2000) 21 ILJ2409 (LC) , that first set the parameters for using entrapment in the employment context.

In this case the Cape Town City Council was approached by a firm of investigators concerning alleged cable theft of which the investigators were aware. The investigators were then appointed. Two investigators randomly targeted a group of workers at a substation and asked for a cable to run electricity for a house for underprivileged children. The women were flashily dressed in a short mini- skirt.[827] They approached the employees twice before a transaction eventually took place. Ultimately, 56 metres of cable changed hands at a price of R14 per metre (a total of R630). The detectives apparently later handed over a lesser amount to the council, and kept the balance for themselves.[828] The transaction was then video taped. The two employees were subsequently

[824] Ibid 246

[825] J Grogan "To Catch a Thief". (2001) 17 (1) *EL* 8

[826] A Dekker "Traps in the context of Labour Law". (2003) 11 (3) *JBL* 151

[827] *Cape Town City Council v SA Municipal Workers Union & others* (2000) 21 ILJ2409 (LC), at 2419 A

[828] supra note 11, at 2435H

dismissed.

The question for decision by the Court was whether the dismissal of the two workers was fair. The two employees had sold property belonging to their employer for their own profit. The fact that they were 'tempted' to do so was irrelevant. An employer cannot be expected to retain employees who so easily succumb to such temptation.[829] However, as Stelzner AJ pointed out, the issue is not as simple as that. There is something inherently repugnant about the idea of tricking any person, including an employee, into performing a criminal act. The Court summarised the reason why the law has traditionally treated the practice with suspicion thus:

> *"Although courts and commentators around the world appear to differ ... [about] the issue in principle ... the nub of the concern which emerges ... is that persons who, in the absence of intervention by the traps, might never have committed or considered committing a crime are caused by the conduct of the traps to enter into criminal activity".* [830]

Moreover,

> *"The conduct of the trap/s is inevitably, in the absence of legislative intervention, in itself unlawful (as the inciter is the accomplice of the crime committed) and that very conduct secures the conviction of the person 'trapped'".* [831]

The law gives expression to these reservations in two ways. The first is to disregard evidence obtained by trapping when deciding whether the accused committed the offence. Without such evidence, the prosecution may be left with nothing else.[832] The other protection against trapping is to treat it as an absolute defence to a criminal charge. If the accused can prove that he or she did nothing more than co-operate with trappers, there can be no conviction.[833]

---

[829] Grogan op cit note 9, 8

[830] supra note 11 , at 2426 H-J

[831] supra note 11, at 2427A

[832] supra note 11, at 2427A

[833] Grogan op cit note 9, 9

The court held that evidence obtained by means of entrapment would be admissible if the conduct of the trap did not go beyond providing an opportunity to commit an offence. This will be established by means of a two-stage enquiry. The first question is whether the trap's conduct went beyond the mere providing of an opportunity to commit an offence. If it did, the evidence may still be admitted provided that public and private interests are weighed up against each other.[834]

The fist stage of the enquiry as set out in the judgment at 2433, read with 2430–2431, quoting s 252A (2) of the Criminal Procedure Act 51 of 1977):

- the nature of the offence;
- the availability of other techniques of investigation to obtain proof
- whether an average person in the same position would be induced to commit the offence;
- the degree of persistence and the number of attempts;
- the type of inducement;
- the timing of the conduct;
- whether the conduct involved an exploitation of human characteristics such as emotions or friendship or personal or professional circumstances;
- whether a particular vulnerability was exploited;
- the proportionality between the involvement of the official compared with that of the accused;
- whether before the trap was set there was reasonable suspicion that the accused had committed an offence; and
- whether the official acted in good or bad faith

The second stage of the enquiry is set in the judgement at 2433, read with 2431–2432, quoting s 252A (3) of the Criminal Procedure Act).

In weighing up the public and private interests, the court should look at other questions:

- the nature and seriousness of the offence;
- whether it would be difficult to uncover the crime without a trap;
- whether the crime is so frequently committed that special measures are required to detect it;
- the extent of the effect of the trap;
- the nature and seriousness of any infringement of any fundamental right; and
- whether the setting of a trap and means used were proportional to the seriousness of the offence

[834] Dekker op cit note 10, 151

The court found that, all the facts considered, the two traps had provided the two employees with more than an opportunity to commit an offence. This conclusion was suggested by several factors:
• the two employees involved were not suspected of stealing; in fact, and on its own initiative the investigation agency approached the Council with information suggesting that employees were involved in theft;[835]
• the female investigator was flashily dressed;
• the investigators tried to elicit sympathy by saying that they needed the cable for underprivileged children;
• the investigators made several attempts before the employees succumbed to their request;[836] and
• the two investigators were guilty of an offence and enriched themselves in the process by claiming more money from the Council than the amount actually received from the two employees.[837]

The court in this case did not allow the evidence. But the court did indicate that law enforcement would be impeded if the evidence obtained from a trapping situation were never to be allowed. The court stated that careful scrutiny by the courts is necessary to ensure fairness.[838]

Although the Court did not consider it necessary to make a definite finding in principle on whether trapping in the workplace should be allowed, Stelzner AJ left no doubt about her views:

> *"I might state, by way of an aside, that I would be reluctant if not unlikely to hold that a system of trapping (obviously properly constrained) may never be fair in the employment context. I say this because throughout the various jurisdictions to which I have referred already in this judgment it is noteworthy that, despite a sense of concern and disquiet about the unfettered use of entrapment, no jurisdiction has been prepared to hold (albeit in the criminal context) that entrapment should never be permissible. It seems to me that, provided the courts are satisfied that the use of entrapment is properly scrutinised and the admissibility of evidence obtained as a result thereof carefully regulated, then courts tend*

[835] supra note 11, at 2435 E-G

[836] supra note 11, at 2435 H-J

[837] supra note 11, at 2436 A-B

[838] supra note 11, at 2434 F

to recognise that there are circumstances in which law enforcement (and the pursuit of justice generally) would be impeded if the evidence obtained from a trapping situation were excluded. I see no reason why that reasoning should not be equally applicable in the employment context, provided of course that proper constraints are applied".[839]

In the case of *Caji and African Personnel Services (Pty) Ltd* (2005) 26 *ILJ* 150 (CCMA) the court again relied on Section 252A of Criminal Procedure Act 51 of 1977 to be invoked as guideline to judge admissibility.

The applicant was employed by the respondent labour broker to provide services to its client, Path Plastics. A private investigator who was conducting an investigation at the premises of a business opposite that of Path Plastics observed several plastic containers on those premises and upon enquiring where they came from had the applicant pointed out to him. The investigator then approached the applicant and another employee, who went with the investigator to the Path Plastics premises, where the applicant climbed over the fence and brought out five plastic buckets and a pool filter, which were then loaded onto the investigator's bakkie in exchange for money. The respondent was later called to the offices of Path Plastics and shown a video of the transaction. The video tape was sold to the respondent by the investigator's employer for R5 000. After a disciplinary enquiry both the employees were dismissed.[840]

It was argued on behalf of the applicant that the evidence obtained by the private investigator should not be admissible on the basis that he induced the applicant to take part in a criminal act, in which he himself partook.[841]

It was argued on behalf of the respondent that the applicant was merely presented with an opportunity to be dishonest, as most people are presented with, on a daily basis during the ordinary

[839] supra note 11, at 2434 E-H

[840] *Caji and African Personnel Services (Pty) Ltd* (2005) 26 *ILJ* 150 (CCMA) , at 151 A-B

[841] supra note 24, at 154 E-F

course of life.[842]

The court in its judgment referred to the case of Cape *Town City Council v SAMWU & others* (2000) 21 ILJ 2409 (LC); [2001] 11 BLLR 1239 (LC).[843]

The commissioner then considered the evidence of both parties having regard to s 252A and found several contradictions between the evidence of the investigator and that of the applicant. According to the court neither evidence was above scrutiny.[844] While the investigator testified that the applicant had contacted him on several occasions to finalize the deal, the applicant averred that the investigator had induced and coerced him to undertake the theft.[845] Where the two witnesses contradicted each other the onus was on the respondent to prove the facts. The commissioner held that the investigator had sold the tape to the respondent, and so had a vested interest in the outcome of the matter. In the circumstances the onus was on the respondent to show that the applicant had not been induced or forced to take part, and in the absence of such evidence, the evidence of the investigator, according to the commissioner, should not be allowed to stand. In the absence of that evidence the dismissal was substantively unfair.[846] The commissioner awarded the applicant compensation.

