Title:

The employee's right to privacy versus the employer's right to monitor electronic transmissions from the workplace

By

Name: Patience Chigumba

Student number: 208515916

Supervised By: Darren Subramanien

DECLARATION

I, Patience Chigumba do hereby declare that unless specifically indicated to the contrary in this text, this dissertation is my own original work and has not been submitted to any other university in full or partial fulfilment of the academic requirements of any other degree or other qualification.

Signed at Pietermaritzburg on this the 12th Day of December 2013.

Signature: *P Chigumba.*

ABSTRACT

Privacy is important because it represents human dignity or the preservation of the 'inner sanctum'. Due to technological developments the operational concerns of employers are continuously threatened or challenged by the employee's right to privacy in the workplace. It is common knowledge that employees all over the world are exposed to numerous privacy invasive measures, including drug testing, psychological testing, polygraph testing, genetic testing, psychological testing, electronic monitoring and background checks. The issue at the heart of this dissertation is to determine to what extent privacy is protected in the South African workplace given advancements in technology and the implications (if any) for the right to privacy. A secondary aim of the dissertation is to attempt to provide a pragmatic balance between the privacy concerns of employees and the operational needs of employers in this technological age. This dissertation mainly focuses on the invasion of privacy in the workplace through the monitoring of focus areas of email, internet and telephone correspondences of the employee. To provide an answer to the research issue discussed above, this dissertation addresses four ancillary or interrelated issues. First, the broad historical development of the legal protection of privacy is traced, examined and a workable definition of privacy is identified with reference to academic debate and comparative legislative and judicial developments. Secondly legislation on the regulation of monitoring in the workplace is critically examined and discussed. Thirdly, those reasons and practices, which threaten privacy in the employment sphere, are identified and briefly discussed. More specifically, the dissertation considers how these reasons and practices challenge privacy, the rationale for their existence and, if applicable, how these reasons and practices may be accommodated while simultaneously accommodating both privacy and the legitimate concerns of employers. Fourthly, a detailed evaluation of the case law and judicial developments of South Africa on the right to privacy in the workplace are examined so as to seek a balance if any between the employee's right to privacy and the employer's right to monitor. To successfully tackle the above issues the dissertation uses the conventional legal methodology associated with relative legal research, which includes a literature review of applicable law and legal framework and a review of relevant case law.

TABLE OF CONTENTS PAGE

Chapter 1: The right to Privacy

1. Introduction

Privacy notions are deep rooted in history but privacy protection as a public policy question is a modern notion. The right to privacy is one of the most important rights and is recognized all over the world in diverse religions and cultures but it is not an absolute right because it can be limited according to the Constitution of the Republic of South Africa; hence that's where the employer's right to monitor gets favour from. Privacy is a valuable and advanced aspect of personality. The right to privacy is now provided for in the Constitution but in the past it was provided for through other rights like the right to dignity.

1.1 Background:

The right to privacy is not a new legal concept in South Africa. Before this right came into being, decisions supporting privacy were based on property rights and contract because an independent right to privacy was not recognized. "Privacy is the right to be left alone; the most comprehensive right and the most valued by civilized men'- a legal shield which could be asserted by the individual against the prying eyes of the public".[1] This became the same proposition in our courts through the case of,*O'Keeffe v Argus Printing and Publishing Co. Ltd and Others*.[2] The modern law of invasion of privacy arose from a need to protect the individual's dignity and mental tranquillity in a sophisticated and developed society where technology has enabled the former boundaries of privacy to be invaded.[3]

The Constitution of South Africa is partially new and explicitly protects the right to privacy. Before the Constitution came into force, the right to privacy had always been and is still protected at common law. The right to privacy was protected at common law under personality rights and the available remedy was under actio injuriarum, which provided that, for one to get relief, the act complained of must have been wrongful, intentional and violated one or other real rights related to personality which every free man was entitled to enjoy.[4] It took time for the

[1]*Olmstead v The United States 277 US 4381927*.
[2]*O'Keeffe v Argus Printing and Publishing Co. Ltd and Others 1954 (3) SA 244 (C)*.
[3]A Cockhead. "A Critical Analysis of Law of Privacy with Reference to Invasion of Privacy of Public Figures. (1990) pg 5.
[4]*R v Umfaan 1908 TS 62*.

legal system to establish a right to privacy that was not intertwined with personality rights. Judgments which provided for privacy were limited to the right to dignity, honour and self-respect. In the *S v A* case[5] Botha AJ stated that, the right to privacy is included in the concept of*dignitas* and the infringement of a person's privacy prima facie constitutes an impairment of his *dignitas*. This was the same reasoning in the *O'Keeffe*[6]case which held that, "the unlawful publication of a person's photograph and name for advertising purposes constituted an aggression upon the person's dignitas." This serves as proof to confirm that before the constitution came into being, the right to privacy was provided for under the right to dignity.

