THE SOUTH AFRICAN EMPLOYER'S REGULATION OF INTERNET MISUSE IN THE WORKPLACE

by

BIANCA LEE-ANNE SINGH

211541441

This Research Project is submitted in partial fulfilment of the regulations for the LLM Degree at the University of KwaZulu-Natal.

STATEMENT OF ORIGINALITY

This project is an original piece of work which is made available for photocopying and for inter-library loan.

_____

ACKNOWLEDGEMENTS

My Lord and Saviour Jesus Christ without whom I am nothing, for giving me the strength to complete this work. My parents Sue and Manoj Singh to whom I am eternally grateful for your love, sacrifices and support that continually surrounds me. Last my dear Kyle Nalathoren for all the encouragement and belief in me even when I did not believe in myself.

Isaiah 40:31

”but those who hope in the LORD will renew their strength. They will soar on wings like eagles; they will run and not grow weary, they will walk and not be faint.”

CONTENTS

TABLE OF CASES AND STATUTES

Cases

Bernstein V Bester NO 1996 (2) SA 751 (CC).

Bramford & others v Energiser (SA) Limited [2001] 12 BALR 1251 (P).

Council for Scientific & Industrial Research v Fijen (1996) 17 ILJ 18 (A).

CWU v Mobile Telephone Networks (Pty) (Ltd) 2003 8 BLLR 741 (LC).

Dauth and Brown & Weirs Cash & Carry (2002) 23 ILJ 272 (CCMA).

Galago Publishers (Pty) Ltd v Erasmus 1989 1 SA 276 (A)

Goosen v Carolines Frozen Yoghurt Parlour (Pty) Ltd and another 36 (1995) 16 ILJ 396 (IC)

Gouws Score v Price and Pride Furnishers [2011] 11 BALR 1155 (CCMA).

Grobler v Naspers Bpk 2001 (4) SA 938 (LC)

In Re Hyundai Motors Distibutors (Pty) Ltd and Others v Smith and NO and Others 2001 (1) SA 545 (CC).

Jane Doe v XYZ Corporation 382 N.J.Super. 122 (Appellate Division N.J., December 27, 2005).

Knox v State Department of Indiana 93 F 3d 1327.

Memela and Another v Ekhamanzi Springs 33 ILJ 2911 (LC) 2012.

Moonsamy v Mailhouse (1999) 20 ILJ 464 (CCMA).

Morse v Future Reality Ltd ET case number 54571/95.

MWO obo Coetzer v Champion Casinos (CCMA 15 August 2000 (case number 16821) unreported).

NK v Minister of Safety and Security 2005 (6) SA 4 9

Owens & Hutton v Morgan Stanley & Co Inc United States District Courts Southern District of New York 96 CIV 9747 (1996).

Philander v CSC Computer Sciences [2002] 3 BALR 304 (CCMA)

Premier Medical and Industrial Equipment (Pty) Ltd v Winkler & Another 1971 (3) SA 866 (W).

Protea Technology Ltd and another v Wainer and others (1997) 9 BCLR 1225 (W).

Sappi Novoboard (Pty) Ltd v Bolleurs (1998) 19 ILJ 784 (LAC).

Sedick and another/ Krisay (Pty) Ltd [2011] BALR 879 (CCMA)

Statutes

Constitution of the Republic of South Africa

Copyright Act No 98 of 1978

Electronic Communications and Transactions Act No 25 of 2005

Employment Equity Act No 55 of 1998

Compensation for Occupational Injuries and Diseases Act 130 of 1993

Occupational Health and Safety Ac No 85 of 1993

Regulation of Interception of Communications and Provision of Communicated-related Information Act No 70 of 2002

The Code of Good Practice on Dismissal

The Code of Good Practice on the Handling of Sexual Harassment Cases GG No 19049 of 17 July 1998.

Film and Publications Board Act No 65 of 1996

TABLE OF BOOKS AND ARTICLES

Books

Burchell J *The law of defamation in South Africa* Cape Town: Juta, (1985)

Buys R *Cyberlaw@SA: the law of the Internet in South Africa* 3ed Pretoria: Van Schaik, (2000).

Neethling J, Potgieter JM & Visser PJ *Law of Delict* 4ed Durban: Lexis Nexis, (2002).

Papadopolous S & Snail S *Cyberlaw @ SA III : The law of the Internet in South Africa* 3ed Pretoria: Van Schaik, (2012).

Van Jaarsveld F & Van Eck BPS *Principles of Labour Law* 2ed Durban: Lexis Nexis, (2002).

Journals

Aiello JR 'Computer based monitoring: Electronic surveillance and its effects' (1993) 23(7) *Journal of Applied Social Psychology* 499-507.

Beech W 'The right of an employer to monitor employees electronic mail, telephone calls, internet usage and other recordings' (2005) 26 *Industrial Labour Law Journal* 650-660.

Bibby A 'Who got e-mail' At work, e-mail and the web become public'(2001) 40 *The magazine of the ILO World of Work* 1-34

Boyd DM & Elison NB 'Social network sites: Definition, history and scholarship' (2008) 13 *Journal of Computer-Mediated Communications* 210-230.

Calisti MC 'You are being watched: The need for notice in employer monitoring' (2008) 96(4) *Kentucky Law Journal* 649-668.

Calitz K 'Vicarious liability of employers: Reconsidering risk as the basis for liability' (2005) 3 *TSAR* 215-235.

Chalykoff J & Kochran TA 'Computer-aided monitoring: Its influence on employee satisfaction and turnover' (1989) 40 *Personnel Psychology* 807-834.

Ciochetti C 'The eavesdropping employer: A 21st century framework for employer monitoring' (2001) 48 *American Business Law Journal* 285-369.

Coetzee J 'The Electronic Communications and Transaction Act 25 of 2002: Facilitating electronic commerce' (2004) 3 *Stellenbosch Law Review* 501-521.

Collier D 'Workplace privacy in the cyber age' (2002) 23 *Industrial Labour Journal* 1743-1760.

Currie I 'The concept of privacy in the South African Constitution: Reprise' (2008) 3 *TSAR* 449-557.

Ebersohn G 'Internet Law: Peer-to-peer file sharing services' (2003) 2 *TSAR* 376-381.

Ebersohn G 'The unfair business practises of spamming and spoofing' (2003) *De Rebus* 25

Etsebeth V ' The growing expansion of vicarious liability in the information age (part 1)' (2006) 3 *TSAR* 564-580.

Etsebeth V ' The growing expansion of vicarious liability in the information age (part 2)' (2006) 4 *TSAR* 752-765.

Dancaster L 'Internet Abuse: A survey of South African companies' (2001) 22 *Industrial Labour Journal* 862-865.

David J 'Policy enforcement in the workplace' (2002) 21 *Computers and Security* 506-513.

Fazekas CP '1984 is still Fiction: Electronic monitoring in the workplace and US privacy law' (2004) 15 *Duke Law and Technology Review* 1-16.

Fereirra A & Du Plessis T 'Effect of online social networking on employee productivity' (2009) 11 *South African Journal of Information Technology* 1-11.

Flanagan JA 'Restricting electronic monitoring in the private workplace' (1994) 43(6) *Duke Law Journal* 1256-1281.

Frayer CE 'Employee privacy and internet monitoring: Balancing workers rights and dignity with legitimate management interets' (2002) 57(2) *Business Lawyer* 857-874.

Gilburg D 'Management techniques for bringing out the best in generation Y, CIO, Oct. 26, 2007. Available at:http://www.cio.com/article/149053/Management_Techniques_for_Bringing_Out_the_Best_in_Generation_Y (Accessed on 20 June 2015).

Griffiths M 'Internet abuse in the workplace: Issues and concerns for employers and employment counsellors' (2003) 40 *Journal of Employment Counselling* 87-96.

Gule S 'Employers vicarious liability for sexual harassment' (2005) 13(2) *Journal Business Law* 66-69.

Hathi S 'billions lost from social networking' (2008) 12(2) Computers and Security 9.
Horung MS 'Think before you type: A look at e-mail privacy in the workplace' (2005) 11 *Fordham Journal of Corporate and Financial Law* 115-160.

Jansen M 'The protection of copyright on the internet' (2004) 12(2) *Journal Business Law* 100-104.

Jansen M 'The protection of copyright works on the internet- an overview' (2005) 38(3) *The Comparative and International Law Journal of Southern Africa* 344-354.

Johnson J 'Information Technology Policies' (2001) De Rebus 38.

Kesan JP 'Cyber-working or cyber-shrinking?: A first principlesexamination of electroniv privacy in the workplace' (2002) 54(2) *Florida Law Review* 289-332.

Lawacks V & Van der Walt A 'Interception of electronic communications in the workplace' (2005) *Obiter* 133-139.

Le Roux R 'Section 60 of the Employment Equity Act 1998: Will a comparative approach shake the joker out of the pack?' (2006) 27(3) *Obiter* 411-428.

Manmela ME 'Vicarious liabilty: Paying for the sins of others' (2004) 16 *South African Mercantile Law Journal* 125-132.

McGregor M 'The right to privacy in the workplace: General case law and guidelines for using the internet and e-mail' (2004) 16 *South African Mercantile Law Journal* 638-649.

McGregor M 'The use of e-mail and internet in the workplace' (2004) 11(3) *Journal of Business Law* 189-192.

Mischke C 'Intercepting and monitoring employees e-mail communications and internet access' (2003) 12(8) *Contemporary Labour Law* 72-76

Mobida M 'Intercepting and monitoring employees e-mail communications and interenet access' (2003) 15 *South African Mercantile Law Journal* 363-371.

Mobida M 'Who should be liable?' (2003) 11(2) *Journal of Business Law* 112-115.

Muhl C 'Workplace e-mail and internet use: Employees and employers beware' (2004) 26(2) *Monthly Labour Law* 36-45.

A Mukhebeir & L Ristow 'An Overview of sexual harassment: Liability of the employer' (2006) Obiter 259-262.

Nebeker DM & Tatum BC 'The effects of computer monitoring, standards and rewards on work performance, job satisfaction and stress. (1993) 23(7) *Journal of Applied Psychology* 508-537.

Nel S 'Problematic issues regarding transborder cybersmear' (2010) 22 *South African Mercantile Law Journal* 360-387.

Papa LJ & Bass SL 'How employers can protect themselves from liability for employees misuse of computer, internet, and e-mail systems in the workplace'(2004) 10 *Boston Journal of Science and Technology Law* 110-124.

Paul RA & Chung LH 'Brave new cyberworld: The employers legal guide to interactive internet' (2008) 24 *Labour Law* 109-142.

Pistorius T 'Monitoing interception and the big boss in the workplace: is the devil in the details?' (2009) *Potchefstroom Electronic Review* 1-26.

Riedy MK & Wen JH 'Electronic sureviellance of internet access in the American Workplace: Implications for management' (2010) 19 *Information of Technology and Law* 87-99.

Roos A 'Privacy in the facebook era: A South African legal perspective' (2012) 129 *The South African Law Journal* 375-402.

Rothstein LE 'Privacy or dignity?: Electronic monitoring in the workplace' (2000) 9(3) *New York Law School Journal of International and Comparative Law* 379-412.

Smit N & Van der Nest D 'When sisters are doing it for themselves: Sexual harassment claims in the workplace' (2004) 3 *TSAR* 520-543.