Dekker[847] believes that each entrapment case must be examined on its own merits to determine

---

[842] supra note 24, at 154 G

[843] supra note 24 at 154 I-J [In her judgment Stelzner H AJ extensively analysed South African and foreign jurisprudence and academic writings on the topic. While the point was not decided, she noted at para 60: "I might state ... that I would be reluctant if not unlikely to hold that a system of trapping (obviously properly constrained) may never be fair in the employment context". She then goes on to state that entrapment cannot be allowed to take place without regulation or careful scrutiny of courts and that the provisions of s 252A of the Criminal Procedure Act 51 of 1977 (the CPA) may be invoked as a guideline in the employment context, together with any other additional considerations required by fairness in the discretion of the court].

[844] supra note 24, at 158 & 159

[845] supra note 24, at 158 & 159

[846] supra note 24 , at 160

[847] A Dekker "Vice or devices: employee monitoring in the workplace". (2004) 16 (4) *SA Merc LJ* 628

whether the evidence obtained should be allowed. The following cases illustrate this point.

In the case of *Lawrence v I Kuper & Co* (1994) 15 ILJ 1140 (IC); the applicant, (49 years old), was employed by the respondent as a building inspector. His most important duties were to visit buildings owned or managed by the respondent and to submit written inspection reports to his immediate superior. For this purpose he was given the use of a company car. In terms of his employment contract dated 14 January 1991, he undertook, *inter alia*, to devote his time and attention to the respondent's business.[848] It was common cause that the applicant performed his duties in a reasonably competent manner.[849]

The applicant was suspected however of running a private business during office hours and using the company car for that purpose. At a meeting set up by a private investigator , the employee sold a car battery to the investigator , and also issued him with a letter of thanks from ' B& B Enterprises' and five more business cards as advertisement for future business . The agent videotaped the meeting.[850]

The arbitrator in this case held that an employer may sometimes be faced with a situation in the workplace where it becomes necessary for him to employ the services of a private investigator in order to obtain concrete evidence against an employee who is suspected of being involved in some improper conduct such as accepting bribes, or passing on trade secrets to competitors, or of dealing in dagga or other harmful drugs with fellow-employees. The arbitrator held that in such circumstances he could not see why an employee could not be under surveillance. The evidence thus so obtained may then according to the arbitrator be used to give a warning, or a disciplinary enquiry. The arbitrator held further that the seriousness of the offence or contravention, the interests of the company, and the work record of the employee should determine *inter alia* whether he or she should be summarily dismissed or be given a lesser penalty. [851]

[848] *Lawrence v I Kuper & Co* (1994) 15 ILJ 1140 (IC), at 1141 F-H

[849] supra note 32, at 1141 F-H

[850] supra note 32, at 1142 D

[851] supra note 32 , at 1142 G

The nature of the applicant's daily duties in the present case were such that he was for most of the time left free to do his own thing. He travelled alone from place to place by car and the respondent had no effective means of controlling or supervising his movements. In these circumstances it was neither improper nor unfair for the respondent to have arranged for his entrapment. [852]

In the case of *SA Transport & Allied Workers Union on behalf of Assegai v Autopax* (2002) 2 BALR 171 (AMSSA); the applicant employee was employed as a coach driver by the respondent. He was dismissed after a disciplinary enquiry where he was found guilty of gross negligence in that he failed to exercise control over a ticket book and of two counts of gross misconduct in that he issued a stolen and/or missing ticket to a passenger and failed to pay in the money handed to him for that ticket. On a further count he was found not guilty.

In arbitration proceedings the arbitrator was required to consider the admissibility of a video recording made without the employee's knowledge by a private investigator who recorded the transaction with the false ticket. The union argued that the video footage was an invasion of the employee's privacy and that it was unconstitutional and should not be allowed. The arbitrator had reference to the constitutional right to privacy, which included the right not to have the privacy of one's communications infringed.[853]

The arbitrator allowed the videotape as evidence. He found that the conduct of the bus driver while driving a bus would not constitute confidential information. The arbitrator stated that a conversation in the course of employment between a bus driver and passenger was also not confidential, and therefore the act of taping the conversation was not an infringement of privacy.[854]

In the case of *SATAWU on behalf of Radebe v Metrorail Wits* (2001) 22 ILJ 2372 (ARB); the grievant, who had been employed by the company since 1974, was charged with misconduct

---

[852] supra note 32, at 1146 F-J

[853] *SA Transport & Allied Workers Union on behalf of Assegai v Autopax* (2002) 2 BALR 171 (AMSSA), at 171

[854] supra note 37, at 171G

relating to dishonesty, theft and insubordination. It appeared that, while working as an access controller at Boksburg East Station, he had accepted marked money from two undercover protection officers who were conducting an 'honesty test' exercise.[855]

The court held that where entrapment was used, an employee should be liable to a certain extent but the circumstances of the entrapment can be used as a mitigation since the entrapment itself diminished the moral blameworthiness of the offender.[856]

The agent's evidence was allowed. The arbitrator found that an employer is allowed to embark on honesty exercises to rid itself of dishonest behaviour. The arbitrator held however that these exercises must be balanced against fairness, and should not be improper or criminal. In this case the arbitrator held that the exercise of honesty checks were not improper in view of the fact that the employer experienced ongoing financial losses, and because the employees were informed beforehand that honesty tests were to be conducted.[857]

In the case of FAWU *obo Karolus and Two a Day Ltd* (WE 8383-02) 24 April 2003; the employer experienced problems with petrol theft. After more regular stock takes could not solve the problem, the employer installed a video camera to monitor the petrol pumps. The video camera recorded the employee filling a tank with petrol without authorisation. The video evidence was allowed by the arbitrator. The arbitrator found that the camera was not set up to entrap the applicant but merely to monitor use of the pump. The recording was made while the employee was on duty. At the time the employer had a direct interest in the actions of the employee, and so therefore could not have been an invasion of privacy.

In *SACCAWU obo Libi and Weirs Cash & Carry* (EC 2163 – 01), 3 April 2002; two investigators posed as installers of closed circuit television cameras. They approached two employees who were selected at random. The investigators asked one of the employees for headache tablets and the other for a tin of custard. Both the employees handed over the goods. One of them handed over the

[855] *SATAWU on behalf of Radebe v Metrorail Wits* (2001) 22 ILJ 2372 (ARB); at 2372 C-D

[856] supra note 39, at 2377 I- [It was however Smalberger JA who ventured that the offender must be held liable to an extent but that the circumstances of his entrapment be used as mitigation since the entrapment itself diminished the moral blameworthiness of the offender (*S v Petkar* 1988 (3) SA 571 (A))].

goods with the knowledge that he was being filmed. The court refused to allow the videotape as evidence. The court held that the trapping in this case was a fishing expedition. The court held further that there was no suspicion of these employees. The court held that applicants were not entirely innocent, but the detectives' conduct towards them did not comply with the spirit, purpose, and objects of the Constitution, and so the tapes could not be allowed.[858]

The case of *SACCAWU on behalf of Jacobs and Portswood Hotel* (WE 39639) 29 June 2001; involved the situation where the Portswood Hotel had a policy that guests were not allowed to entertain prostitutes in their rooms. This was a policy that was to be strictly enforced by the desk clerks of the Hotel. The Hotel did spot checks on their desk clerks by means of a 'mystery guest'. One such 'mystery guest' requested a prostitute. The desk clerk assisted him by making all the necessary arrangements with the agency. The desk clerk was then dismissed. The arbitrator allowed the evidence supplied by the trap ('mystery guest'), as the agent merely supplied an opportunity to the clerk to commit an offence. The clerk could not prove that the conduct of the agent went beyond that.