1.2 Meaning of Privacy:

The right to privacy is intertwined with the right to dignity that's why it is fundamental to both the social and personal development of an individual. This right concerns a person's choice of whether he/she wants to allow others to know about his/her activities.This right involves protection against infringement from other people and even against the state. Remp maintains that,

> Privacy refers to the social balance between an individual'sright to keep information confidential and the societal benefit derived from sharing information, and how this balance is codified to give individuals the means tocontrol personal information.[7]

The right to privacy in the context of the employment relationship is unique and very difficult to clarify. On the one hand, the employee has a right to privacy but he or she is supposed to be honest and loyal, especially during working hours, and stands in a relationship of trust with his or her employer.[8] There are a number of theories of privacy, although the definitions of privacy are not all encompassing Tavani[9] proposes that privacy is, *"in a situation with regard to others [if] in that situation the individual ... is protected from intrusion, interference, and information access by others"*.The South Africa Constitution on the other hand defines privacy or

[5]1971 (2) SA 293 (T).
[6]1954 (3) SA 244 (C).
[7] M Remp Ann. The 2/" Century: Meeting the Challenges to Business Education (1999) pg 117.
[8]A Dekker. Vices or Devices" Employee Monitoring in The Workplace (2004) 16 SA Merc LJ pg 622, 625.
[9]H.T Tavani. 2007. 'Philosophical theories of privacy: Implications for an adequate online privacy policy', *Metaphilosoph*, **38**(1): 1-22. pg 10

"Informational Privacy" or "Data Protection as: "*... the right not to have their person or home searched, their property searched, their possessions seized or the privacy of their communications infringed*."[10] Informational privacy is, therefore, achieved when one has control of his or her personal information.[11]According to McQuoid – Mason, most of the definitions are synonymous with amongst others "solitude", "anonymity and reserve", "intimacy" and "being let alone".[12] The definitions are argued to be useless in that they do not shed light as to when a court is willing to consider an invasion to the right to privacy.[13]

They are instances which amount to a breach of privacy in terms of the common law for example: entry into private residence, the reading of private documents, the disclosure of private facts acquired through an unlawful intrusion and the disclosureof private facts in breach of confidentiality.[14]The Constitution, primarily conceives of privacy as the limited access to the self and the control over information about oneself.[15] In *Investigating Directorate: Serious Economic Offences v Hyundai MotorDistributors*[16] the Constitutional Court described privacy as, " the right to be let alonewhen it pointed out that individuals did not lose their right to privacy once they venturedoutside the "truly personal realm" and "inner sanctum" because privacy protects people not places".Furthermore another case described privacy as the right to be left alone,which went beyond being "a negative right to occupy a space free from governmentintrusion" but also protected personhood.[17] Both cases were emulating one and the same thing that the right to privacy does not only apply to one's private life but in society also.

Neethling[18] on the other hand states that, "Privacy is an individual condition of life characterised by exclusion from publicity. This condition includes all the personal facts which the person himself at the relevant time determines to be excluded from the knowledge of outsiders and in

[10]S Eiselen, A Roos , T Pistorius & D Van der Merwe. (2006). *Information and communications technology law*. Durban: LexisNexis pg 353.
[11] Ibid
[12] McQouid – Mason. *The Law of Privacy in South Africa* (1978) 98 – 99.
[13] Ibid.
[14]*Bernstein v Bester NO 1996 (2) SA 751 (CC) 784*.
[15] M, Gondwe. *The Protection of Privacy in the Workplace: A Comparative Study.* (2011) Published dissertation for a Degree of Doctor of Law at Stellenbosch University. page 130
[16]*Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors 2000 (10) BCLR 1079 (CC).*
[17]*National Coalition for Gay and Lesbian Equality v Minister of Justice 1999 (1) SA 6 (CC) 60* D – E.
[18]Neethling et al *Neethling's Law of Personality* (1996) pg 36.