Stafford C & Mearns MA ' What happens when organisations embrace social networking? Knowledge sharing at multinational business solution corporations' (2009) 11(4) *South African Journal of Information Management* 1-11.

Subramanien D & Whitear-Nel N 'A fresh perspective on South African law relating to the risks posed to employers when employees abuse the internet' (2013) 37 *South African Journal of Labour Relations* 9-23.

Swaya ME & Einstein SR 'Emerging technology in the workplace' (2005) 21 *Labor Lawyer* 1-18.

Thomas JH, Englander F & Englander V 'Ethical, legal and economic aspects if employer monitoring of employee electronic mail' (1999) 19 *Journal of Business Ethics* 99-108.

Van Eck BPS 'Misuse of the internet at the workplace' (2001) 2 *De Jure* 364-369.

Van Jaarsveld M 'Forearmed is forewarned: Some thought on the inappropriate use of computers in the workplace' (2004) 16 *South African Mercantile Law Journal* 651-666.

War WA 'Social software: Fun and games, or business tools' (2008) 34(4) *Journal of Information Science* 591-604.

Whitear-Nel N 'Child pornography in the workplace' (2011) 32 *Industrial Law Journal* 787-804.

Young KS & Case CJ ‘Internet abuse in the workplace: New trends in risk management’ (2004) 7 *CyberPsychology and Behaviour* 105-111.

Zhou AZ & Fink D ‘The intellectual capital web’ (2003) 4 *Journal of Intellectual Capital* 34-48.

1. INTRODUCTION

It is highly unlikely that any business can be successfully co-ordinated without the use of computers and the internet. It can almost be said with certainty that every business requires the use of such technology. The necessity for the use of technology in the work place has increased so much over the years that it can be regarded as an inherent tool needed to accomplish almost any task. This means that employees spend a lot more time engaging with technology than previously and this can often become a slippery slope very quickly as employers may face serious consequences when their employees inappropriately use internet facilities provided by them.

The provision of computers and internet facilities in the work environment should serve one main function and that should be to enable employees to use such resources to advance the employers interests. However this is not the reality of what actually happens within an employees work space. Employees use these facilities for personal reasons and not for work related purposes and it is this type of misuse that creates tension in the workplace between the interests of the employer and that of the employee.

The unauthorised use of internet in the workplace by employees leaves employers potentially vulnerable to legal liability. The employer as a result of this unauthorised use faces consequences for actions belonging to his employee's online activities. The employer may foresee such problems and the risks that his employee's abuse can cause to his business such as both criminal and civil liability as well as the lowering of the employer's reputation and try to curb any occurrences of misuse by implementing strategies in the workplace to deal with this such as monitoring internet use and disciplinary action.

Despite the legal nature of the problem facing employers there is also a social element to this type of problem of internet misuse in the workplace that is often overlooked which may hold the key to reducing internet abuse. This requires an examination into the reasons why the internet is abused and striking a balance between the interests of the employer and the employee to ensure a healthy working environment where employees are performing tasks efficiently and employee morale is high. Employee morale was often the determining factor in the past approach to regulation and the reason why regulation remained minimal for a long period of time.

1.1 History of regulation in South Africa

Since the inception of the computer in the workplace and prior to the risks of internet abuse becoming apparent to employers in the working environment, employers often adopted a laissez-faire approach to regulation[1]. In light of this unregulated approach most employers encouraged employees to better acquaint themselves with technology and practices such as surfing the internet[2]. The reasoning behind such a free reign was owed to employer's belief that employees who used the internet for amusement would in return be better equipped to use such facilities at work[3]. These employers failed to see the risks to their companies that such an approach would result in as well as the grave potential for abuse.

However not all employers opted for this approach of no regulation of internet facilities. There were employers who recognised the danger of having internet usage at work being completely unregulated and adopted an informal approach to regulating these facilities[4]. These informal policies for regulation proved to be ineffective as it lacked a coherent strategy to effectively deal with abuse[5]. Many employers were reluctant to put into action any formal measures to regulate the use of internet facilities as they believed that regulating and the monitoring of internet usage would negatively impact upon company's culture and employee morale as employees would constantly feel as though they were being watched or spied on[6].

In present times such a relaxed view is no longer accepted[7]. This is largely attributed to the increasing number of company's who have been called upon to account for the online activities of their employees as well as to deal with the impact that such misuse has upon the employers business. Examples of this can be found in the following cases which illustrate the rationale behind why a passive approach cannot be used. An American oil company was ordered to pay $2 million in damages to a female employee who received emails of a sexual nature from the internal server or British insurance company who had to pay half a million pounds for the actions of his employees who sent out defamatory emails regarding their main

[1] M Mcgregor 'The use of e-mail and internet at work' (2004) 11(3) *Journal of Business Law* 189.
[2] M Mcgregor ''The right to to privacy in the workplace: General case law and guidelines for using the internet and e-mail' (2004) 16 *South African Mercantile Law Journal* 644.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] L Dancaster 'Internet abuse: A survey of South African companys' (2001) 22(4) *ILJ* 862.
[7] M McGregor 'The use of e-mail and internet at work' (2004): (note 1 above) 189

competitor[8]. Although these are not South African based cases they provide a sound illustration for why the past approach of non-regulation can no longer be accepted.

The need for regulation is even greater in present times as those entering the workforce now classified as Generation Y is much younger than those employees who have previously been employed[9]. This means that they are more prone to using internet facilities for personal reasons during working hours. Another reason why the need for regulation cannot be ignored is that employee's tend to be working longer hours than in the past[10]. This often means that the internet is used for recreational purposes as a form of escapism from these long working hours[11]. Furthermore the introduction of Wi-Fi in the workplace creates the need for regulation as it allows employees the freedom to access the employer's domain on almost any device. This creates both the opportunity and access for abuse as employees most likely have the passwords and unlimited use of the network[12]. A change in the way regulation takes place is also imperative as the risks posed by internet misuse and the interests of the employer it infringes is much greater than the past as more and more of the employer's business is now technologically dependant.

1.2 Interests of the employer threatened by misuse.

1.2.1 Decrease in productivity

Internet usage for employee's personal use and not for the employer's business interests in the workplace has an enormous potential to be a distraction to employees during working hours[13]. As employers spend more time on the internet for non-work related purposes, this leads to a decrease in employee productivity. This results in employees failing to complete assigned tasks or handing in tasks that are delayed[14]. The decrease in productivity can often be attributed to the use of social networking sites for recreational purposes[15]. This includes the use of networks such as Facebook, Twitter, Instagram and Snapchat among many others

[8] A Bibby 'Who got e-mail' At work, e-mail and the web become public'(2001) 40 T*he magazine of the ILO World of Work* 2

[9] D Gilburg 'Management techniques for bringing out the best in generation Y, CIO, Oct. 26, 2007. Available at:http://www.cio.com/article/149053/Management_Techniques_for_Bringing_Out_the_Best_in_Generation_Y (Accessed on 20 June 2015).

[10] M Griffiths 'Internet abuse in the workplace: Issues and concerns for employers and employment counsellors' (2003) 40 *Journal of Employment Counselling* 91.

[11] Ibid.

[12] M Griffiths (note 10 above) 90.

[13] C Ciochetti 'The eavesdropping employer: A 21st century framework for employer monitoring' (2001) 48 *American Business Law Journal* 285.

[14] M McGregor 'The use of e-mail and internet at work' (2004) (note 1 above) 189.

[15] S Hathi 'billions lost from social networking' (2008) 12(2) *Computers and Security* 9.

which are becoming increasingly popular. Productivity is further decreased as blockages in the systems occur when the system is being used to its capacity[16]. This is due to the overloading of networks when the internet is excessively used by many users at the same time[17]. These blockages in the system mean that incoming and outgoing business e-mails and other electronic messaging cannot reach the employer's business[18]. This was evidenced in the Dancaster study where it was found that 68.83% of employers had problems with employees loafing on the internet during work hours[19].

1.2.2 Abuse of company resources

Internet misuse by employees has damaging and long lasting effects on the company's essential resources which it requires to function at optimal levels. Use of the internet for reasons other than the employers business can lead to efficiency of the employer's computer systems being compromised[20]. These systems cost the employer large sums of money and repairs to them do not come cheap. Employee overuse leads to the systems either slowing down or becoming blocked[21]. The sole cause of this attributed to how simply one can share, download or live stream large files off the internet such as video, music and other media files[22]. This threat is rapidly increased when employee's access social networking sites and other third party applications as these sites promote the sharing of these files which is a common practice associated with using social media[23]. The Dancaster study evidenced this point by finding that 64.71% of employers had problems with degrading system performance due to employee misuse of workplace internet facilities.

When employees spend excessive amounts of time during the working day on the internet for purposes other than their assigned tasks, it endangers the professional reputation of the employers business as employees may use this opportunity to post unprofessional posts on social networks, blogs and chat rooms that the employer does not want to be associated

[16] M McGregor 'The right to privacy in the workplace: General case law and guidelines for using the internet and e-mail' (2004) (note 2 above) 646.
[17] Ibid.
[18] L Dancaster (note 6 above) 865.
[19] Ibid.
[20] M McGregor ''The right to privacy in the workplace: General case law and guidelines for using the internet and e-mail' (2004) (note 2 above) 646.
[21] Ibid.
[22] C Ciochetti: (note 13 above) 286.
[23] R A Paul & L H Chung 'Brave new cyberworld: The employer legal guide to the interactive internet' (2008) 24 *Labor Law* 109.

with[24]. This threat is heightened by the possibility that the business name could be linked to inappropriate content posted by employees especially if it is accompanied by the company's logo[25]. One of the biggest threats to the employer is the possibility that employee's misuse of the internet may result in confidential information and trade secrets being made public or leaked online[26]. This exposes the employer to corporate espionage and sabotage[27]. It is also possible for the employers systems to be weakened when employee's access unauthorised sites[28]. The reason for this is that it creates the opportunity for malicious software to infiltrate the company's systems this may ultimately result in viruses and even the collapse of the entire system[29].

It is clear that unfettered use of the internet has serious ramifications for the business of the employer as well as deep financial implications. However the most serious consequence that employers are bound to face as a result of employee misuse is the legal liability they are held accountable for on the part of their employees.

2. EMPLOYERS CRIMINAL AND CIVIL LIABILTY FOR EMPLOYEES INTERNET ABUSE.

Employees taking their internet use at work a bit too far passed the uses authorised by the employer may seem harmless but there are real and dangerous threats that are present which frequently leave the employer exposed and vulnerable to liability for the acts of his employees while at work. The employer therefore opens himself up to both criminal and civil liability for the online conduct of his employees.

2.1 Criminal liability

Under the Film and Publications Board Act No 65 of 1996 an employer may face criminal charges if employees view or possess child pornography in the workplace. Adult pornography does not form part of the ambit of this act for criminal law purposes and it is exclusively child pornography over which a criminal sanction exists.

---

[24] Ibid 118.
[25] Ibid 119.
[26] D Collier 'Workplace privacy in the cyberage' (2002) 23 *ILJ* 1743.
[27] T Pistorius 'Monitoring, interception and the big boss in the workplace: is the devil in the detail' (2009) *Potchefstroom Electronic Review* 4.
[28] N Whitear-Nel & D Subramanien 'A fresh perspective on South African law relating to the risks posed to employers when employees abuse the internet' (2013) 37 *South African Journal of Labour Relations* 11.
[29] Ibid.