In the case of *Metrorail and SA Transport & Allied Workers Union on behalf of Magagula* (2002) 23 ILJ 1641 (BCA); the employee, a ticket officer at one of Metrorail's stations, took money from two passengers without issuing them tickets. The passengers were in fact employees of Metrorail who were conducting an 'honesty test'. They reported the employee to security officers. When they confronted him, the employee dropped the money, abandoned his ticket machine and fled. He returned to work the following day. At a disciplinary hearing the employee was found guilty of misconduct, specifically theft, dishonesty, disregarding a lawful instruction, gross negligence and absence without permission. He was dismissed. In arbitration proceedings, the employee denied that he had acted dishonestly and contended that he had been unlawfully trapped by Metrorail's security personnel.[859]

---

[857] supra note 39, at 2379 A-C

[858] *SACCAWU obo Libi and Weirs Cash & Carry* (EC 2163 – 01), 3 April 2002, at 13

[859] *Metrorail and SA Transport & Allied Workers Union on behalf of Magagula* (2002) 23 ILJ 1641 (BCA), at 1641 D-F

The arbitrator considered and approved the comprehensive note by John Grogan[860] Sibergramme 10/2000 on the issue of trapping and the requirements for its use in the employment environment. She was satisfied that in this case the trap in which the employee had been caught was a fair one. The security officers had no reason to suspect that the employee was involved in skullduggery at the time the trap was set and they did not target him specifically, although they did suspect that ticket officers were defrauding Metrorail by taking money without issuing tickets. They did not do anything more than provide the employee with the opportunity to commit the offence; they did not seek to persuade him to do so. In addition, the trap was justified by Metrorail's operational requirements.[861]

In the case of *Mbuli/ Spartan Wiremakers CC* (2004) 5 BALR 598 (MEIBC); the respondent employer was experiencing severe shrinkage of their product and had been informed that the applicant and another employee were involved in stealing and selling the product. The employer arranged for another of its employees, a buyer (who was acting as a trap) to approach the applicant and seek to buy rolls of netting wire from him cheaply. The applicant agreed to sell the wire at less than half its true price, and this transaction was observed and recorded. After a disciplinary enquiry the applicant was dismissed.

The court had to consider whether evidence of the trap was admissible. The admissibility of such evidence in criminal courts is regulated by section 252 A of the Criminal Procedure Act 51 of 1977. The court held this provision may serve as a guideline in the employment context.[862]

The court held that subsection 3 of s 252 A of the CPA 51 of 1977 allows further, for a discretion in regard to the admission of evidence even where it is found that the conduct goes beyond providing

---

44 Where Grogan made the following statement**:** ["As employers struggle to contain ever rising levels of shrinkage, many are resorting to employing 'undercover agents' to tempt workers to expose dishonest inclinations. These 'agents' pose as receivers of stolen goods, and arrange illicit transactions. When the employees succumb to temptation, they are caught red handed and dismissed.

Courts throughout the world have recognised that entrapment is morally dubious, but effective: effective because it secures the arrest and conviction of criminals who might otherwise not be caught; dubious because it can result in the conviction of those who might never have gone wrong had they not been tempted."] (discussed in *Metrorail and SA Transport & Allied Workers Union on behalf of Magagula* (2002) 23 ILJ 1641 (BCA), a t 1647 I)

[861] supra note 43, at 1647 G-H & I-J

[862] *Mbuli/ Spartan Wiremakers CC* (2004) 5 BALR 598 (MEIBC); at 603 H-I and 604 A-D

an opportunity to commit an offence but through a process of weighing up the public interest against the personal interest of the accused with reference, again, to a list of stated factors. The court held that it accepted the evidence obtained by means of a trap in this case. In the present case the applicant had been a willing participant and had not been unduly induced, coerced or tricked into committing the theft and furthermore the fact that staff theft was prevalent.[863]

In the case of *Numsa obo/ Abrahams / Guestro Wheels* (2004) 4 BALR 520 (CCMA); the applicant a dispatch clerk, was dismissed for making out false invoices for the sale of wheel rims to an 'undercover agent', and receiving money from the agent in return. The applicant denied that he had been involved in any corruption. The agent gave evidence at his disciplinary hearing, but refused to testify during the arbitration proceeding. The applicant contended that a written statement by the agent was inadmissible, and that the videotape made by the agent should be disregarded because it was made during an entrapment exercise.[864]

The court had to consider the submission of the applicant that the evidence should not be admitted because it was made during an entrapment process. The court referred to *Lawrence v I Kuper & Company (Pty) Ltd t/a Kupers a member of Investec* 1994 15 ILJ 1140 (IC) ; at 1146 D-H :

> *"In the popular view it is regarded as somewhat unfair, if not unethical, to catch out someone by means of a trap and the modus operandi involving a trap is generally looked upon with disapprobation. Many others believe that it should be used only as a measure of last resort in order to deal with elusive criminals who cannot otherwise be brought to book".*
>
> *"Leaving aside traps used in criminal cases, it would appear that an employer may sometimes be faced with a situation in the workplace when it becomes necessary for him to employ the services of a private investigator in order to obtain concrete evidence against an employee who is suspected of being involved in some improper conduct such as accepting bribes, or passing on trade secrets to competitors, or of dealing in dagga or other harmful drugs with fellow-employees. I cannot see any reason why an employee may*

[863] supra note 46, at 604 D-E and 605 A-C

[864] *Numsa obo/ Abrahams / Guestro Wheels* (2004) 4 BALR 520 (CCMA) , at 520 E-F

not be placed under surveillance in such circumstances. The information or evidence so obtained should then be used to confront the employee and should form the basis for giving him a warning or even a final written warning. Should the employer however decide to hold a disciplinary inquiry, then the cogency of the investigator's evidence, the seriousness of the offence or contravention, the interests of the company, and the work record of the employee should determine inter alia whether he or she should be summarily dismissed or be given a lesser penalty".

The court went on to hold that the evidence did not infringe upon the employee's right to privacy. The court held that the rights of the parties must be weighed, which entails the balancing of the employee's right to privacy against the employer's right to protect his property and economic interest.[865] In this case confidential information concerning the employee was recorded. He was not discussing his own personal affairs. According to him, he was acting as an employee promoting his employer's business, that is, it was part and parcel of his normal functions. Therefore no privacy was infringed or for that matter any right to privacy which could be weighed up against the employer's right to protect its property.[866]

The circumstances of every entrapment case must be examined on their own merits in order to determine whether the evidence so obtained should be allowed.

The judgements set out above provide important and valuable lessons. The use of trapping is not necessarily considered to be unfair. Trapping is permissible when its object is to identify a wrongdoer and not make one.[867] When employers do resort to the use of traps they must ensure that the conduct of the trap consists only of providing an employee with an opportunity to commit an offence, failure to do so will result in the evidence obtained being rendered inadmissible by the court.[868] A successful trap should not be the only evidence against the employee. The evidence obtained from the trap should be supported by other evidence, this should be the case even if the

[865] supra note 48, at 534 I- J and 524 A-B

[866] supra note 48, at 534 I- J and 524 A-B

[867] Grogan op cit note 9, 10

[868] Ibid

supporting evidence is only circumstantial.[869] This may be achieved by producing other evidence linking employees concerned to dishonest practices other than dealings with the trapper.[870]

There are certain cautionary steps and parameters that emerge for the use of entrapment in order to prove wrongdoing on the part of the employer, these are:[871]

- a legitimate commercial need
- high level consent/mandate from the organisation/employer
- must be some reasonable suspicion of wrongdoing
- management must be informed of the *modus operandi* or manner of interception/trap
- management must monitor and be kept informed of the exercise.