respect of which he evidences a will for privacy." The definitions of privacy are in harmony on the fact that privacy is protection of personal information that one does not want to be known by others. Cockhead[19] maintains that it would appear like this definitions of the modern law of invasion of privacy, arose out of a need to protect the individual's dignity and mental tranquillity of people in a sophisticated and developing society where technology has enabled the former boundaries of privacy to be invaded. Cockhead[20] fails to illustrate that the above will apply when one has a legitimate expectation to privacy. In*National Media Ltd v Jooste*[21]it was held that, privacy is an individual condition of life characterised by exclusion from the public and publicity which embraces all those personal facts which the person concerned has determined to be excluded from the knowledge of outsiders and in respect of which he/she has the will that they be kept private.

1.3 Constitutional Right to Privacy:

The Constitution of the Republic of South Africa section 14 provides that,

Everyone has the right to privacy, which includes the right not to have-

(a) their person or home searched;
(b) their property searched;
(c) their possessions seized; or
(d) the privacy of their communications infringed.[22]

Section 14 is said to protect against two types of privacy infringements, ‘‘The first part guarantees a general right to privacy, the second part protects against specific infringements of privacy, namely searches and seizures and infringement of the privacy of

[19]A Cockhead. *A Critical Analysis of Law of Privacy With Reference To Invasion Of Privacy Of Public Figures. (*1990) 5.
[20]Ibid.
[21]*National Media Ltd v Jooste 1996 (3) SA 262 (A).*
[22]The Constitution of the Republic of South Africa of 1996: s 14.

communications".[23]Although the Constitution provides for the right to privacy, for the section to apply to any individual that person must have a legitimate expectation of his/her right to privacy being upheld. It is said that section 14 protects information to the extent that it limits the ability to gain, publish, disclose or use information about others.[24]The second part is a subordinate of the first part in that for constitutional protection to arise one has to furnish proof that the infringement of the specific types of privacy emulated from infringement of the general right to privacy. A legitimate expectation of privacy is subjective in nature but the society must recognize it to be objectively reasonable.[25] The subjective nature of the expectation entail that no one should expect their right to privacy to be upheld if they have consented implicitly or explicitly to its invasion.[26] It has been argued that the fact that an employee has signed a contract with his employer may be regarded as implied consent that he/she will adhere to all company policies including the policy to monitor all employee electronic transmissions.[27]

In my opinion, it is hard for one to satisfy what the society can call being objectively reasonable because there is no set rule of it and society itself comprises of individuals with different expectations that cannot be reconciled as one if they are no set rules to follow. The *Bernstein*[28] case tried to shade light as to what society can regard as being an objectively reasonable expectation of privacy,

> The truism that no right is to be considered absolute implies that from the outset of interpretation, each right is always limited by every other right accruing to another citizen. In the context of privacy this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preferences and home environment which is shielded from erosion by conflicting lights of the community. This implies that community lights and the rights of fellow members place a corresponding obligation on a citizen, thereby shaping the abstract notion of individualism towards identifying a concrete member of civil society. Privacy is acknowledged in the truly personal realm but as a person moves into communal relations and activities such as business and social interaction, the scope of the personal space shrinks accordingly.[29]

[23] Currie & de Waal (2005) Bill of Rights Handbook pg 317 , 318.
[24]Ibid.
[25]Ibid.
[26]Ibid.
[27]Ibid.
[28]*Bernstein vBester 1996 (2) SA 751 (CC) para 67*.
[29] Ibid.

This statement illustrate that there is plenty of room for the right of privacy to be infringed in open society because what the society regards as objectively reasonable must mainly conform to the convictions of that society and since individualism is shunned a person's personal right to privacy can be easily disregarded unless it concerns things which don't involve society intimately. The exercise of one's right to privacy in the public realm means there is more room that right will be infringed and there is no guarantee that your right will be upheld against the other individual's right to whom you are in conflict with. When one waives his/her legitimate expectation to privacy Currie & De Waal states that the test to be applied is what is reasonable pursuant to the values that" link the standard of reasonableness.[30] I am afraid this does not shade more light into what is an objectively reasonable expectation. Neethling maintains that, "the acquaintance with private facts should not only be contrary to the subjective determination and will of the prejudiced party, but at the same time, viewed objectively, also be unreasonable or contrary to the legal convictions of the community".[31] This is the position according to common law. In *Bernstein v Bester*[32] the right to privacy was characterised as lying along a range, where the more a person interrelates with the world, the more the right to privacy becomes attenuated.