Section 2 criminalises child pornography and makes it a punishable offence in our law to access, store or watch child pornography[30]. The Acts scope is wide and it creates upon the employer positive obligations in respect of child pornography. The effect of this is that an employer who suspects, knows or even ought to know that an employee is in possession or is viewing child pornography can be criminally liable for if the employer does not take the steps required by the Act.

Section 24B of the Act makes it an offence to access child pornography[31]. The Act even goes as far as to make it an offence to take steps to access child pornography. This means even typing in a web address of a child pornography site or entering a site which may contain such material is an offence. Possession of child pornography is also a further violation of the Act. Possession of child pornography affects the employer because the meaning of possession is taken to include custody, control, and supervision over a computer or computer system or data storage medium on behalf of another[32]. This suggests that an employer is in possession of child pornography if the employer is in control of the computers in the workplace or the owner of computers which have been used by employees to access child pornography[33]. The meaning of possession according to the act may also lend itself to the situation in which the employee is given a laptop which he may take home and use out of working hours [34]. Therefore where an employee uses this laptop to access or store child pornography the employer will still be liable because as the owner of the laptop the employer is deemed to be in possession of it and this will mean in possession of the contents of the laptop.

The problem with child pornography in the workplace where the employer is held criminally liable is that some form of fault must be present for a crime to have been committed[35]. It would seem that drafters of the legislation envisaged this in the form of *dolus eventualis*. Therefore if *dolus eventualis* is present this would be enough to hold the employer liable criminally under the act for an employee's possession or accessing of child pornography. *Dolus eventualis* in this context would mean that an employer had knowledge of the child

[30] Film and Publications Board Act No 65 of 1996.
[31] Whitear-Nel 'Child pornography in the workplace' (2011) 32 I*LJ* 788.
[32] S1 Film and Publications Board Act
[33] Whitear-Nel (note 31 above) 788.
[34] Ibid
[35] Ibid 789.

pornography been accessed or foresaw the possibility of child pornography being accessed but remained passive and took no action in trying to stop it[36].

Even though the employer has a duty in terms of the act to take positive steps to stop child pornography from being accessed at work this alone is not enough for him to evade criminal sanctions. This duty extends further and the employer is obliged by the act to report these activities to the South African Police Services. The employer has a legal duty resting upon him to report to the SAPS not only when he has knowledge of the crime taking place but also when he even suspects such activities[37]. The employer's duty does not end here and he must also provide the SAPS with all the information necessary relating to the crime. Should the employer fail in his duty as prescribed by the Act this a criminal offence perpetrated by the employer.

It should also be noted that inadvertent access to child pornography is simply not enough to be regarded as criminal possession of child pornography[38]. Access maybe accidental in which case the conduct is not actionable[39]. In determining if the pornography was accessed accidentally the employer will have to take into account the context in which the site or material was accessed[40].

An employer must therefore be aware of what his employees are viewing via the workplace internet facilities and information technology resources at all times as he may find himself criminally liable when employees access, possess or even attempt to possess child pornography which he does not report. This may result in drastic and long lasting effects on the employer personally and on his business as it attaches the stigma of a criminal activity.

2.2 Civil Liability

The threat of criminal charges however are not the only liability faced by the employer when his employees do not tow the line in terms of internet usage. The employer is also threatened by civil liability which may mean the employer can be embroiled in long drawn out civil proceedings which distract him from his business and drain financial resources.

[36] Ibid.
[37] S24 Film and Publications Board Act.
[38] N Whitear-Nel (note 31 above) 789.
[39] Ibid.
[40] Ibid.

Civil liability will be applicable in cases of child pornography. This would be an additional form of liability to criminal action as found in Films and Publications Board Act. The implication of this is that the employer may face both the criminal and civil sanction for child pornography in the workplace if he fails to act against it. The basis of this is the principle of the best interest of the child which requires that the best interest of the child should be paramount as given in the constitution[41].

In South African law we have the law of delict which will be used as a basis for liability but the issue with relying on delictual readdress is that in this specific topic no case law exists to illustrate how it will be dealt with by the courts however an American case may be used to shed some light on the issue. The case of *Jane Doe v XYZ Corporation*[42] concerned a 10 year girl whose pictured had been used to gain access to a child pornographic website by her step-father. The mother of the girl had sued the employer of defendant as she had claimed that uploading such a picture harmed her daughter. The ruling of the court held that in circumstances as those in this case and employer who is aware that employees are using work internet and computers to access child pornography has an active duty to investigate and take action to stop the harmful conduct. Should the employer fail to do so then parties who have been harmed can seek recourse against the employer.

Although no clear case law id present it would be probable that should a case bearing resemblance to Jane's case occur in South Africa our courts are most likely in light of the best interest of child principle, delictual principles and the Film and Publications Board Act to come to the same findings and hold the employer liable civilly for the activity of his employees relating to child pornography.

2.2.1 *Vicarious Liability (Common Law)*

In general the rules relating to civil liability are that when a delict is committed the perpetrator of the delict is personally liable for their wrongful conduct[43]. The common law doctrine of vicarious liability however holds contrary to this general rule. This doctrine recognises that another party may be held liable for the delict of the perpetrating party which has caused loss a third party[44]. This is a form of strict liability and is described as liability

[41] Constitution of the Republic of South Africa 1996 s28.
[42] 382 N.J.Super. 122 (Appellate Division N.J., December 27, 2005).
[43] JS Van Jaarsveld & PBS Van Eck *Principles of Labour Law* 2 (2002) 86.
[44] ME Manemela 'Vicarious liability: Paying for the sins of others' (2004) 16 *SA Merc LJ* 125.

without fault, as the party who is liable is not the party who has perpetrated the delict[45]. The consequence of this doctrine in our law is that employers may now be held liable for the delicts of their employees provided the requirements for vicarious liability are met. This having the implication that any delict committed during an employee's online usage may result in the employer having to bear the liability. The rationale behind use of this doctrine in the workplace is to ensure that employers take steps to ensure that their employee's conduct do not harm or loss to others[46].

In order for an employer to be vicariously liable there must be three requirements that must be met. First, an employer, employee relationship must exist at the time the delict is committed[47]. Second, the delict must have been committed by the employee who causes loss or harm to a third party and third the employee must have acted in the course and scope of his employment[48]. The difficulty with vicariously liability has often been proving that the delict was committed in the course or scope of the employee's employment. However this requirement has been somewhat cleared by the case of *Grobler v Naspers Bpk*[49]. The court held that an employer may still be held liable for a delict even if the conduct that was perpetrated by the employee was not authorised by him. The court's reasoning behind this is that the employment relationship created or enhanced the risk that sexual harassment might occur and this meant that the employer could be vicariously liable for sexual harassment because it was deemed to be in the course of the employee's employment. This has a great significance for employers who face potential liability for their employee's online habits as this prevents them from avoiding liability by claiming that they did not authorise the inappropriate or prohibited activities of their employees when using the internet and therefore the employees were acting outside the scope of their employment. It is noteworthy that the employer is not solely liable for the loss as the employer and the employee become joint and severally liable for the delict[50]. Even though it remains open for the third party to go against the employee who committed the delict, it is more likely that the third party will proceed

[45] J Neethling, JM Visser & PJ Potgieter *The law of delict* 4 (2002) 86
[46] *NK v Minister of Safety and Security* 2005 (6) SA 4 9 para 21.
[47] ME Manemela (note 44 above) 126.
[48] Ibid.
[49] 2001 (4) SA 938 (LC) para 50
[50] ME Manemela (note 44 above) 126.

against the employer because the employer has more financial resources than the employee would[51].

Vicarious liability maybe used as a basis for liability against the employer for various types of employee conduct the most common but not limited regarding internet abuse by employees are harassment, defamation and copyright infringement.

2.2.1 *Harassment*

An employer maybe vicariously liable for sexual harassment perpetrated by any of his employees towards another employee using the internet as a means to perpetrate the harassment[52]. The Code of Good Practice on the Handling of Sexual Harassment Cases[53] broadly defines what constitutes sexual harassment item 4 defines sexual harassment as conduct that is physical, verbal or non-verbal. Relating to internet abuse and use of computers it is the non-verbal type of harassment that is most likely to occur and the employer to be held liable for. Item 4(1)(c) defines non-verbal forms of sexual harassment as conduct that includes unwelcome gestures, indecent exposure, and the unwelcome display of sexually explicit pictures and objects[54]. This means that an employee who displays inappropriate pictures, videos or pornographic material on a computer screen or the sending out emails of a sexual nature maybe deemed to contravene this and the employer can be vicariously liable.

The case of *Bramford v Energiser (SA) Ltd*[55] was a case in which employees circulated pornographic and sexual offensive material using the companies e-mailing system[56]. The arbitrator stated that the employee's actions were not socially acceptable and that the jokes and material sent between the employees where so offensive that they also held a racial connotation which one should seek to avoid in the new South African society[57]. The arbitrator further stated that although employees may enjoy this in private in workplace such practices should not be condoned[58]. The reason for such remarks is that an employer can be found vicariously liable for direct harassment, indirect harassment and even any behaviour

[51] Ibid.
[52] N Whitear-Nel & D Subramanien (note 28 above) 15
[53] GG 19049 of July 1998.
[54] Code of Good Practice on the Handling of Sexual Harassment Cases
[55] 2000 12 BALR 1251 (P)
[56] Supra para 4
[57] Supra para 20
[58] Supra 46

that creates an unproductive, uncomfortable working environment[59]. An example of how sexual harassment can be perpetrated by employees using the internet is also illustrated in the case of *Smuts v Backup Storage Facilities & Others* where a manger viewed pornographic material on a company provided computer during work hours[60].

An example of this type of behaviour is illustrated in the English case of *Morse v Future Reality Ltd*[61] where a female employee shared an office with male co-workers who viewed explicit images of a sexual nature and often circulated the images via email to other colleagues and spoke about these images. She was not directly in contact with these images but the court conduct of downloading sexual content created a hostile working environment. Another case which illustrates vicarious liability for sexual harassment is the case of *Knox v State Department of Indiana*[62] an American where the department of corrections was held vicariously liable for the conduct of an employee who sent out emails asking for sexual intercourse from junior employees. These cases do not represent a South African law perspective and therefore extend beyond of the scope of this dissertation but simply serve to illustrate the manner in which harassment can occur through computer and internet faculties in the workplace and to further depict that this issue in the workplace is not isolated to only South Africa

Sexual harassment is not the only type of harassment that an employer may be vicariously liable for, it is also possible that harassment of a racist nature may result in liability. An example of racist material being circulated via the internet at work can be found in the case of *Cronje v Toyota Manufacturing*[63] in which the Commissioner held that a picture of a gorilla bearing Zimbabwean Presidents Robert Mugabe's head on the gorillas body circulated in the company's internal e-mail system was a crude, offensive, racist stereotype, developed over centuries by white people that associates black people with primates who hold a lower level of intelligence and morality[64].