It must be kept in mind that employers do not have the unlimited or absolute right to intrude on the personal lives of their employees or to test the virtues of individuals on a random basis, the reason being is that entrapment techniques result in the commission of crimes by people who would not otherwise engage in criminal conduct. Therefore employers must tread carefully so as not to engage in criminal conduct for the sole purpose of entrapping others.[872]

[869] Ibid

[870] Ibid

[871] M, Beumont, "Entrapment of employees – Is all evidence admissible". (2004) 4 (6) *Fair Employment Practice* 73

[872] K Hofmeyr. "The problem of Private Entrapment". (2006) *The Criminal Law Review*. 331.

CHAPTER 10

The Protected Disclosures Act 26 of 2000 as it applies to Electronic Communication in the Workplace

When the employer monitors the activities of their employees the information obtained by the employer will potentially serve as legitimate grounds to dismiss, warn and discipline employees. As discussed earlier (in chapter 9) this information that is obtained by the employer is normally information that is communicated between employees, through the telephone, Internet and e- mail.

However, there will be instances and specific occasions where the monitoring of employees' activities, will result in the employer becoming aware of information that employees have exchanged with other individuals, and no disciplinary action will be permitted because the communicated information is said to be protected. In other words, the employer will not have grounds to dismiss or discipline the employee based on the exchange of this information.[873]

In terms of the Protected Disclosures Act 26 of 2000 (PDA), employees are protected against dismissal or any prejudicial conduct if they disclose information to certain persons concerning the commission of criminal offences, miscarriages of justice, unfair discrimination and conduct detrimental to health and safety or the environment.[874]

The preamble to the PDA affirms that criminal and other irregular conduct in organs of state and private bodies are detrimental to good, effective, accountable and transparent governance in organs of state and open and good corporate governance in private bodies and can endanger the economic stability of the Republic and have the potential to cause social damage.[875]

---

[873] J Grogan. *Workplace Law*. 8ed. (2005) 143

[874] Ibid

[875] Protected Disclosure Act 26 of 2000 [In terms of section1 of the PDA, disclosure means any disclosure of information regarding any conduct of an *employer* , or an *employee* of that *employer* , made by any *employee* who has reason to believe that the information concerned shows or tends to show one or more of the following:

(a) that a criminal offence has been committed, is being committed or is likely to be committed;

(b) that a person has failed, is failing or is likely to fail to comply with any legal obligation to which that person is subject;

Parliament seeks to combat crime and corruption in the workplace by encouraging 'whistle blowing' by employees regarding an impropriety, i.e. 'unlawful and irregular conduct' by employers and fellow employees. The commitment by Parliament is further highlighted due to the fact that employees who take such action are to be protected from victimization by their employers.[876] The intention is to create a culture which will facilitate and promote the disclosure of information by employees that relates to criminal and other irregular conduct in the workplace in a responsible manner. This is achieved by the formulation of comprehensive statutory guidelines for the disclosure of such information and subsequent protection against any reprisals or backlash as a result of such disclosure.[877]

The dismissal of employees for disclosing such information is automatically unfair, provided that the disclosure was made in good faith and, if the information is incorrect, the employee had reason to believe that it was true.[878]

To be protected a disclosure must be made to: a legal adviser in accordance with s 5; an employer in accordance with s 6; a member of cabinet or of the executive council of a province in accordance with s 7; a person or body in accordance with s 8; or any other person or body in accordance with s 9 of the Act.

In addition to dismissal an employee may be subjected to suspension, demotion, harassment, intimidation, being transferred against his or her will or being subjected to early retirement.[879]

(c) that a miscarriage of justice has occurred, is occurring or is likely to occur;
(d) that the health or safety of an individual has been, is being or is likely to be endangered;
(e) that the environment has been, is being or is likely to be damaged;
(f) unfair discrimination as contemplated in the Promotion of Equality and Prevention of Unfair Discrimination Act , 2000 (); or Act 4 of 2000]
(g) that any matter referred to in paragraphs *(a)* to *(f)* has been, is being or is likely to be deliberately concealed;

[876] A Landman "A Charter for Whislte Blowers: A note on the Protected Disclosure Act". (2001) 22 *ILJ* 37

[877] Ibid

[878] Ibid 37, [see s 187 1(h) of the Labour Relations Act 66 of 1995].

[879] Ibid 42

Any employee who has been subjected to the above, that is, an occupational detriment in breach of s 3, may approach any court having jurisdiction, including the Labour Court established by s 151 of the Labour Relations Act 66 of 1995, for appropriate relief.[880]

For the purposes of the LRA, including the consideration of any matter emanating from this Act by the Labour Court, any dismissal in breach of s 3 is deemed to be an automatically unfair dismissal as contemplated in s 187 of that Act, and the dispute about such a dismissal must follow the procedure set out in chapter VIII of the LRA; and any other occupational detriment in breach of s 3 is deemed to be an unfair labour practice as contemplated in part B of schedule 7 to the LRA. A dismissal of a 'whistle blower' constitutes an automatically unfair dismissal. The Labour Court is entitled to order the reinstatement of the whistle blower or to order compensation not exceeding an amount equal to twenty four months times the monthly remuneration payable to the employee at the date of dismissal.[881]

The following cases illustrate the application of the PDA

In the case of *Grieve v Denel* (2003) 24 ILJ 551 (LC), the applicant was preparing a report for the company's board concerning certain allegations of wrongdoing by the general manager of one of

[880] Section 1 of the PDA 2000 defines 'occupational detriment' in relation to the working environment of an *employee* , as :

a) being subjected to any disciplinary action;
b) being dismissed, suspended, demoted, harassed or intimidated;
c) being transferred against his or her will;
d) being refused transfer or promotion;
e) being subjected to a term or condition of employment or retirement which is altered or kept altered to his or her disadvantage;
f) being refused a reference, or being provided with an adverse reference, from his or her *employer* ;
g) being denied appointment to any employment, profession or office;
h) being threatened with any of the actions referred to paragraphs *(a)* to *(g)* above; or
i) being otherwise adversely affected in respect of his or her employment, profession or office, including employment opportunities and work security

9 Landman op cit note 4, 43

[10] *Grieve v Denel* (2003) 24 ILJ 551 (LC) at 554 B-E & F-H.

[11] supra note 10, at 562 E-D

its divisions when he was charged with misconduct.[882] The applicant was not charged expressly with making disclosures, but had been charged in relation to those disclosures with misconduct arising form the manner in which he obtained the information which led to the disclosures. The applicant was also charged with accessing pornographic sites on the internet and using e-mail to send pornographic, sexist or other unsavoury messages and/or images. [883]

The applicant was accordingly suspended from his duty, and summoned to attend a disciplinary inquiry. Grieve referred a dispute to the CCMA, claiming he was the victim of unfair labour practice. He then launched an urgent application for an order restraining Denel from instituting disciplinary action against him pending the outcome of the enquiry.[884]

The court held that the disclosures which Grieve intended to make appeared to be bona fide and that, if true, those disclosures revealed possible criminal conduct.[885]

According to the court *prima facie*, the disclosures accordingly fell within the terms of the PDA. Furthermore, it was questionable why Denel chose to press other unrelated charges (including examining pornography on a company computer) at the same time. The court also held that an 'occupational detriment', against which employees are protected under the PDA, is wide enough to include being subjected to a disciplinary inquiry.[886]