It is only the inner sanctum of a person that is truly protected from privacy. This was the idea emulated in the *Bernstein* case and it was the same proposition emphasized in the *Case* v *Minister of Safety and Security*[33] case which held that,

> What erotic material I may choose to keep within the privacy of my home, and only for my personal use there, is nobody's business but mine. It is certainly not the business of society or the state. Any ban imposed on my possession of such material for that solitary purpose invades the personal privacy which s 13 of the Interim Constitution guarantees that I shall enjoy.

The *Bernstein*[34]case held that, a very high level of protection should be given to the individual's intimate personal sphere of life and the maintenance of its basic preconditions, and that there was a final untouchable sphere of human freedom that was beyond any interference from any public

[30] Currie & de Waal (2005) *Bill of Rights Handbook* .pg 317 , 318.
[31] J Neethling. *Personality rights: A comparative overview* CISA Vol 38(2) July 2005.
[32]*Bernstein v Bester NO 1996 (2) SA 751 (CC) 784.*
[33]*Case v Minister of Safety and Security 1996 (3) SA 617 (CC) para 91.*
[34]*Bernstein v Bester NO 1996 (2) SA 751 (CC) 784.*

authority. Langa DP elaborated on the above by clearly stating that the right to privacy does not relate solely to the individual within his or her intimate sphere.[35] He further said that, when people are in their offices or in their cars or on mobile telephones they still retain a right to be left alone by the State unless certain conditions are satisfied.[36] When a person has the ability to decide what he or she wishes to disclose to the public and has a reasonable expectation that such a decision will be respected, the right to privacy will come into play.[37] Ackerman J in contrast to the above held that , this inviolable core to a legitimate expectation of privacy is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the individual's activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation.[38] It is important to note that a person's legitimate expectation to privacy does not extend to unlawful activities done in private. The *Jordan*[39] case is authority on this, as Ngcobo J said,

> I do not accept that a person who commits a crime in private, the nature of which can only be committed in private, can necessarily claim the protection of the privacy clause…The law should be as concerned with crimes that are committed in private as it is with crimes that are committed in public.

Dekker[40] maintains that, the infringement of the right to privacy can sometimes be justifiable in the context of the employment relationship. To determine justifiability, it is necessary to balance the competing interests of the employer (the right to economic activity) and the employee (the right to privacy).[41] Under the interim Constitution, the right to privacy could be restricted if it was reasonable and justifiable, and if the restriction did not negate the essential content of the right.[42] The limitation clause provided for certain levels of scrutiny, in terms of which stronger protection was awarded to certain rights. [43]The right to privacy did not fall within that category,

---

[35]*Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others 2001 1 SA 545 (CC).*
[36] Ibid
[37] Ibid
[38]*Bernstein v Bester NO 1996 (2) SA 751 (CC) 784.*
[39]*S v Jordan and Others (Sex Workers Education and Advocacy Task Force and Others as Amici Curiae 2002 6 SA 642 (CC).*
[40] A Dekker. Vices or Devices" Employee Monitoring in The Workplace (2004) 16 SA Merc LJ pg 622, 625.
[41]*Goosen v Caroline's Frozen Yogurt Parlour (Pty) Ltd 1995 16 ILJ 396 (IC).*
[42] Ibid.
[43] Ibid.

and so a restriction of the right to privacy had only to be reasonable and justifiable.[44] An infringement would be reasonable if the interest underlying the limitation is of sufficient importance to outweigh the constitutionally protected right and the means must be proportional to the objective of the limitation.[45]

Chatfield & Hakkila[46] submit that, in the context of mobile phone communications, users consider their mobile phones personal and private; same as a handbag or a wallet.This is the case because it has been found that users perceived voice communications, emails, pictures and Short Message Services (SMS's) have different levels of privacy.[47] As signified in the previous paragraph, the Constitutional Court perceives an individual's expectation of privacy as a continuum with one's personal and intimate life at the one end and communal or business life at the other end.[48] A person's expectation of privacy decreases along the continuum as one moves further away from his/her personal domain.[49] Both employers and employees have a right to privacy that is recognized by the Constitution of South Africa.[50] Lease[51] is of the idea that, employers have legitimate requirements for wanting to monitor or intercept employees' personal communications which take place in the general course of business. In contrast, the Constitutional Court points out that an employee cannot be expected to have no right to privacy in the workplace.[52] Furthermore, employees will always be entitled to some level of privacy, meaning that the employer cannot force an employee to relinquish all rights to privacy.[53] Therefore, there is need for the employer to clearly differentiate between what is considered private and what is considered business related data.[54] The difference in expectations of privacy between personally-owned devices and organisation-owned devices therefore means that