The way in which racial harassment can also be perpetrated online was shown in the facts of the case of *Dauth and Brown & Weirs Cash & Carry*[65] where an employee sent an e-mail

[59] V Etsebeth 'The growing expansion of vicarious liability in the information age (part 2)' (2006) 4 *TSAR* 760.
[60] [2003] 2 BALR 219 CCMA para 6.
[61] ET case number 54571/95.
[62] 93 F 3d 1327.
[63] 2001 3 BALR 213 (CCMA).
[64] Supra para 43
[65] (2002) 23 ILJ 272 (CCMA).

containing derogatory anti-Semitic comments to Jewish staff members. The American case of *Owens & Hutton v Morgan Stanley & Co Inc*[66] illustrated that an employer can be held vicariously liable for racial harassment. In this case racially derogatory jokes where electronically circulated which resulted in a discrimination claim against the employer of the offending employees. The above two case also do not form part of South African labour law but are included to illustrate factual examples of racial harassment using internet faculties.

2.2.2 *Copyright Infringement*

Copyright infringement is another a delict which an employer may find that he is liable for even though the breach was perpetrated by his employees and not him personally. The internet is a place which allows its users to access a wide range of resources ranging from books, music, movies pictures and other types of media. Many of these works however are protected by copyright laws and users cannot freely distribute and use them without breaching copyright laws. Copyright is protected by the Copyright Act No 98 of 1978. This act not only protects works in the real world but also exists to protect works on the internet[67].

Copyright protects the ideas of the protected work and not the form in which the idea is expressed[68]. For the employer to be vicariously liable the person claiming that they hold copyright rights in the work must prove that they actually do hold a copyright over the work and this will be done by showing the following:

a) The work is original[69].
b) The work falls into the definitions of works covered by the ambit of the act[70].
c) If the work takes the form of a broadcast or a program carrying signal the work must be reduced to some material form to be protected[71].
d) A copy right must exist over the work because of the authors domicile, nationality or residence[72].
e) The term of the copyright is still operative and has not expired[73].

[66] United States District Courts Southern District of New York 96 CIV 9747 (1996).
[67] V Etsebeth (note 59 above) 761.
[68] R Buys *Cyberlaw@SA: the law of the Internet in South Africa* (2000) 3.
[69] S2(1) Copyright Act.
[70] S2(1) and s1(1) Copyright Act.
[71] S2(2) Copyright Act.
[72] S3,S4 and S37 Copyright Act.
[73] S3(2) Copyright Act.

f) A sufficient degree of similarity exists between the work that is copyrighted and the alleged infringed work[74].

The implication of the Act is that once an employee infringes a copyright the holder of the copyright may then choose to hold the employer vicariously liable for the infringement.

2.2.3 *Defamation*

Defamation may be another delict which the employer may be liable for. Defamation is defined as the 'unlawful intentional, publication of defamatory matter referring to the plaintiff who causes his or her reputation to be impaired'[75]. An employer may therefore be liable in the circumstances where an employee posts defamatory matter online or circulates emails regarding defamatory matter about another party. The problem that often arises with cases of defamation and the internet is the requirement and publication of the defamatory matter and considering if it is satisfied[76]. Publication on the internet takes place when the defamatory matter is received, heard or seen by another party who understands the defamatory nature of the content and either originates or is passed on by the employee[77]. The employer can also find himself liable as a publisher or disseminator of defamatory matter where he has provided the offending employee with the tools or equipment to access the internet where the defamatory matter was shared[78]. This will mean that the employer will now be directly liable as he will be deemed to be a publisher of the defamatory matter because of his ownership over the tools used to perpetrate the defamation[79].

2.2.2 *Statutory Liability*

2.2.2.1 *Employment Equity Act 55 of 1998*

The Employment Equity Acts main objective is to regulate the relationship between employers and employees that relate to either discrimination or affirmative action measures within the working environment[80].Section 5[81] of the Act states that an employer must take positive steps to eradicate all forms of discrimination in the workplace and that employers

[74] *Galago Publishers (Pty) Ltd v Erasmus* 1989 1 SA 276 (A)
[75] J Burchell *The law of defamation in South Africa* (1985) 35.
[76] M Van Jaarsveld 'Forearmed is forewarned: Some thoughts on the inappropriate use of computers in the workplace.' (2004) 16 SA *Merc LJ* 663.
[77] V Etsebeth (note 59 above) 756.
[78] Ibid 757.
[79] *CWU v Mobile Telephone Networks (Pty) (Ltd)* 2003 8 BLLR 741 (LC).
[80] Employment Equity Act.
[81] Employment Equity Act.

who do not adhere to this will be liable for damages. The following are the types of discrimination that steps should be taken to eliminate race, gender, sex, pregnancy, marital status, family responsibility, ethnic or social origin, colour, sexual orientation, age, disability, religion, HIV status, conscience, belief, political opinion, culture, language, birth or on any other arbitrary ground . Therefore an employer can acquire statutory liability based on s5 where his employees use internet facilities to encourage or comitt acts of discriminatory behaviour against other employees. This can be done by using of the employers internal e-mail facilities, social media and display of inappropriate material on company electronic devices such as tablets and laptops to disseminate discriminatory material.

However this is not strict liability and an employer may avoid liability in certain circumstances. This is provided for in various provisions of the act that provide the employer with steps he make take to avoid liability. Section 60(2)[82] provides that in circumstances where there is discriminatory conduct the employer must consult with all relevant parties and must take the necessary steps to eliminate that conduct and comply with the provisions of the Act. This provision provides the employer with the opportunity to address the discriminatory conduct by doing so he will have escaped liability[83]. What is deemed to be necessary steps taken by the employer must be judged against the existing policies for such conduct in the workplace[84]. If an employer fails to adhere to s60(2) and does not take the necessary steps and it has also been proved that the employee has committed some kind of discriminatory conduct then the employer to must be deemed to have contravened the act .if the employee has been found to have contravened the act by committing discriminatory using the internet at work and the employee knowing of such conduct fails to take steps to eliminate the conduct liability can be attributed to the employer for those acts[85] .

It is possible however for an employer to avoid liability without even having to take necessary steps as required in s60 (2) and s60 (3). Section 60(4)[86] states that an employee is not liable for discriminatory conduct of an employee if the employer is able to prove that, he has done all that was reasonably practicable to ensure that employees do not comitt acts of discrimination. Where an employee has then used the internet to comitt acts of discrimination an employee will not be liable if he has taken reasonable steps eliminate that conduct. This

[82] Ibid.
[83] A Mukhebeir & L Ristow 'An Overview of sexual harassment: Liability of the employer' (2006) *Obiter* 259.
[84] Ibid.
[85] Ibid.
[86] Employment Equity Act.

could take places in many ways such as an internet usage policy condemning such conduct or monitoring internet use in the workplace. This will therefore allow the employer to avoid liability completely.

2.2.2.2 *Electronic Communications and Transactions Act 25 of 2005 (ECTA)*

The aim of ECTA is to facilitate and enable electronic transactions in a manner that creates a sense of confidence and legal certainty in any kind of electronic transaction and communication. One of the benefits ECTA is that it allows contracts to be formed and entered online without parties ever having to meet face to face. This may be trouble for employers as it allows employees to form contracts in the company name online without the employer even having knowledge of such a transaction. This is specifically mentioned in s22[87] states that no agreement shall be without legal force based solely on the fact that it is in the form of data messages. However it should be noted that the common law requirements for a valid contract must also still be present[88]. With online contracts what was difficult to determine was the time and place which an online contract is concluded as these issues will often arise when considering validity of online contracts. According to Chapter 3 of ECTA an online contract comes into force and the time and place of acceptance of the offer by the offeree of the contract. Section 23(1)[89] in these circumstances the Act provides that an offer will be considered as received when the complete data messages have been received in the information system of the offeree and the offeree can retrieve such data messages.

This means that an employee may conclude a contract simply by means of text message or email which will bind the employer to perform under that contract. It is therefore then possible that the recipient of data messages from an employee may have a valid and enforceable contract if they have reasonable grounds for believing that the employee concluding the contract has authority to do so, the common law contractual elements are met and accepts the terms contained in the data messages[90]. This having the consequence that an employer may be bound to contracts he does not want to render performance to.

2.2.2.3 *Occupational Health and Safety Act85 of 1993(OHSA)*

[87] Electronic Communications and Transactions Act
[88] V Ethsebeth (note 59 above) 763.
[89] Electronic Communications and Transactions Act
[90] Electronic Communications and Transactions Act

The aim of this Act is to ensure that a safe and healthy working environment is created for all employees and this applies equally to both physical and psychological well-being. This means an employer has a legal duty to employee to create such an environment[91]. An employer who fails to take steps to ensure a safe and healthy work environment is then deemed to be contravention of this Act. Any type of act that results from internet usage in the workplace that creates a workplace that is psychologically damaging to employees and hostile will require the employer to take steps or be liable for such acts of his offending employees. Section 38 states that where an employer fails in his duties as accorded by the Act such an employer may face a fine not exceeding R100 000 and even up to two years imprisonment[92].

2.2.2.4 *Compensation for Occupational Injuries and Diseases Act 130 of 1993 (COIDA)*

COIDA is a compensation scheme for employees who suffer injuries and diseases as a result for their occupations. Section 5 provides that an employee is eligible for compensation for an injuries sustained that are work related, this will be the position even if the injury is of no fault of the employer because for an employee to successfully rely on this section all that needs to be shown is a casual connection between the injury sustained by the employee and the employee's employment[93]. Employees have in the past been successful in claiming psychological injury in the form of post-traumatic stress disorder as injury and receiving compensation however these cases did not involve any element of internet use[94]. This means it is open to an employee who has suffered psychological injuries as a result of material they have been exposed to or received on the employer's internal system or explicit displayed on a computer screen to claim compensation from the employer in terms of s50 if as a result they suffer psychological injury.

Despite the potential legal liability employers face when employees misuse internet facilities this should not spell the end of computers in the workplace as much of the misuse can be eradicated by meaningful regulation of internet usage by employees.

3. MEASURES EMPLOYERS CAN ADOPT TO MINIMISE THE RISK OF INTERNET MISUSE

[91] s8(1) Occupational Health and Safety Act.
[92] Occupational Health and Safety Act.
[93] Compensation for Occupational Injuries and Diseases Act
[94] *Urquhart v Compensation Commissioner* (2006) 27 ILJ 96 (E)

3.1 *Monitoring and Interception in terms of the Regulation of Interception of Communications and Provision of Communicated-related Information Act 70 of 2002.*

One of the most effective and modern approach to discourage employees from misusing the internet is to employ the provisions that permit monitoring of internet facilities that are set in to place in terms of the Regulation of Interception of Communications and Provision of Communicated-related Information Act 70 of 2002 (RIC Act). This Act allows that in special circumstances an employer is allowed to monitor the internet usage of his employees. However these instances are exceptions to the main purpose of the Act which are expressly mentioned in s1[95]. Section 1 of the Act states that the main objective of the RIC Act is to prohibit the intentional interception of any communication.

Intercept is defined as meaning the aural or any other acquisition of the contents of any communication by any method including an interception device so that some other party beside the sender recipient or intended recipient of that communication has access to the contents of the communication[96]. The definition of interception includes monitoring of communication through a monitoring device, viewing, examination or inspection of the contents of any direct or indirect communication as well as any diversion of communications from the intended sender to any other destination[97]. Inception in terms of the Ric Act therefore has a corresponding meaning to intercept[98]. Monitoring is not dealt with separately under the Act but is included as a facet of interception process[99].