The employer was accordingly interdicted from proceeding with any disciplinary action or enquiry against the employee regarding any of the allegations contained in the notice to attend a disciplinary enquiry addressed to him pending the determination of an unfair labour practice dispute between the parties.[887]

---

[884] supra note 10, at 554 H- I

[885] supra note 10, at 560 B-D

[886] supra note 10, at 563 C-D

[887] supra note 10, at 564 A-D

In the case of CWU *& another v Mobile Telephone Networks* (2003) 24 ILJ 1670 (LC), the applicant employee had accused his superiors of giving preferential treatment to a particular labour broker from whom it had hired workers.[888] The allegation was made twice via e- mail to MTN's business risk unit, as well as to a number of senior employees.[889] The employee subsequently went one better; he accused MTN's management of corruption. He immediately was suspended and summoned to attend a disciplinary hearing.[890] Like Grieve, the employee in Mobile Telephone Networks obtained a temporary interdict restraining the company from instituting disciplinary action. On the return date, the court accepted that an occupational detriment, for the purposes of the PDA, includes being dismissed, demoted, harassed or intimidated.[891]

The commissioner held that the PDA is designed to encourage a 'culture of whistle blowing', however protection granted by the Act is not absolute; it is not designed to protect disclosures based on mere rumours and conjecture.[892] The court held that the employee's allegations did not convey information; they were merely expressions of opinion. There was no factual basis, however tenuous, in any of his communications to justify the conclusion that MTN's management had acted improperly. Furthermore, the commissioner held that the disclosure had been made publicly, whereas the PDA protects only private disclosures.[893] Finally, the employee had not attempted to make use of MTN's elaborate procedures which includes a confidential hot line for reporting alleged wrongdoing. The application was dismissed with costs.[894]

In the case of *H and M Ltd* (2005) 26 ILJ 1737 (CCMA), the employee was dismissed after making highly critical complaints to a shareholder of the company, resident in Spain, in which she listed forty two complaints concerning the management of the South African branch of the company.

---

[888] *CWU & another v Mobile Telephone Networks* (2003) 24 ILJ 1670 (LC), at 1673 E-F

[889] supra note 16, at 1673 G-J & 1674 A-C

[890] supra note 16, at 1674 D-J

[891] Grogan op cit note 1, 154

[892] supra note 16, at 1678 E-J

[893] supra note 16, at 1678 E-J

[894] supra note 16, at 1678 E-J

The employee claimed that the disclosure was protected in terms of the Protected Disclosures Act 26 of 2000, and thus she was entitled to protection against dismissal.

The commissioner in relation to employee protection in terms of the PDA mentioned the following:[895]

- The person claiming protection in terms of the Act should be an employee.
- The disclosure must contain information that the employee has reason to believe that is authorised in the PDA.
- The employee must have some factual basis for his or her disclosure.
- The disclosure must be made in good faith.
- The *bona fides* of the employee in making the disclosure are important to determine the factual accuracy of the conduct complained of.

The commissioner determined that only three of the forty two contentious complaints qualified as protected disclosures for the purposes of the Act, but nevertheless awarded compensation for the dismissal, which he found to have been substantively unfair.[896]

In the case of *Tshishonga v Minister of Justice & Constitutional Development & another* (2007) 28 ILJ 195 (LC), the applicant found no-one in government willing to investigate his complaints. Frustrated by the lack of progress the applicant issued a press statement to the media in which he set out information about the alleged irregularities. He was suspended pending a disciplinary enquiry. The employee's disclosures had been made in a press statement in which he set out information about alleged improprieties which had taken place within the Department of Justice, in which he was employed.

This case dealt with the first claim before the Labour Court for compensation under the Protected Disclosures Act 26 of 2000. The court made a comprehensive survey of the philosophy and purpose underlying the provisions of the PDA, and of similar legislation passed internationally, in

---

[895] *H and M Ltd* (2005) 26 ILJ 1737 (CCMA), at 1738 A-E

[896] supra note 23, at 1792 E-F

order to protect employees who disclosed improprieties by their employers or other employees. The court made a detailed analysis of the relevant sections of the PDA in order to determine what would constitute a disclosure for the purposes of the PDA, and what requirements must be met in order for such a disclosure. The court noted that the PDA contains a four-stage process that begins with an analysis of the information to determine whether it is a disclosure.[897] If it is, then the next question is whether it is protected.[898] The third stage is to determine whether the employee was subjected to any occupational detriment[899] and the last stage is to determine what remedy should be awarded for such treatment.[900]

The court determined that only three of the forty two contentious complaints qualified as protected disclosures for the purposes of the Act, but nevertheless awarded compensation for the dismissal, which he found to have been substantively unfair to be protected.[901] The court found that having regard to all the circumstances of the case the applicant employee had acted reasonably in making his complaint to the media, and that he had met all the requirements prescribed in s 9 of the PDA. The disclosure was therefore protected.[902]

The applicant was, as a result of the disclosures, held to have suffered an occupational detriment and was awarded the maximum prescribed compensation, that is, twelve month's remuneration.[903]

The protection of the PDA is not unconditional. The PDA does set certain limits of what constitutes a protected disclosure, as well as the manner of permissible disclosure by workers.

---

[897] *Tshishonga v Minister of Justice & Constitutional Development & another* (2007) 28 ILJ 195 (LC), at 227 F-H & 228 A-B

[898] supra note 25, at 231-236

[899] supra note 25, at 239H & 240 A

[900] supra note 25, at 245-249

[901] supra note 25, at 245-249

[902] supra note 25, at 245-249

[903] supra note 25 , at 285C

The protection extended to employees by the PDA is not unconditional. The definition of 'disclosure' clearly envisages that it is only the disclosure of information that either discloses or tends to disclose forms of criminal or other misconduct that is the subject of protection under the PDA. The disclosure must also be made in good faith. An employee who has a deliberate intention to embarrass, harass or tarnish the reputation of the employer is not likely to satisfy the requirement of good faith. The purpose of the PDA would be undermined if genuine concerns or suspicions were not protected in an employment context even if they later proved to be unfounded.[904]

The PDA records that it is incumbent on every employer and employee to disclose criminal or irregular conduct in the workplace, and that employees should be protected against reprisals as a result of such disclosures. Good, effective and transparent governance by employers is obviously in the broader social interest and employees should be encouraged, without fear of reprisal, to disclose information relating to suspected criminal and other irregular conduct by their employers.[905]

[904] Landman op cit , note 4

[905] Ibid

CONCLUSION

The use of electronic communication tools especially the use of the Internet and e- mail facilities has become a necessity for any employer, and the likelihood that the use of these 'tools' will decrease due the potential risks posed to the employer, such as vicarious liability for defamation, sexual harassment, copyright infringement (all of which may be perpetrated by irresponsible employees.) is unlikely. How else in the information age in which we live , will employers be able to advertise, contract, network with international companies and engage clients on a international scale and in doing so making themselves global players without the use of the Internet, e- mail, telephone , fax and of course a computer.

In other words the litigation involving employers being sued by employees for invasion of privacy, for defamation, and for harassment is not going to disappear from CCMA or Labour Court rolls any time soon.

Bearing this in mind, it may be seen that it is not unreasonable for employers to use any and all available technologies to monitor employees' conduct. It is generally felt that employees who enter an employer's premises to do paid work have left 'private' space and entered a 'public arena', where they should expect to be observed by their supervisors. This argument however may prove unsustainable, the reason being, that even though individuals are to a large extent under the control of their employers while at work, it is simply not possible for the basic human need for privacy to be given up entirely during working hours. It is true as far as the electronic monitoring of employees is concerned, that employees should expect a degree of supervision. Employers do have a vested interest in monitoring employees' communication in the workplace, but the methods used by the employers must not be intrusive.

Employers would need to take the pro- privacy arguments into account. Privacy is not an absolute right nor is it a paramount value. The right to privacy however is closely linked with the paramount value of human dignity and it exists where there is a reasonable expectation to privacy and the workplace is one such area.