[44]A Dekker. Vices or Devices" Employee Monitoring in The Workplace (2004) 16 SA Merc LJ pg 622, 625.
[45] Ibid.
[46] C Chatfield. & J Hakkila. 2005. 'It's like if you opened someone else's letter — User perceived privacy and social practices with SMS communication'. **In *Proceedings of the seventh international conference on human computer interaction with mobile devices and services***, Salzburg, Austria, pg219, 222.
[47] Ibid.
[48] S Eiselen, A Roos, T Pistorius & D Van der Merwe. (2006). *Information and communications technology law*. Durban: LexisNexis.pg 353
[49] Ibid.
[50] D, Collier. 2002. 'Workplace privacy in the cyber age', *Industrial Law Journal*, 23: pg 1743-1759.
[51] D, Lease. 2005. 'Balancing productivity and privacy: Electronic monitoring of employees.' Paper presented at the European Management and Technology Conference, Rome, Italy, June 2005.
[52] D, Collier. 2002. 'Workplace privacy in the cyber age', *Industrial Law Journal*, 23: pg 1743-1759.
[53] Ibid.
[54] Ibid.

theorganisation's computer usage policies cannot be extended to include personally-owned devices.[55] A separate policy that specifically caters for the unique characteristics of personally-owned devices should be drafted.

To determine whether the right to privacy has been infringed, a balance must bestruck between the right of individuals to be left alone and the right of the State toinfringe the individual's privacy in order to achieve some State objective, forexample, crime prevention. The Constitutional Court adopted the view, as espoused by the United States, that individuals retain the right 'to be left alone' by the state unless certain conditions are met.[56]Further in *Mistry v Interim Medicaland Dental Council of South Africa and Others*[57] it was held that the more public theundertaking and the more closely it would be regulated, the more attenuatedwould the right to privacy be and the less intense any possible invasion.[58] In developing interception and monitoring legislation consistent with the valuesof the Constitution, there must be a balance between the need to make legislativeprovision equipping law-enforcement with the means to combat crime and theneed to retain a modicum of privacy of communications.[59]

1.4 Limitation of the right to privacy

The right to privacy is not an absolute right; it is subject to limitation just like other rights in Chapter 2 of the Constitution. These rights are subject to limitation under section 36 of the Constitution which provides for a test that has to be satisfied in order for an infringement on a right to be allowed. The right to privacy is subject to limitation by a law of general application to the extent that it is reasonable and justifiable in an open and democratic society, based on human dignity, equality and freedom, taking into account all relevant factors including those mentioned in the section. *S v Makwanyane*[60]is a landmark case on the issue of how, when and why the

[55] P, Hunter. 2007. 'Is now the time to define a mobile security policy', *Computer Fraud and Security*, 6: pg10-12.
[56] 1991 2 SA 117 (W).
[57]*Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC) ;1998 (7) BCLR 880 (CC).*
[58]*Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC)* para 27.
[59]Ibid.
[60]*S v Makwanyane 1995 (3) SA 391 (CC); 1995 (6) BCLR 665 (CC).*

Constitutional court will allow a limitation of a right. In the *Makwanyane* case the constitutional court held as follows,

> The limitation of constitutional rights for a purpose that is reasonable and necessary in a democratic society involves the weighing up of competing values, and ultimately an assessment based on proportionality. This is implicit in the provisions of s33 (1) (lC). The fact that different rights have different implications for democracy, and In the case of our constitution for an open and democratic society based on freedom and equality', means that there is no absolute standard which can be laid down for determining reasonableness and necessity. Principles can be established, but the application of those principles to particular circumstances can only be done on a case by case basis. This is inherent in the requirement ofproportionality, which calls for the balancing of different interests. In thebalancing process, the relevant considerations will include the nature of thelight that is limited and the importance to an open and democratic societybased on freedom and equality; the purpose for which the light is limited andthe importance of that purpose to such a society; the extent of the limitation,its efficacy and particularly where the limitation has to be necessary, whetherthe desired ends could reasonably be achieved through other means lessdamaging to the light in question. In the process regard must be had to theprovisions of s33(1) (IC), and the underlying values of the Constitution,bearing in mind that, as a Canadian Judge has said, 'the role of the Court is notto second-guess the wisdom of policy choices made by the legislators.[61]