Indirect communication is protected by the RIC Act. This has an important bearing on employers as the definition of such communication is the transfer of information weather done through messages, data, text, speech, sound, music, signals, radio frequency spectrum, visual images or any combination of these types of communications[100]. A consequence of the RIC Act covering indirect communications means that employers now have the authority to intercept emails and browsing activities of employers because of the wide scope which

[95] Regulation of Interception of Communications and Provision of Communicated-related Information Act
[96] S1 Regulation of Interception of Communications and Provision of Communicated-related Information Act .
[97] Ibid.
[98] Ibid.
[99] V Lawack-Davids & A van der Walt 'The interception of electronic communications in the workplace' (2005) *Obiter* 134.
[100] S1 Regulation of Interception of Communications and Provision of Communicated-related Information Act

indirect communications span[101]. However in light of the main objective of the Act situations in which employers may use interception is limited.

In accordance with this aim there is a general prohibition on interception. In terms of this prohibition no person may intentionally or attempt to intercept, authorise or procure another to intercept any communication either in its occurrence or transmission[102]. Despite this general prohibition interception in the workplace is permitted in the Act by three exceptions to this prohibition. This having the effect an employer can intercept any internet messaging whether email or other and any websites visited by his employees if the employer finds himself in any of these three exceptions.

Firstly, s4 (1)[103] permits a party to the communication to intercept it. The RIC Act however fails to provide a meaning for the term party and its ordinary meaning would have to prevail[104]. Therefore either the sender of the recipient or any recipient to whom the communication is duplicated to can intercept the communication without having contravened the Act[105]. The employer can therefore rely on this section for authority of interception if he was a party to the communication or he was forwarded such communication by someone who was a party to the communication itself.

Secondly, consent is sufficient to lift the prohibition on interception. This is because s5 (1)[106] provides that one can intercept and even record communication if one of the parties to the communication has provided prior written consent to intercept. An employer can in terms of s5 (1) intercept his employees communications if firstly, consent was obtained prior to the interception having taken place. If no consent has been obtained prior to the interception it may still be possible for an employee to ratify such interception, if such ratification does occur then objection or defence to interception by the employee will no longer be tenable[107]. Secondly an employer can only rely on this section to intercept if the consent provide by the employee was done in writing. It may be possible for an employer to secure such consent in the contract of employment or other policies provided that such consent is given voluntarily

[101] V Lawack-Davids & A van der Walt (note 97 above) 134.
[102] S2 Regulation of Interception of Communications and Provision of Communicated-related Information Act
[103] Regulation of Interception of Communications and Provision of Communicated-related Information Act
[104] W Beech ' The right of an employer to monitor an employee's electronic mail, telephone calls, internet usage and other recordings' (2005) 26 *ILJ* 656.
[105] Ibid.
[106] Regulation of Interception of Communications and Provision of Communicated-related Information Act
[107] W Beech (note 102 above) 656.

by the employee and such employee is aware of the scope such consent as general consent will be unenforceable[108].

If these two requirements are not adhered to no employer can validly use s5 (1) as a basis for interception. Employees who have not provided written consent prior to interception may still have their communications intercepted. This may occur in the situation where the communication involved is multi-party and one of the parties to this communication has provided the employer with prior written consent[109]. Such interception is possible because s5 (1) provides that interception is possible if one of the parties to the communication gives prior written consent.

Thirdly s6 (1)[110] permits an employer to intercept any indirect communication in the course of carrying on business. If business use is therefore the justification for interception it can be done, provided that certain requirements are met in accordance with the act. These requirements are technical and requires that the purpose of the interception must be establish if there has been unauthorised use of the system and to establish the existence of particular facts[111]. Although not expressly mentioned these purposes may include establishing if offensive and unauthorised sites have been visited, establishing if the internet has been used for unauthorised purposes and to protect the employers systems by exposing any risks and illegitimate use of the system[112]. Unlike s5(1) no prior written consent is required from the employees all that is needed to permit an employer to intercept communication is that s6(2)(d)[113] requires that all reasonable efforts must be made to make employees aware that their communications maybe intercepted . This having the effect that if interception is for business use then an employee need not give prior written consent for his communications to be intercepted or consent at all. This has been a point which has been met with much debate because of the implications that such a lack of consent has on the constitutional right to privacy of the employees and weather employers in light of the Act can simply just disregard this.

[108] Ibid.
[109] V Lawack-Davids & A van der Walt (note 97 above)135
[110] Regulation of Interception of Communications and Provision of Communicated-related Information Act
[111] S6(1) Regulation of Interception of Communications and Provision of Communicated-related Information Act
[112] N Whitear-Nel & D Subramanien (note 28 above) 18.
[113] Regulation of Interception of Communications and Provision of Communicated-related Information Act

Much uncertainty surround these provisions of the RIC Act and exactly how it is to be adopted and carried in the workplace remains to be seen as there are presently no binding decisions concerning the application of the Act in the context of employment regarding the exceptions to s2.

3.1.1 *Employers duty to protect employee's constitutional rights during interception.*

Interception and monitoring of employees browsing activity and e-mail accounts may seem like drastic step taken by the employer in light of employee's constitutional right to privacy. The concern of privacy infringement is heightened when employees start to store personal information on their work equipment such as computers, laptops and tablets. This very often leads to the question how far can employers go when intercepting employee's internet activities without violating their constitutional rights.

S14 of the Constitution guarantees the right to privacy to everyone and makes provision that the right to privacy is extended to protect against infringement of ones communications[114]. This is right offers employees a defence against having any of their communications intercepted or monitored. This is where employers begin to find themselves in a compromising situation. This is because of the competing interests involved. On one side there is the employer who is concerned with protecting himself against the consequences caused by such misuse and on the other the employees who have an expectation of privacy in their communications in the workplace[115]. The employer however finds himself carrying the much heavier burden as the case of *Ekhamanzi Springs (Pty) Ltd v Mnomiya*[116] held that where employers are aware that employees constitutional rights are being infringed they have a positive duty to step in and come to the assistance of exploited employees[117].

The right to privacy is operative and protected in the workplace as s8 (3) of the Constitution provides that rights are also to be protected vertically[118]. This having the implication that constitutional rights should be protected even between private parties and not just the state. This section allows for the right of privacy to be invoked in the workplace between both the employer and the employee. Support for this right being extended to the workplace is found in the case of In *Re Hyundai Motors Distibutors (Pty) Ltd and Others v Smith and NO and*

[114] 1996 Consititution.
[115] V Lawack-Davids & A van der Walt (note 97 above 133.
[116] (DA2/13) [2014] ZALCD 17.
[117] Supra para 29.
[118] 1996 Constitution.

Others[119] where the Constitutional Court recognised that privacy extends beyond a person's "intimate core" and extends to the workplace of the employee[120]. However the court acknowledged that once one enters into a public space the right of privacy decreases. The constitutional court in *Bernstein V Bester NO*[121] stated that privacy in the workplace is an 'amphorus and elusive concept'[122]. The Constitutional court further went on to hold that although there is a higher expectation of privacy in one's personal space and affairs once one moves away from this and into more communal and public activities such as business and social interactions the scope and expectation of this right diminishes[123]. Despite the diminishing of the right to privacy it does not mean that employee has no expectation of privacy, such a right does still exist but only much less than in the employees private life. These cases have the effect that an employer may intercept or monitor an employee's internet usage as their expectation of privacy is decreased once they enter the working place. However employers must not go too far and open this up to abuse where they begin to use inception for purposes other than those permitted by the Act.

Although the right to privacy is guaranteed in the constitution it is not absolute and its application can be limited according to s36 of the Constitution known as the limitations clause[124]. Therefore it is open to the employer to argue that an infringement of employee's right to privacy is justifiable under s36 but only once the harm of such a limitation will cause has been taken into account[125]. In addition to this it will be necessary that the extent of an employee's right to privacy in the workplace be balanced against competing rights of the employer[126]. Such interests would be the employer's rights to protect his legitimate business interests and society's needs to rid itself of unlawful conduct[127].

South African law has very little case law relating to the issue specifically of email and internet monitoring and the right to privacy. However there have been decided cases relating to telephone tapping and the right to privacy in the workplace. These cases may provide a basis to how courts may interpret the right when relating to internet communications and a

[119] 2001(1) SA 545 (CC).
[120] Supra para 87
[121] 1996 (2) SA 751 (CC).
[122] Supra para 67.
[123] Supra para 77.
[124] 1996 Constitution.
[125] BPS van Eck 'Misuse of the internet at the workplace' (2001) 46 *De Jure* 365.
[126] C E Frayer 'Employee Privacy and internet monitoring: Balancing workers rights to dignity with legitimate management interests' (2002) 57 *Business Lawyer*.
[127] N Whitear-Nel & D Subramanien (note 28 above) 16.

guideline for other courts to base their findings upon. These arguments can often be used to justify when an employer can cross the bounds of an employee's privacy.

The first case that considered this issue was the case of *Goosen v Carolines Frozen Yoghurt Parlour (Pty[128]) Ltd and another* and was decided under the interim constitution. This case dealt with an employer who relied on transcripts of telephone conversations without the consent of his employer in his disciplinary procedure to prove that he had not had a fair hearing and the chairperson was biased[129]. Although the main issue in the case was admissibility of evidence the court considered the right to privacy in s13 and the limitation clause s33 under the Interim Constitution. The court in *Goosen* took a similar approach to the right to privacy as in prior decisions and held that although traditionally human rights were thought of as been protection by the citizen for violations of rights by the state. This being the vertical protection of rights[130]. A horizontal application can be invoked to protect individuals and their relationships with one another. Therefore the court accepted that in certain instances it is appropriate for the Bill of Rights including the right to privacy to apply horizontally between private parties such as the employment relationship[131]. The bearing this then had was that it was now established that employee's right to privacy extends to the workplace and not just interactions with the state.

The case of *Protea Technology Ltd and another v Wainer and others[132]* was decided under the final Constitution and this case delved more into the issue of privacy in the workplace than *Goosen*. In this case the employer had without the consent of the employee recoded his telephonic conversations to prove that the employee was acting in breach of his restraint of trade agreement. *Wainer* the employee argued that the recording of his telephonic conversations were an infringement of his right to privacy. The court in determining whether the employer's actions constituted a violation of *Wainers* right to privacy found that the scope of a person's privacy extends only to where there is a legitimate expectation of privacy. The test for this legitimate expectation is whether there is a subjective expectation of privacy which society recognises as objectively reasonable[133]. The court went further in defining the bounds of this right and held that in the employment context it is acceptable for an employee

[128] 36 (1995) 16 ILJ 396 (IC).
[129] Supra para 399.
[130] Supra para 402.
[131] Supra.
[132] (1997) 9 BCLR 1225 (W).
[133] Para 543.

to make or receive calls that are unrelated to the employers business or the employer's interests. It is in these types of calls that an employee with have a legitimate expectation of privacy[134]. However when these calls are related to the employers affairs, the employer is entitled to have access to the content of such communications. the court stated that this expectation of privacy exists only when the communications are personal and private and not connected to the employers business and once an employee abandons his private matters and moves into communications connected to the employers affairs he can no longer has the benefit of using the right to privacy to guard such communications. The court held that where the calls related to the employers business, the employer has the right to know both the substance and manner which the employee is conducting himself[135].