Workers invest much of their lives in the workplace and have an interest in the maintenance of working conditions which acknowledge their existence as autonomous beings. This is particularly true of today's society, where the traditional 'nine- to - five' working hours are no longer a reality for many employees. Employee duty may in such instances continue through evenings and

weekends. In these circumstances, it seems implausible to expect employees to put their private lives on hold and devote 100% of working time to work related matters. This is especially true of private communications of employees who work long and extended hours. Such workers sometimes have no choice but to carry out some private business during working hours.

In the case of *Moonsamy v The Mailhouse* (1999) 20 ILJ 464 (CCMA) (at 496 H-I), the court held that there exist a balancing of competing interests of the employer and employee. This includes the employer's right to economic activity as against the employees' right to privacy. The court held that it was very difficult to clarify, with any degree of precision, the nature of the right to privacy of an employee on the premises of the employer during working hours.

In terms of the *Moonsamy* decision (*supra*), to determine the degree and expectation of privacy the court held that this is determined by the working environment and by a case - by - case basis. A decision held also by American Courts in the case of *Katz v US* 389 US 347 (1967) and *O'Connor v Ortega* 480 US 709 (1987).

According to the *Moonsamy* decision (*supra*), the monitoring, which includes the electronic monitoring of employees can only be conducted by way of prior consent obtained from the employee, consent granted in terms of the employment contract, or authorization by the Labour courts in terms of section 158 of the Labour Relations Act 66 of 1995.

In terms of section 5 of the Regulation of Interception of Communications and Provision of Communication – Related Information Act 70 of 2002, communication may be intercepted if prior consent of such interception is given in writing by one of the parties to the communication.

The best solution for an employer burdened with the issue of employee privacy as well as at the same time trying to protect his business and himself form injury and embarrassment is to draft a policy where the employer acquires not only the right to infringe upon the employee's right to privacy in appropriate circumstances but also to dismiss or discipline an employee for reasons relating to the misuse of communication tools. The policy will serve as the basis of a defence for the employer, against claims which are the result of unlawful actions committed by employees.

BIBLIOGRAPHY

1. Beech, W. "The Right of an Employer to Monitor Employees Electronic Mail, Telephone Calls, Internet Usage and Other Recordings". (2005). 26 *ILJ 654- 659.*

2. Beumont, M "Entrapment: Is all evidence admissible". (2004). 6 *Beumont Express* 73. Butterworths. Accessed: 03 September 2007

3. Burchell, J *Principles of Criminal Law*. 3ed. Cape Town: Juta (2005)

4. Burchell, JM *The Law of Defamation in South Africa.* Cape Town: Juta *(*1985)

5. Calitz, K. "Vicarious liability of employers: reconsidering risk as the basis for liability". (2005). 2 *TSAR* 215- 218.

6. Coetzee, J. "The Electronic Communications and Transaction Act 25 of 2002: facilitating electronic commerce". (2004). 15 (3) *Stell LR* 511 -513.

7. International Labour Office, "Monitoring and Surveillance in the Workplace" (1993). 12. (1), *Conditions of Work Digest* 11.

8. Cohen, T "The Regulation of Interception of Communications and Provisions of Communication-related Information Act, No. 70 of 2002" (2003) *ISPA Advisory 10.*

9. Colucci, M "The Impact of the Internet and New Technologies on the Workplace". Ed. R Blanpain. The Hague, Netherlands: Kluwer Law International (2002).

10. Collier, D. "Workplace Privacy in the Cyberage". (2002). 23 *ILJ* 1756.

11. Court, L. and Warmington, C. "The Workplace Privacy Myth: Why Electronic Monitoring is here to Stay". (2004). *Oklahoma City University Law Review: Employment and Labor Law* 15. *Westlaw*

12. Dancaster, L "Internet Abuse: A Survey of South African Companies". (2001). 22 *ILJ* 862.

13. Dekker, A. "Vice or devices: employee monitoring in the workplace". (2004). *16 (4) SA Merc LJ* 624-635.

14. Dekker, A. “Traps in the context of Labour Law”. (2003). 11 (3) *JBL* 151.

15. De Villiers, R. “Computer programs and copyright; the South African Perpsective”. (2006). 123 (2) *SALJ* 315-337.

16. Ebersohn, G. “Unfair business Practices of Spamming and Spoofing”. (2003). De *Rebus* 25-26.

17. Ebersohn, G. “Analysis of spam legislation”. (2004). 4 (3) *JBL* 137-142.

18. Etsebeth, V. “The growing expansion of vicarious liability in the information age (part 1)”. (2006). 3 *TSAR* 564-566.

19. Etsebeth, V. “The growing expansion of vicarious liability in the information age (part 2)”. (2006). 4 *TSAR* 755- 759.

20. Gereda, S. “The Truth about Spam”. September (2003) De *Rebus* 51-52.

21. Grogan, J. *Workplace Law*. 8 ed. Cape Town: Juta (2005).

22. Grogan, J. “Workplace Privacy: controlling communications abuse”. (2004). 20 (2) *EL* 9.

23. Grogan, J. “Vicarious harassment: Employers become reluctant insurers”. (2004). 20 (4) *EL* 3.

24. Grogan, J “To Catch a Thief”. (2001). 17 (1) *EL* 8.

25. Gule, S. “Employers’ vicarious liability for sexual harassment”. (2005). 13 (2) *JBL* 66 -67.

26. The *Oxford minireference Dictionary & Thesaurus*. Ed. S Hawker & C Cowly. (1997).

27. Hofman, J …et al. *Cyberlaw: A Guide For South Africans Doing Business Online.* Cape Town : Ampersand Press (1999)

28. Hofmeyr, K. “The problem of Private Entrapment”. (2006). *The Criminal Law Review*. 331.

29. Jacobs, W. "The Electronic Communications Act: Consumer Protection and Internet Contracts". (2004) 16 *SA Merc LJ*

30. Lane, F S *The Naked Employee*. Printed in the United States of America (2003)

31. Lawack Davids, VA & van der Walt, A. "Interception of Electronic Communications in the Workplace". (2005). 26 (1) *Obiter* 133- 139.

32. LE Roux, R. "Aspects of South African law as it applies to corruption in the workplace". (2004). 17 (2) *SACJ* 174 – 175.

33. Lidovho, G J. "The internet and the piracy of copyrightable computer software in South Africa: some comparative perspectives". (2006). 123 (2) *SALJ* 339.

34. Lloyd, I J & Simpson, M Law *on the Electronic Frontier*. Edinburgh: Edinburgh University Press (1994)

35. Lyon, D Surveillance *after September 11*. USA: Blackwell Publishing Inc (2003)

36. Lyon, D Surveillance *as Socialising: Privacy, Risk and Digital Discrimination*. London and New York: Routledge (2003)

37. Martin, EA and Law, L. *Oxford Dictionary of Law*. 6 ed. (2006).

38. Manamela, ME. "Vicarious liability: 'paying for the sins of others'": case comments. (2004). 16 (1) SA *Merc LJ 126*.

39. McGregor, M. "The right to privacy in the workplace: general case law and guidelines for using the Internet and e- mail". (2004.) 16 (4) *SA Merc LJ*

40. Mcgrath, JE *Loving Big Brother: Performance, Privacy and Surveillance Space*. London and New York: Routledge (2004)

41. McGregor, M. "The use of e- mail and Internet at Work". (2003). 11 (3) *JBL*190-192

42. McQuoid –Mason, D "Invasion of privacy: common law v constitutional law delict: does it make a difference?". (2000). *Acta juridica* 227-254

43. Michalson, L. “The use of the e- mail and the Internet in the Workplace” In: *Cyberlaw S.A: the internet and the law*. CD-ROM (1999) 196- 209.