The court in *S v Makwanyane*[62] was basically elaborating on the test set out in section 36 of the Constitution although when the case was heard the limitation clause was section 33 of the Interim Constitution. It also emphasized that they cannot be any set rules as to when a court will allow for the limitation of a right but every case will have to be examined according to its own merits and limitation must be sought when other solutions have been attempted and failed. Section 36 of the Constitution lays out the test for limitation as follows,

> (1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including-
>
> *(a)* the nature of the right;
>
> *(b)* the importance of the purpose of the limitation;
>
> *(c)* the nature and extent of the limitation;
>
> *(d)* the relation between the limitation and its purpose; and

[61]Ibid.
[62]Ibid.

(e) less restrictive means to achieve the purpose.

(2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.[63]

S v Bhulwana[64] sums up the provisions of the limitations clause by saying,

> In sum, therefore, the court places the purpose, effects and importance of the infringing legislation on one side of the scales and the nature and effect of the infringement caused by the legislation on the other. The more substantial the inroad into fundamental lights, the more persuasive the grounds of justification must be.[65]

A right can be limited if the limitation is authorised by a law of general application and as so far as it is justifiable ina democratic society based on the criteria set out in subsection 36(1) (a)-(e). *The National Coalition for Gay and Lesbian Equality and Another v Minister of Justice and Others*[66]is authority on the fact that the court can hold a limitation to be unjustifiable if it is a sever limitation on a right and if the limitation itself serves no valid purpose. Ultimately therefore, the purpose of any given law will be weighed up against the importanceof the fundamental right that it stands to infringe.[67]The *Moonsamy*[68] case held that,

> The rights that a citizen is entitled to in his or her personal life cannot simply disappear in his or her professional life as a result of the employer's business necessity. At the same time the employer's business necessity might legitimately impact on the employee's personal rights in a manner not possible outside the workplace. Therefore there is a clear balancing of interests.[69]

This case highlights that the fact that an employer may have company policy that allows for the monitoring of the employees electronic transmissions does not mean it's a valid limitation of the employees right to privacy and workplace policy does not extend to one's social life outside the workplace. The employee's expectation of privacy will have to be weighed against the

[63]Act 108 of 1996: s 36.
[64] (1996) 1 (SA) 388 (CC).
[65]*S v Bhulwana (1996) 1 (SA) 388 (CC)* para 18.
[66] 1999 (1) SA 6 (CC).
[67] W Beech. "Right of Employer to Monitor Employees' Electronic Mail, Telephone Calls, Internet Usage and other Recordings" 2005 (26) *Industrial Law Journal* pg 655.
[68] (1999) 20 ILJ 464 (CCMA).
[69]*Moonsamy v The Mailhouse(1999) 20 ILJ 464 (CCMA)* at 471G.

employer's expectation to protect his business interests. From the employer's perspectives it seems as privacy is not an absolute right because it is his/her equipment that is being used by the employee and he has to protect his/her business from viruses, excessive use and cyber loafing which implies the employees omission to do assigned work.[70]It is from the same reasoning that Le Roux[71] states,

> The employer is also permitted to set more general standards relating to conduct in the work place and to the use of equipment and tools. The employer can, for example, prescribe when personal computers may be used, for what purposes they may be used, and how they may be used. The same applies to access to the Internet. If an employee fails to comply with these rules it will, in principle, be open to the employer to discipline an employee for such a failure. In the correct circumstances this may also justify the disciplinary sanction of dismissal.

The employer has a right to protect his property, interests and to operate an effective and efficient business through limitation of the employee's right to privacy. [72]The employer also has a duty upon him to make sure he is operating his business in a safe and non-discriminatory environment.[73] The misuse of the employer's electronic transmission equipment in the workplace poses a lot of risk for the employer hence the employee's right to privacy has to be limited. The misuse of e-mail for private purposes may increase the employer's overhead costs, cause communication delays and even blockages of communication systems.[74]

In conclusion according to what was discussed in this chapter, the right to privacy is mainly protected when one has got a reasonable/legitimate expectation to expect that his/her right must be observed in a given situation. The right to privacy has been developed on a case-by-case basis with the content of the right being defined differently and whether the right to privacy trumps the employer's right to monitor depends also on a case-by-case basis as discussed in this chapter.