If the approach for privacy as set down in the *Wainer* case is to stand in regards to the right of privacy between employer and employer there seems to be two factors that need to be present. Firstly the employee must have formed a subjective expectation of privacy in the employment relationships. Secondly society must recognise that such an expectation is reasonable.

The next case which the CCMA had an opportunity of interpreting the right to privacy was in the case of *Moonsamy v Mailhouse* . *Moonsamy*[136] the employer argued that the interception of his telephone calls was contrary to his constitutional right to privacy. The CCMA interpreted this right in much more detail than previous cases. The arbitrator had found that the issue underlying this case was the competing interests of both parties. The arbitrator accordingly held that the recording of *Moonsamy* conversations where indeed a violation of right to privacy as protected in the constitution. The arbitrator however did not stop his findings there and went on to consider if such an infringement was justifiable according s36 of the constitution the limitation clause. The arbitrator then structured this around the five premises that need to be present for a limitation of a constitutional right to be successful. These premises where decided as:

a) The nature of the right- the Canadian Charter was relied on to shed light on this premise. The arbitrator in this ground made a finding very similar to that of the judge in the *Wainer* case. He held that an employer has a reasonable expectation of privacy at his employer's premises and that such a reasonable expectation can only exist when

[134] Supra.
[135] Supra.
[136] (1999) 20 ILJ 464 (CCMA).

the employer has a subjective expectation of privacy that society recognises as reasonable. The arbitrator acknowledged that it is very difficult to precisely formulate the extent to which an employee's privacy can be protected on the employer's premises[137].

b) The importance of the purpose of the right- it was recognised that employees do have rights within the workplace. However the arbitrator cautions that the employer's right to economic activity is no longer as guaranteed in the final constitution as it was in the interim constitution. As a result of this he believes that an employee's personal rights should take precedent over the employer's right to economic activity[138].
c) The nature and extend of the limitation- the arbitrator held that while it may be acceptable for an employer to monitor the extend of the activity, this is where the employers monitoring should end. The employer should not consider the content of the employee's communications unless the employee has given consent or that disclosure is necessary for business reasons[139].
d) The relation between the limitation and the purpose- the arbitrator held that the method of obtaining the information by telephone tapping was invasive. It was further held that this method would only be acceptable if it was the only method that could be used to secure the information[140].
e) Less restrictive means to achieve the purpose- it was held that if the employer could have used other methods of obtaining the information from the telephone calls he should have done so. The arbitrator went on to hold that if telephone tapping was the only way then consent of the employee should have been sought[141].

Although the *Moonsamy* case is not binding law and is only a finding of the CCMA it provides a logical and fair opportunity to see how courts are most likely to interpret the right to privacy when dealing with internet misuse. However if this will be the situation remains to be seen as we have to date not had any cases specifically addressing this.

Apart from the constitutional rights that are threatened when an employer adopts interception and monitoring as a means to stop internet abuse there further effects both positive and negative that monitoring and interception may result in. Even though these are not legal

[137] Para 66
[138] Supra
[139] Supra 67
[140] Supra .
[141] Supra 68.

considerations they provide an insight that they may assist in solving legal issues relating to employee misuse of internet facilities. The legal aspects of regulation can also not be looked at in isolation without considering the social elements as there is a clear link which shows that monitoring extensively negatively impacts employee morale.

3.1.2 *Effects of monitoring and interception in the workplace*

Monitoring and interception in the workplace may seem like and easy and effective way for an employer to tackle the problems of internet misuse in the work environment but employers should be cautious about the potential effects such monitoring may ultimately result in. An employer may through monitoring successfully decrease internet misuse but research has shown that productivity levels decrease when employees are constantly surveilled[142]. This may be of concern to the employer as employees who work in environments where there are high levels of monitoring and surveillance are found to be more stressed[143]. Productivity is also further lessened as constant monitoring discourages employers from using the internet[144]. This is counterproductive as the internet and computers are often essential tools in an employee completing tasks efficiently and competently. Not only is performance affected by monitoring but heavy monitoring in the workplace also disintegrates the relationship between the employer and the employee[145]. The consequence of this being that the relationship of mutual trust starts to breakdown and the unequal power of the parties come to the forefront[146]. Employees being monitored perceive such monitoring as the employee having low expectations of them and simply work to fulfil these low expectations rather than working above and beyond such expectations[147]. Employees in these circumstances also find the need to supress their creativity and ingenuity which discourages both employee and organisational growth as employees feel threatened to conform to the employer's norm[148].

[142] C Ciochetti (note 13 above)357.
[143] DM Nebeker & BC Tatum 'The effects of computer monitoring, standards and rewards on work performance, job satisfaction and stress. (1993) 23(7) *Journal of Applied Psychology* 508.
[144] C Stafford & M Mearns 'What happens when employees embrace social networking' (2009) 11(4) *South African Journal of Information Management.*
[145] J R Aiello 'Computer based monitoring: Electronic surveillance and its effects' (1993) 23(7) *Journal of Applied Social Psychology* 499.
[146] Ibid.
[147] J Chalykoff & T A Kochran 'Computer-aided monitoring: Its influence on employee satisfaction and turnover' (1989) 40 *Personnel Psychology* 807.
[148] T J Hodson, F Englander & V Englander 'Ethical, legal and economic aspects of employer monitoring of employee electronic mail' (1999) 19(1) *Journal of Business Ethics* 99.

However the employer should not only look to the negatives of internet usage in the workplace but must also consider the benefits it has in the work environment for the employer and employees. Internet, e-mail and social networking can boost employee morale and lead to a happier and productive workplace. Employees are now found to be working much longer hours and harder than in the past this seems to muddy the waters between work and personal time. This often results in the employee needing some lenience when it comes to using the internet for personal reasons[149]. This approach been referred to as accommodating the 'workplace dynamic'[150]. Employees who accorded such lenience are found to leave their workstations less and they do not have to leave work to attend to personal matters[151]. This ultimately will benefit the employer and his business.

The best approach for an employer to adopt is a medium between monitoring and giving employees the flexibility to use the internet for personal reasons. This will lead to a healthy workplace and good relationships between the employer and the employer which is inevitable for the employer to have to have a successful business operations.

3.2 *Other methods to minimise risks of internet misuse*

Interception and monitoring are not the avenues available to an employer to reduce internet abuse in the workplace although they are the most common various other methods remain open to the employer to adopt. An employer could install web page content checking software in to the systems[152]. An employer can also invest in content monitoring software[153]. The problems with utilising these methods are that they are expensive to install and will require sophisticated in-house technical support to operate[154]. This is therefore not practical for all businesses. Training of staff to reduce the risk of unauthorised use is another option which is both cost efficient and effective[155]. An employer can also use an internet usage policy to minimise risks.

4. EMPLOYERS RECOURSE AGAINST OFFENDING EMPLOYEES

[149] C Ciochetti (note 13 above) 291.
[150] C P Fazekas '1984 is still Fiction: Electronic monitoring in the workplace and US privacy law' (2004) 15 *Duke Law and Technology Review* 5.
[151] M S Horung 'Think before you type: A look at e-mail privacy in the workplace' (2005) 11 *Fordham Journal of Corporate and Financial Law* 124.
[152] V Ethsebeth (note 59 above) 762.
[153] Ibid 764.
[154] M Van Jaarsveld (note 76 above) 651.
[155] V Ethsebeth (note 59 above) 762.

Although an employer may take steps to eradicate internet abuse in the workplace, he may still however be vulnerable to liability despite these steps. In the event that an employer has been exposed to such liability and is now faced with legal action due to his employees conduct online an employer is not left without recourse in the law. This recourse however will be against the employee responsible for the internet misuse himself in his personal capacity.

4.1 *Internet usage policy*

An employer may adopt an internet usage policy in the workplace that is applicable to all employees[156]. This policy will compromise of the rules and standards for use of computers and internet in the workplace[157]. This policy will seek to regulate internet use during working hours. The internet usage policy has many benefits among them are that they have the power to potentially shield the employer from any liability arising out of his employees misuse, it creates certainty as to the purposes for which the internet can acceptably be used, to inform employees about the dangers of unauthorised use of the internet and the penalties for inappropriate online practices[158]. It also serves as a way that an employer can use to minimise risks posed by employees who use internet facilities inappropriately.

4.1.1 *Content of the internet usage policy*

For the policy to be effective and serve its purpose it is recommended policy concern itself with the following issues. The policy should from the very outset as an overarching rule clearly state that use and access to the internet should be used mainly to advance the employers interests and serve the employers functions[159]. It is open to the employer to either completely have a ban on personal use or state that personal use is permitted but reasonably only[160]. It should however be recommended that given the advantages of personal use moderately that employers should consider a complete ban carefully. If private use is permitted by the policy it should not be done without qualification. The employer may do this

[156] J Johnson 'Information Technology Policies' (2001) *De Rebus* 38.
[157] M Van Jaarsveld (note 76 above) 663-664.
[158] Ibid.
[159] M McGregor ''The right to privacy in the workplace: General case law and guidelines for using the internet and e-mail' (2004) (note 2 above) 648
[160] Ibid.

by adding in the policy that private and personal use may only be used if such is for legal purposes, ethical and considers the rights of fellow employees[161].

The internet usage policy should also clearly set out rules regarding email in the workplace. Emails for the employer's business purposes should be given priority[162]. It is recommended that the employer permit use of personal email but this use should be restricted to emails that are related to family responsibility and to some extend of a social nature provided it does not hinder the employers ability to perform his duties. Receiving emails with large attachments should be limited and should only be sent out of peak times as these cause delays and blockages in the employers system[163]. These emails will only be prohibited if they are for work related purposes.

The employer should also create in the internet usage policy limitations on the content of the emails sent. Employees should not use the employers email facilities for either the sending or receiving of any media files such as pictures, music books and other types of communications[164]. An employee should also refrain from sending any email that contains content which contain any communication that is offensive to any person or that the employee suspects will be offensive[165].

Spam also poses a risk towards productivity and due to these provisions relating to spam should also be included in the internet usage policy[166]. A clear a ban on forwarding spam should be created. Employees should also take steps to request that unwelcomed spam that is sent excessively be stopped[167]. This provision would include sending material that is discriminatory, sexually explicit or abusive[168].

Unauthorised downloading should also be addressed in the internet usage policy[169]. The provision on this should provide that no employee may copy, modify, forward or download any work that a copyright subsists over, unless permission for its use has been granted[170].

---

[161] Ibid.
[162] Ibid.
[163] Ibid.
[164] Ibid 649.
[165] Ibid.
[166] G Ebersohn 'The unfair business practises of spamming and spoofing' (2003) *De Rebus* 25.
[167] Ibid.
[168] M McGregor 'The use of internet and e-mail in the workplace' (2004) (note 1 above) 191.
[169] Ibid.
[170] McGregor'' The right to privacy in the workplace: General case law and guidelines for using the internet and e-mail' (2004) (note 2 above) 649.

There should also be a prohibition on the disclosure of any company secrets and confidential information without the consent of the employer[171]. Employees should also be prohibited using the company logo or any trade marks unless the employer authorises this[172].

The internet usage policy must also contain the extent to which the employees may expect privacy of their communications. The internet usage policy should contain the instances when employee's communications maybe monitored or stored[173]. The policy should also consider the privacy of password-protected resources on an employee's computer[174].