44. Mischke, C. “Workplace Privacy, e- mail interception and the law”. (2003). 12 (8) *CLL* 72- 78.

45. Mischke, C. “Disciplinary action and the Internet”. (1999). 9 (5) *CLL* 43- 46.

46. Mischke, C. “Disciplinary action and the internet: responding to employee abuse of e-mail, network access and internet access”. (1999) 12 *CLL* 46.

47. Mischke, C. “Dismissal for abuse of e- mail”. (2002). 11 (6). *CLL* 51.

48. Modiba, M. “Intercepting and Monitoring Employees e- Mail Communications and Internet Access”. (2003). 15 (3) *SA Merc LJ*

49. Monmonier, M *Spying with Maps*. Chicago: The University of Chicago Press (2004)

50. Morris, J “The Use and Monitoring of E- mail and the Internet at Work in English Law”, *Bulletin of Labour Law and Industrial Relations,* No. 40, 2001, Kluwer Law International

51. Muhl, C J. “Workplace e-mail and Internet use: employees and employers beware” February (2003) Monthly *Labor Review* 37

52. Safavi -Naini, SR and Yung, M Digital Rights Management: Technologies, Issues, Challenges and Systems. (selected papers) (Eds). Germany : Springer (2005)

53. Neethling, J. “The concept of privacy in South African law: notes”. (2005). 122 (1) *SALJ* 18-28

54. Norris, C & Wilson, D Surveillance*, Crime and Social Control.* England: Ashgate Publishing Limited (2006)

55. Oliver, H. “E- mail and Internet Monitoring in the Workplace: Information Privacy and Contracting - Out” (2002) 31 *ILJ* 321-322.

56. Pfleeger, CP & Pfleeger, SL Security *in Computing*. 4 ed. Massachusetts.: Prentice Hall (2006)

57. Pistorius, T. "From snail to e- mail- a South African perspective on the web of conflicting rules on the time of e- contracting". (2006). 39 (2) *CILSA* 178-213.

58. Pitt, G Employment *Law*. (5ed). United Kingdom: Ashford Colour Press. (2004)

59. Ressler, JS. "Privacy, "Plaintiffs, and Pseudonyms: The Anonymous Doe Plaintiff in the Information Age". (2004). 53 (1) The *University of Kansas Law Review*. 196-202.

60. South African Law Reform *Commission Privacy and Data Protection* project 124. (2005). 15

61. Schwikkard, PJ & van der Merwe, S Principles *of Evidence*. 2 ed. Cape Town: Juta (2002)

62. Schachter, V. & Swanson, SM. "Workplace Privacy and Monitoring: New Developments affecting the Rights of Employers and Employees" (2006) Order No. 8966 Practising *Law Institute* 152-153. *Westlaw*

63. Snyman, CR *Criminal Law*. 4 ed. Durban: Butterworths (2002)

64. Stassen, P. & Stassen, K. "New Legislation". (2005). *De Rebus* 39-40.

65. Squires, D. "The Problem with Entrapment". (2006) 26 (2). *Oxford Journal of Legal Studies*. 351- 376.

66. *Van Eck, BPS "*Misuse of the Internet at the Workplace*".* (2001). *De Jure* 46

67. Van Jaarsveld, M. "Forewarned is Forearmed: Some Thoughts on the Inappropriate Use of Computers in the Workplace*".* (2004). 16 (4) *SA Merc LJ* 661

68. Van der Walt, JC & Midgley, JR *Principles of Delict*. 3 ed. Durban: Lexis Nexis Butterworths (2005)

69. Van Zyl, SP. “An employer’s vicarious liability with reference to the internet and e-mail”. (2006). 39 (1) *De Jure* 131-133.

70. Watney, M. “Regulation of Internet pornography in South Africa (1)”. (2006). 69 *THRHR* 227-228

71. Watney, M. “Regulation of Internet pornography in South Africa (2)”. (2006). 69 *THRHR* 385-386.

72. Weckert, J Electronic *Monitoring in the Workplace: Contorversies and Solutions*. United Kingdom: Idea Group Publishing (2005)

CASE LIST

ABSA Bank Ltd v Born Equipment (Pretoria) (Pty) Ltd 2001 (1) SA 372 (SCA)

Allied Workers Union of South Africa obo Ncube v Northern Crime Security CC (1999) 20 ILJ 1954 (CCMA)

Bamford & Others/ Energiser (SA) Ltd (2001) 12 BALR 1251 (P),

Bartnicki v. Vopper, 532 U.S. 514, 541-42, n.1 (2001)

Bazley v Curry (1999)174 DLR (4^{th})

Bernstein v Bester 1996 (4) BCLR 449 (CC)

Blakey v. Continental Airlines, Inc., 751 A.2d 538 (N.J. 2000)

Bohach v. City of Reno, 932 F.Supp. 1232, 1233 (D. Nev. 1996).

Boothman v Canada [1993] 3 FC 381 (TD)

Briggs v. American Air Filter Co., Inc., 455 F. Supp. 179, 180- 82 (N.D. Ga.)

Cape Town City Council v South African Municipal Workers Union obo Beukes and Dollie (2000) 21 *ILJ* 2409 (LAC)

Caji and African Personnel Services (Pty) Ltd (2005) 26 *ILJ* 150 (CCMA)

Changula v Bell Equipment (1992) 13 ILJ 101 (LAC)

Chemical Workers Industrial Union & another v AECI Paints (Natal) (Pty) Ltd (1988) 9 ILJ 1046 (IC)

Copley v. Bax Global, Inc, 80 F. Supp. 2d 1342, 1344 (S.D. Fla. 2000)

Cronje/ Toyota Manufacturing (2001) 3 BALR 213 (CCMA)

County Fair Foods (Pty) Ltd v CCMA & others (1999) 11 BALR 1117 (LAC)

Costa da Ouro v Reddy 2003 4 SA 34 (SCA)

CWU v Mobile Telephone Networks (Pty) Ltd 2003 8 BLLR 741 (LC)

Cycad Construction (Pty) Ltd v CCMA & Others (1999) 20 *ILJ* 2340 (LC) 2344A–E)

Dauth / Brown and Weir's Cash and Carry [2002] 8 BALR 837 (CCMA)

Deal v. Spears, 980 F.2d 1153, 1155-57 (8th Cir. 1992)

Epps v. St. Mary's Hosp. of Athens, Inc., 802 F.2d 412, 416-17 (11th Cir. 1986).

Faragher v City Boca Raton 524 US 775 (1998)

FAWU *obo Karolus and Two a Day Ltd* (WE 8383-02) 24 April 2003;

Feldman (Pty) Ltd v Mall 1945 AD 733

Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 633 (E.D. Pa. 2001)

Garrity v. John Hancock Mutual Life Ins. Co., No. CIV.A. 00- 12143-RWZ, 2002 WL 974676, at 2 (D. Mass. May 7, 2002)

Grieve v Denel (2003) 24 ILJ 551 (LC)

Griggs-Ryan v. Smith ,904 F.2d 112 (1st Cir. 1990)

Grobler v Naspers 2004 (4) SA 220 (C).

Goosen v Caroline's Frozen Yoghurt Parlour (1995) 16 ILJ 396 (IC)

H and M Ltd (2005) 26 ILJ 1737 (CCMA)

Halford v United Kingdom [1997] IRLR 471 ECHR

Harley v. McCoach, 928 F. Supp. (E.D. Pa. 1996)533.

Investigating *Directorate: Serious Economic Offences and Others v Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2001 (1) SA 545 (CC)

In re Pharmatrack, Inc., 329 F.3d 9, 22 (1st Cir. 2003).

James v. Newspaper Agency Corp., 591 F.2d 579, 581 (10th Cir. 1979).