However this outcome must be communicated in the policy. There are also other considerations and provisions which the employer may wish to include in his policy as there are no hard and fast rules as to what the policy should include, this is completely left in the discretion of the employer and his interests. Employers should be cautious however as to the kind of limits that they set as adopting a flexible policy will result in employees being more positive and accommodating of such rules, especially if they permit employees with a reasonable amount of freedom in online practices[175].

For the policy to be enforceable in the most effective manner the policy should be annually reviewed to accommodate and adapt the changing needs and advancements of the employers business[176]. The policy must also be brought to attention of employees so that they are aware of the standard they are held[177]. This may be done by having the policy visible on notice boards, common use areas, all staff websites, and on all staff computers when the employer logs on. The policy must also be drawn to the employee's attention on recruitment and training[178]. An employer may also incorporate this in the initial contract of employment this ensures that it form part of the rules and standards the employee agrees to adhere to.

The internet usage policy should however not operate without force and disciplinary measures must be in place for contravention of the policy. This would be the recourse which the employer may have against his employee as contravention of the policy will be deemed to

[171] Ibid.
[172] Ibid.
[173] N Whitear-Nel & D Subramanien (note 28 above) 20.
[174] Ibid.
[175] M Van Jaarsveld (note 76 above)665
[176] M McGregor 'The use of e-mail and internet at work' (2004) (note 1 above) 191.
[177] M McGregor ' The right to privacy in the workplace: General case law and guidelines for using the internet and e-mail' (2004) (note 2 above) 650.
[178] Ibid.

be an act of misconduct and the employee may then face disciplinary action based on the contravention. This may mean that if an employee does not act in accordance with the internet usage policy in force they may ultimately be dismissed due to misconduct. This serves to show that an internet usage policy in the workplace has a twofold purpose. First, is seeks minimise the risk employers may face for liability and second it acts as a means in which an employer may have recourse against an employee who has breached the policy or caused the employer to face liability.

For the employer to rely on the contravention of the policy for a grounds of dismissal it is not enough simply for the employer to have an internet usage policy on its own in place. The policy must also comply with Schedule 8 of the Code of Good Practice on Dismissal[179].

4.1.2 *Schedule 8 of the Code of Good Practice on Dismissal*

The Constitution ins s23(1)[180] states that everyone is entitled to fair labour practices as part of the giving effect to this constitution duty Schedule 8 of the Code of Good Practice serves to protect this right. For the employer to successfully dismiss an employee for breach of the policy the dismissal must be fair. According to schedule 8 a dismissal may only be deemed fair if the dismissal complies with the following guidelines as set out by the Code. These guidelines state that the employee must have contravened some standard of conduct or rule that regulates conduct in the workplace. If it is shown that a rule or standard is contravened then the following must be shown. First, the rule was valid or a reasonable rule[181]. Second, the employee was aware or could have been reasonably expected to be aware of the rule or standard[182]. Third, the rule has been applied consistently by the employer and fourth dismissal is an appropriate sanction for contravention of the rule[183].

It is often with these provisions of the code that employers need to be aware of as they often create difficulty in dismissals even when there has been a clear breach of the policy. This then leaves the employer unable to act on such a breach. The few cases that exist on this topic show exactly this point.

[179] Labour Relations Act No 66 of 1995.
[180] 1996 Constitution.
[181] Item 7(i) Code of Good Practice on Dismissal
[182] Item 7(ii) Code of Good Practice on Dismissal
[183] Item 7(iii) Code of Good Practice on Dismissal

In the case of *Gouws Score v Price and Pride Furnishers*[184] a company had sent out a memorandum prohibiting unauthorised software from being downloaded. This memorandum set out that contravention of this was a dismissible offence. The employer in question was found to be playing games on his computer. He was then asked to remove the software from the game which he did and faced no sanction for his conduct. A few months later the employee was dismissed for viewing pornographic material on a disk at his computer. The company stated it was because he had failed to uphold the memorandum. The employee then challenged his dismissal and was successful. The CCMA found that his dismissal was unfair due to the inconsistent manner in which the employer had dealt with company rules. The reasoning of the commissioner behind this ruling was that the employee should have faced disciplinary action on his first offence of playing games during work hours on his office computer. The employers failure to discipline the employee the first time meant that he could not discipline him the second time for contravening the same rule because of the employers inconsistency in applications of the rule.

Another case in which a dismissal challenged on the grounds of fair was the case of *Bramford & others v Energiser (SA) Limited*[185]. This case dealt with a group of employees who were found to be using the employer's facilities to send emails to each other which contained pornographic material, crude jokes and chain letters which spanned thousands of messages sent between the employees. The applicants were given a disciplinary hearing and were dismissed. The employees challenged their dismissal claiming that it was unfair because there was no clear rule against the sending or receiving of such information, that the employer was consistent in singling them out from other employees and that dismissal was a sanction which was too harsh.

On the first ground that no clear rule existed the arbitrator had found that there were policies in place that prohibited such conduct and that if the employees were not aware of these policies and provisions they had only themselves to blame. The arbitrator found that a clear rule did exist and referred the employees to various documents that employees received relating to the use of office computers. A copy of this was even posted in the copy machine area and the reception of the head office. This document clearly set out that inappropriate use of office computers will be punished by dismissal.in addition to this an email was sent to all employees on the topic of usage of company computers this email clearly stated that any files

[184] [2011] 11 BALR 1155 (CCMA).
[185] Note 55 above.

from external sources are prohibited from being loaded onto any office computers unless they are needed for business use. The email also stated that the employee's computers were business tools and were to be used as office tools.

Regarding the grounds of consistency the arbitrator found that other employees who were allegedly also guilty of inappropriate use of the employers computers had no evidence against them showing their involvement. The argument that the sanction is a too harsh sanction was also not successful as it was held that although dismissal for a first offence is usually not appropriate if the conduct is of a serious gravity that the employment relationship becomes intolerable.

An employer may also dismiss an employee for misuse of internet where the offence was one which had the effect of seriously damaging the employment relationship as held in the case of *Cronje v Toyota Manufacturing*.[186] The court in this instance held that in accordance with the Code of Good Practice dismissal was an appropriate sanction when acts of internet misuse result in the employment relationship becoming intolerable. The court held that an employment relationship becomes intolerable when the trust, mutual confidence and respect cannot be repaired.

The same view was taken in the case of *Dauth and Brown & Weirs Cash & Carry*[187] where an employee was dismissed for anti-Semitic comments made to Jewish shareholders and directors in an e-mail. The Commissioner stated that dismissal was appropriate as the gravity of the conduct of the employee made the employment relationship intolerable. This however is not a South African case and has no bearing on South African law other than to depict the factual scenario.

Dismissal is not the only way in which an employer can deal with an employee who has misused the internet and exposed the employer to liability. The employer also may choose readdress in the form of breach of the employee's duties that are owed to him. This may often be the best and easiest route as it is simpler to prove that the employee has not acted in the employer's interests.

4.2 *Breach of Fiduciary Duties of Good Faith and the Employer Right to Exercise Control*

[186] Note 63 above.
[187] Note 65 above.

Once the employment contract has been concluded a fiduciary relationship exists between the employer and the employee. One of these duties is the duty to act in good faith this duty is accepted as an implied term of the contract of employment[188]. This means that the duty of good faith forms part of the obligations of the employee even if these duties are not expressed set out in the employment contract[189]. This is because the relationship that exists between the employer and the employee is a relationship of mutual trust and confidence[190]. An element of the duty of good faith is also the duty that the employees always act and put the best interests of his employer before his own interests[191].

The employment contract also gives rise to another aspect closely related to the fiduciary duty of good faith and that is the employers right to exercise control of the employees activities during working hours. This principle simply means that by virtue of the employment contract the employee is the subordinate of the employer and is therefore obligated to comply with all lawful commands of the employer[192]. This has often been referred to as the employers right to expect that employees will act in a subordinate capacity[193].

The implications of the right to exercise control and the employees duty of good faith is that once and employee is found to have abused the employers internet facilities during working hours he is immediately in breach of his duty of good faith as he acts in his best interests over that of his employers[194]. On the basis of breach the fiduciary duty the employer is then justified in claiming damages from the guilty employee. Where an employee has failed to adhere to the internet usage policy of the employer, he may be found guilty of disobedience[195]. The employer can then on the strength of this take disciplinary steps necessary[196].

Breach of the employment contract can also be taken a step further. In circumstances where an employer is held vicariously liable for the online conduct of his employees the employee

[188] *Sappi Novoboard (Pty) Ltd v Bolleurs* (1998) 19 ILJ 784 (LAC).
[189] *Premier Medical and Industrial Equipment (Pty) Ltd v Winkler & Another* 1971 (3) SA 866 (W).
[190] *Council for Scientific & Industrial Research v Fijen* (1996) 17 ILJ 18 (A).
[191] JS Van Jaarsveld & PBS Van Eck (note 43 above) 111.
[192] *Smit v Workmens Compensation Commisioner* 1979 (1) SA 51 (A).
[193] JS Van Jaarsveld & PBS Van Eck (note 43 above) 110.
[194] M Van Jaarsveld (note 76 above) 654.
[195] Ibid.
[196] Ibid.

and the employer become joint and severally liable[197]. However what happens in practice is that the third party is most likely to recover loss from the employer as the claim against the employer is more financially sound[198]. If the vicarious liability arose out of the employee's negligence or the employee intentionally committed acts on the internet that resulted in the employer's vicarious liability and the employer has already paid out damages to the third party, the employees conduct constitutes breach of the employment contract[199]. The employer can then proceed against the employee for the remedies arising out of breach of contract.

5. CONCLUSION

It is clear that internet facilities in the workplace offers both advantages and disadvantages which are far reaching for the employer. However it is evident that its effectiveness and benefit in the workplace outweighs the threats which they pose to the employer. There is therefore no way that a complete ban or total eradication of technology in the working world will ever succeed. What an employer should therefore adopt is a system which sets clear restricts of what is permissible during working hours and penalties for such conduct but bears in mind that the current work force may respond negatively to an environment which bars out use of internet for non-work related purpose. In turn this will create a low productivity, demotivated working environment where employees are less productive and unhappy. An easy solution to this would be to allow access for personal and non-work related use during lunch breaks and use that is monitored and not unregulated.

The employer is faced with major battles when his employees do not adhere to internet usage limits set in the workplace in the form of both civil litigation and criminal action. This threatens both the employers business and his pocket drastically. The only way that an employer can overcome this is by efficiently regulating internet usage in the workplace through internet usage policies and disciplinary measures and remain constantly vigilant about his employee's activities online while also respecting his employee's constitutional rights to privacy by not being too intrusive. However exactly where our law stands on most of these matters is still too be tested by our courts as South Africa has very little binding decisions that can be relied on as authority. What remains clear however is that a passive

[197] ME Manemela (note 44 above) 126.
[198] Ibid.
[199] Ibid.

approach to the use internet in the workplace no longer serves the employer or the employee well.

BIBLIOGRAPHY

Primary Sources

Cases

Bernstein V Bester NO 1996 (2) SA 751 (CC).

Bramford & others v Energiser (SA) Limited [2001] 12 BALR 1251 (P).

Council for Scientific & Industrial Research v Fijen (1996) 17 ILJ 18 (A).

CWU v Mobile Telephone Networks (Pty) (Ltd) 2003 8 BLLR 741 (LC).

Dauth and Brown & Weirs Cash & Carry (2002) 23 ILJ 272 (CCMA).

Galago Publishers (Pty) Ltd v Erasmus 1989 1 SA 276 (A)

Goosen v Carolines Frozen Yoghurt Parlour (Pty) Ltd and another 36 (1995) 16 ILJ 396 (IC)

Gouws Score v Price and Pride Furnishers [2011] 11 BALR 1155 (CCMA).

Grobler v Naspers Bpk 2001 (4) SA 938 (LC)

In Re Hyundai Motors Distibutors (Pty) Ltd and Others v Smith and NO and Others 2001 (1) SA 545 (CC).

Jane Doe v XYZ Corporation 382 N.J.Super. 122 (Appellate Division N.J., December 27, 2005).

Knox v State Department of Indiana 93 F 3d 1327.

Memela and Another v Ekhamanzi Springs 33 ILJ 2911 (LC) 2012.

Moonsamy v Mailhouse (1999) 20 ILJ 464 (CCMA).

Morse v Future Reality Ltd ET case number 54571/95.

MWO obo Coetzer v Champion Casinos (CCMA 15 August 2000 (case number 16821) unreported).

NK v Minister of Safety and Security 2005 (6) SA 4 9

Owens & Hutton v Morgan Stanley & Co Inc United States District Courts Southern District of New York 96 CIV 9747 (1996).

Philander v CSC Computer Sciences [2002] 3 BALR 304 (CCMA)

Premier Medical and Industrial Equipment (Pty) Ltd v Winkler & Another 1971 (3) SA 866 (W).

Protea Technology Ltd and another v Wainer and others (1997) 9 BCLR 1225 (W).

Sappi Novoboard (Pty) Ltd v Bolleurs (1998) 19 ILJ 784 (LAC).

Sedick and another/ Krisay (Pty) Ltd [2011] BALR 879 (CCMA)

Statutes

Constitution of the Republic of South Africa

Copyright Act No 98 of 1978

Electronic Communications and Transactions Act No 25 of 2005

Employment Equity Act No 55 of 1998

Compensation for Occupational Injuries and Diseases Act 130 of 1993

Occupational Health and Safety Ac No 85 of 1993

Regulation of Interception of Communications and Provision of Communicated-related Information Act No 70 of 2002

The Code of Good Practice on Dismissal

The Code of Good Practice on the Handling of Sexual Harassment Cases GG No 19049 of 17 July 1998.

Film and Publications Board Act No 65 of 1996

Secondary sources

Books

Burchell J *The law of defamation in South Africa* Cape Town: Juta, (1985)

Buys R *Cyberlaw@SA: the law of the Internet in South Africa* 3ed Pretoria: Van Schaik, (2000).

Neethling J, Potgieter JM & Visser PJ *Law of Delict* 4ed Durban: Lexis Nexis, (2002).

Papadopolous S & Snail S *Cyberlaw @ SA III : The law of the Internet in South Africa* 3ed Pretoria: Van Schaik, (2012).

Van Jaarsveld F & Van Eck BPS *Principles of Labour Law* 2ed Durban: Lexis Nexis, (2002).

Journals

Aiello JR 'Computer based monitoring: Electronic surveillance and its effects' (1993) 23(7) *Journal of Applied Social Psychology* 499-507.

Beech W 'The right of an employer to monitor employees electronic mail, telephone calls, internet usage and other recordings' (2005) 26 *Industrial Labour Law Journal* 650-660.

Bibby A 'Who got e-mail' At work, e-mail and the web become public'(2001) 40 *The magazine of the ILO World of Work* 1-34

Boyd DM & Elison NB 'Social network sites: Definition, history and scholarship' (2008) 13 *Journal of Computer-Mediated Communications* 210-230.

Calisti MC 'You are being watched: The need for notice in employer monitoring' (2008) 96(4) *Kentucky Law Journal* 649-668.

Calitz K 'Vicarious liability of employers: Reconsidering risk as the basis for liability' (2005) 3 *TSAR* 215-235.

Chalykoff J & Kochran TA 'Computer-aided monitoring: Its influence on employee satisfaction and turnover' (1989) 40 *Personnel Psychology* 807-834.

Ciochetti C 'The eavesdropping employer: A 21st century framework for employer monitoring' (2001) 48 *American Business Law Journal* 285-369.

Coetzee J 'The Electronic Communications and Transaction Act 25 of 2002: Facilitating electronic commerce' (2004) 3 *Stellenbosch Law Review* 501-521.

Collier D 'Workplace privacy in the cyber age' (2002) 23 *Industrial Labour Journal* 1743-1760.

Currie I 'The concept of privacy in the South African Constitution: Reprise' (2008) 3 *TSAR* 449-557.

Ebersohn G 'Internet Law: Peer-to-peer file sharing services' (2003) 2 *TSAR* 376-381.

Ebersohn G 'The unfair business practises of spamming and spoofing' (2003) *De Rebus* 25

Etsebeth V ' The growing expansion of vicarious liability in the information age (part 1)' (2006) 3 *TSAR* 564-580.

Etsebeth V ' The growing expansion of vicarious liability in the information age (part 2)' (2006) 4 *TSAR* 752-765.

Dancaster L 'Internet Abuse: A survey of South African companies' (2001) 22 *Industrial Labour Journal* 862-865.

David J 'Policy enforcement in the workplace' (2002) 21 *Computers and Security* 506-513.

Fazekas CP '1984 is still Fiction: Electronic monitoring in the workplace and US privacy law' (2004) 15 *Duke Law and Technology Review* 1-16.

Fereirra A & Du Plessis T 'Effect of online social networking on employee productivity' (2009) 11 *South African Journal of Information Technology* 1-11.

Flanagan JA 'Restricting electronic monitoring in the private workplace' (1994) 43(6) *Duke Law Journal* 1256-1281.

Frayer CE 'Employee privacy and internet monitoring: Balancing workers rights and dignity with legitimate management interets' (2002) 57(2) *Business Lawyer* 857-874.

Gilburg D 'Management techniques for bringing out the best in generation Y, CIO, Oct. 26, 2007. Available at:http://www.cio.com/article/149053/Management_Techniques_for_Bringing_Out_the_Best_in_Generation_Y (Accessed on 20 June 2015).

Griffiths M 'Internet abuse in the workplace: Issues and concerns for employers and employment counsellors' (2003) 40 *Journal of Employment Counselling* 87-96.

Gule S 'Employers vicarious liability for sexual harassment' (2005) 13(2) *Journal Business Law* 66-69.

Hathi S 'billions lost from social networking' (2008) 12(2) Computers and Security 9. Horung MS 'Think before you type: A look at e-mail privacy in the workplace' (2005) 11 *Fordham Journal of Corporate and Financial Law* 115-160.

Jansen M 'The protection of copyright on the internet' (2004) 12(2) *Journal Business Law* 100-104.

Jansen M 'The protection of copyright works on the internet- an overview' (2005) 38(3) *The Comparative and International Law Journal of Southern Africa* 344-354.

Johnson J 'Information Technology Policies' (2001) De Rebus 38.

Kesan JP 'Cyber-working or cyber-shrinking?: A first principlesexamination of electroniv privacy in the workplace' (2002) 54(2) *Florida Law Review* 289-332.

Lawacks V & Van der Walt A 'Interception of electronic communications in the workplace' (2005) *Obiter* 133-139.

Le Roux R 'Section 60 of the Employment Equity Act 1998: Will a comparative approach shake the joker out of the pack?' (2006) 27(3) *Obiter* 411-428.

Manmela ME 'Vicarious liabilty: Paying for the sins of others' (2004) 16 *South African Mercantile Law Journal* 125-132.

McGregor M 'The right to privacy in the workplace: General case law and guidelines for using the internet and e-mail' (2004) 16 *South African Mercantile Law Journal* 638-649.

McGregor M 'The use of e-mail and internet in the workplace' (2004) 11(3) *Journal of Business Law* 189-192.

Mischke C 'Intercepting and monitoring employees e-mail communications and internet access' (2003) 12(8) *Contemporary Labour Law* 72-76

Mobida M 'Intercepting and monitoring employees e-mail communications and interenet access' (2003) 15 *South African Mercantile Law Journal* 363-371.

Mobida M 'Who should be liable?' (2003) 11(2) *Journal of Business Law* 112-115.

Muhl C 'Workplace e-mail and internet use: Employees and employers beware' (2004) 26(2) *Monthly Labour Law* 36-45.

A Mukhebeir & L Ristow 'An Overview of sexual harassment: Liabilty of the employer' (2006) Obiter 259-262.

Nebeker DM & Tatum BC 'The effects of computer monitoring, standards and rewards on work performance, job satisfaction and stress. (1993) 23(7) *Journal of Applied Psychology* 508-537.

Nel S 'Problematic issues regarding transborder cybersmear' (2010) 22 *South African Mercantile Law Journal* 360-387.

Papa LJ & Bass SL 'How employers can protect themselves from liability for employees misuse of computer, internet, and e-mail systems in the workplace'(2004) 10 *Boston Journal of Science and Technology Law* 110-124.

Paul RA & Chung LH 'Brave new cyberworld: The employers legal guide to interactive internet' (2008) 24 *Labour Law* 109-142.

Pistorius T 'Monitoing interception and the big boss in the workplace: is the devil in the details?' (2009) *Potchefstroom Electronic Review* 1-26.

Riedy MK & Wen JH 'Electronic sureviellance of internet access in the American Workplace: Implications for management' (2010) 19 *Information of Technology and Law* 87-99.

Roos A 'Privacy in the facebook era: A South African legal perspective' (2012) 129 *The South African Law Journal* 375-402.

Rothstein LE 'Privacy or dignity?: Electronic monitoring in the workplace' (2000) 9(3) *New York Law School Journal of International and Comparative Law* 379-412.

Smit N & Van der Nest D 'When sisters are doing it for themselves: Sexual harassment claims in the workplace' (2004) 3 *TSAR* 520-543.

Stafford C & Mearns MA ' What happens when organisations embrace social networking? Knowledge sharing at multinational business solution corporations' (2009) 11(4) *South African Journal of Information Management* 1-11.

Subramanien D & Whitear-Nel N 'A fresh perspective on South African law relating to the risks posed to employers when employees abuse the internet' (2013) 37 *South African Journal of Labour Relations* 9-23.

Swaya ME & Einstein SR 'Emerging technology in the workplace' (2005) 21 *Labor Lawyer* 1-18.

Thomas JH, Englander F & Englander V 'Ethical, legal and economic aspects if employer monitoring of employee electronic mail' (1999) 19 *Journal of Business Ethics* 99-108.

Van Eck BPS 'Misuse of the internet at the workplace' (2001) 2 *De Jure* 364-369.

Van Jaarsveld M 'Forearmed is forewarned: Some thought on the inappropriate use of computers in the workplace' (2004) 16 *South African Mercantile Law Journal* 651-666.

War WA ‘Social software: Fun and games, or business tools’ (2008) 34(4) *Journal of Information Science* 591-604.

Whitear-Nel N ‘Child pornography in the workplace’ (2011) 32 *Industrial Law Journal* 787-804.

Young KS & Case CJ ‘Internet abuse in the workplace: New trends in risk management’ (2004) 7 *CyberPsychology and Behaviour* 105-111.

Zhou AZ & Fink D ‘The intellectual capital web’ (2003) 4 *Journal of Intellectual Capital* 34-48.