Jandak v. Village of Brookfield, 520 F. Supp. 815, 824-25 (N.D. Ill. 1981)

Jardine / Tongaat Hulett Sugar Ltd [2002] 4 BALR 426 (CCMA);

Johnson v Randy Daily Mails (1928 AD 190)

Katz v US 389 US 347 (1967).

Kalam/ Bevcap (Nampak) (2006) 6 BALR 565 (MEIBC);

Lawrence v I Kuper & Co (1994) 15 ILJ 1140 (IC);

Latchmiah/Billiton Aluminium SA (PTY) LTD T/A Bayside Aluminium (2006) 6 BALR 569 (MEIBC)

Lotus River, Ottery, Grassy Park Residents Association v South Peninsula Municipality 1999 (2) SA 817 (C)

Magajane v Chairperson North West Gambling Board and others (2006) 5 SA 250 (CC)

Marobie – FL, Inc. v. Nat. Ass'n of Fire Equip. Dist 983 F. Supp. 1167 (N.D. III.1997)

Mbuli/ Spartan Wiremakers CC (2004) 5 BALR 598 (MEIBC);

McLaren v. Microsoft Corp, 1999 WL 339015 (Tex. Ct. App. 1999)

Media 24 v Grobler 2005 JDR 738 (SCA)

Meloff v. New York Life Inc, 51 F.3d 372 (2nd Cir. 1995), on remand at No. 92 CIV .7126 KTD, 1999 WL 604871 (S.D.N.Y., 10 August 1999).

Metrorail and SA Transport & Allied Workers Union on behalf of Magagula (2002) 23 ILJ1641 (BCA)

Minister of Safety & Security v Jordaan t/a Adre Jordaan Transport 2000 (4) SA 21 (SCA)

Ministre du Travail v. Societe Peintures Corona [1980] 6 Dr. Soc. 317

Minister of Law and Order v Ngobo 1992 4 SA 822 (A)

Mistry v Interim Medical and Dental Council of South Africa and Others 1998 (4) SA 1127 (CC)

Moonsamy v Mailhouse 1999 (20) ILJ 464 (CCMA)

Morse v Future Reality Ltd (ET case number 54571/95).

Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002)

Philander/ CSC Computer Sciences (2002) 3 BALR 304 (CCMA)

National Media v Bogoshi 1998 4 SA 1195 (SCA)

National Media Ltd and Another v Jooste 1996 (3) SA 262 (A)

National Media Ltd and Another v Jooste 1994 (3) SA 634 (C)

Nottingham City Council v *Amin* [2000] 1 WLR 1071

Ntsabo v Real Security CC [2004] 1 BLLR 58 (LC)

Numsa obo/ Abrahams / Guestro Wheels (2004) 4 BALR 520 (CCMA)

O'Connor v Ortega 480 US 709 (1987)

Owens v Morgan Stanely and Co. Inc., No. 96 Civ. 9747, 1997 WL 403454 (S.D.N.Y 1997).

Proceedings Commissioner v Ali Hatem 1999 1 NZLR 30

Protea Technology Ltd and another v Wainer and others 1997 (9) BCLR 1225 (W)

Pretoria Society for the care of the Retarded v Loots (1997) 18 ILJ 981 (LAC)

Rv Dyment 1988 (2) SCR 417

S v Dube 2002 (2) SA 586 (N)

S v Kidson 1999 (1) SACR 338 (W)

S v Malinga 1963 (1) SA 692 (A)

S v Chesane 1975 (3) SA 172 (T)

S *v Petkar* 1988 (3) SA 571 (A)

SACCAWU obo Libi and Weirs Cash & Carry (EC 2163 – 01), 3 April 2002;

SACCAWU on behalf of Jacobs and Portswood Hotel (WE 39639) 29 June 2001

SA Polymer Holding t/a Magpak (1996) 8 BALR 978 (LAC)

SA Transport & Allied Workers Union on behalf of Assegai v Autopax (2002) 2 BALR 171 (AMSSA)

SATAWU on behalf of Radebe v Metrorail Wits (2001) 22 ILJ 2372 (ARB)

Smuts v Backup Storage Facilities [2003] 2 BALR 219 (CCMA)

Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996)

South African Railways & Harbours v Marais (1950 (4) SA 610(A)

Sugreen / Standard Bank of SA [2002] 7 BALR 769 (CCMA)

Sylvester / Neil Muller Constructions [2002] 1 BALR 113 (CCMA)

Tap Wine Trading CC and another v Cape Classic Wines (Western Cape) CC and another 1999 (4) SA 194 (C)

Third Circuit in Fraser v. Nationwide Mutual, 352 F.3d 107 (2d Cir. 2003).

Toker Bros (Pty) Ltd and Keyser (2005) 26 ILJ 1366 (CCMA)

Tshishonga v Minister of Justice & Constitutional Development & another (2007) 28 ILJ 195 (LC)

United States v. Mullins, 992 F.2d 1472 (9th Cir. 1992)

United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003)

Van Wyk Independent Newspapers Gauteng (Pty) Ltd and others (2005) 26 ILJ 2433

(LC)

Vega-Rodriguez v. P. R. Tel. Co., 110 F.3d 174, 179 (1st Cir. 1997)

Vernars v Young 539 F.2 966 (3d Cir 1976)

Viljoen v Smith 1977 (1) SA 309 (A)

Volkwyn / Truworths Ltd [2002] 4 BALR 455 (CCMA)

Watkins v. L.M. Berry & Co., 704 F.2d 577, 582-84 (11th Cir. 1983)

Witham v Minister of Home Affairs 1989 (1) SA 116 (ZH)

Legislation

South Africa

- Film and Publications Amendment Act 18 of 2004
- The Regulation of Interception of Communications Related Information Act 70 of 2002
- The Electronic Communications and Transaction Act 25 of 2002
- Protected Disclosure Act 26 of 2000
- The Employment Equity Act 55 of 1998
- Basic Conditions of Employment Act 75 of 1997
- Labour Relations Act 66 of 1995
- Films and Publications Act 65 of 1996
- Constitution of the Republic of South Africa Act 108 of 1996
- Copyright Act 98 of 1978

France

- Computer Science and Freedom Act of 6 January 1978

Germany

- Telecommunications Act of 25 July 1996

Italy

- The Data Protection Act and the Workers' Statute Act 31 of 1996

United States of America

- Electronic Communications Privacy Act , 18 U.S.C

Websites

1. Amagid. "Work Computers Not Protected by Privacy Rules". .https://message.computerlaw.com/GH_PrintFriendly.asp?HID=40&CATID. Accessed : 05October 2007

2. AMA Survey, Workplace Monitoring and Surveillance: Policies and Practices (American Management Assoc. 2001), at http:// www.amanet.org/research/pdfs/emsfu_short.pdf. Acessed 23 February 2007

3. M J Bassett et al. … " An Overview of E-Mail and Internet Monitoring in the Workplace. http://www.fmew.com/archive/monitoring/.

4. Dichter and Burkhardt, "Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age". (June 1999), available at <http://www.mlb.com/art61499.html>> Accessed: 04 October 2007.

5. W M Gavre. "E-Mail Sexual Harassment, Company Liability and Document Production". (2000). http://www.parsonsbehlelaw.com/publications.asp?ID=267&Topic. Accessed: 04 October 2007

6. SE Gindon, "Guide to Internet and e –mail in the Workplace". http://www.info-law.com/guide.html. Accessed 05 October 2007

7. Regulation of Investigatory Powers Act (RIPA), The "Regulation of Investigatory Powers Act" is available at, << http://www.legisaltion. hmso.gov.uk/acts/acts2000/20000023.htm>>. Accessed: 25 May 2007

8. www.hmso.gov.uk/si2000/20002699.htm

9. www.new-law-journal.co.uk/Index/Index%201999%20.pdf

10. http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm>

11. www.spectorsoft.com. Accessed: 03 October 2007