---

[70] T Pistorious. Monitoring, interception and Big Boss in the workplace: is the devil in the details? (2009) PER vol.12 no.1 Potchefstroom. pg 3.

[71]PAK Le Roux. "Employment Practices in the Age of the Internet" (Unpublished paper delivered at the E-commerce and Current Commercial Law Workshop on 29 August 2003 at Sandton Johannesburg) pg 5.

[72] T Pistorious. Monitoring, interception and Big Boss in the workplace: is the devil in the details? (2009) PER vol.12 no.1 Potchefstroom pg 4.

[73] Ibid

[74] T Pistorious. Monitoring, interception and Big Boss in the workplace: is the devil in the details? (2009) PER vol.12 no.1 Potchefstroom pg 5.

Chapter 2:Legislation on Monitoring

2. Introduction

Together with the Constitutional provisions mentioned in chapter 1, there are a number of pieces of legislation which protect (and protected) the individual right to privacy in their communications by regulating the monitoring of Internet, telephone and E-mail communications in a direct or indirect fashion. Some of these legislations have now been repealed but are relevant to this paper so as to trace how legislation has evolved over the years so as to cater for the needs of the employee's right to privacy.

2.1 The Interception and Monitoring Prohibition Act (IMP) 127 of 1992:

The Act came into effect in February 1993, prior to the enactment of the Interim Constitution (1993). The stated purpose of the Act is both to prohibit the interception and monitoring of certain communications, and to provide for authorisation to do so in certain circumstances.

As indicated in its long title, the IMP Act is directed at prohibiting the interception of certain communications, monitoring certain conversations or communications, providing mechanisms for the interception of postal articles and communications as well as the monitoring of conversations or communications when a serious offence is committed or the security of South Africa is threatened. It states that its purpose is,

> [to] prohibit the interception of certain communication and the monitoring of certain conversations or communication; to provide for the interception of postal articles and communications and for the monitoring of conversations or communication in the case of a serious offence of if the security of the Republic is threatened.[75]

The purpose statement itself is proof enough that it applied to specific communications which were telephone and postal communications. The primary objective of the IMP Act is not crime prevention but the protection of confidential information from illicit eavesdropping.[76]
Section 2(1) of the IMP Act provides for the prohibition of interception and monitoring. This section states that:

[75]The Interception and Monitoring Prohibition Act 127 of 1992.
[76]N Bawa. The Regulation of the Interception of Communications and Provision of Communication Related Information Act. (2008) pg 297.

> No person shall intentionally and without the knowledge or permission of the dispatcher intercept a communication which has been or is being or is intended to be transmitted by telephone or any other manner over a telecommunication line; or intentionally monitoring any conversation or communication by means of a monitoring device so as to gather confidential information concerning any person, body or organization.[77]

In order to understand the extent of this prohibition we will have to consult the definitions of certain words in the provision. A 'telecommunication line' is extremely widely defined to include any apparatus, instrument, pole, mast, wire, pipe, pneumatic, or other tube, thing means which is or may be used for or in connection with the sending, conveying or transmitting or receiving of signs, signals, sounds, communication or other information.[78]This definition can be said to have been phrased wider than the purpose to include the electronic equipment, linking and distribution systems that serve to connect computers to one another.

A 'monitoring device' is defined as

> [A]ny instrument, device or equipment which is used or can be used, whether by itself or in combination with any other instrument, device or equipment, to listen to or record any conversation or communication.[79]

The prohibition contained in section 2(1)of IMP Act which relates to 'no person' and since the term is not defined in any manner can therefore be given its ordinary meaning to include, an employee(whether a natural or juristic person) or a representative of the employee. A judge has authority to give permission to monitor but must be convinced that a serious offence has been or is being or will be committed and cannot be investigated in any other manner.[80] The offence under investigation must have been committed over a lengthy period of time, on an organised or regular basis, or harm the country's economy.[81] A judge may only direct the interception or monitoring of an article or communication for three months at a time.[82] Any member of the SAPS executing a direction may enter into any premises to install a monitoring device, or to

[77] Act 127 of 1992: s 2 (1).
[78] Act 127 of 1992: s 1.
[79] Act 127 of 1992: s1.
[80] Ibid.
[81] Ibid.
[82] Ibid

intercept a postal article or communication.[83]Van Dokkuln[84]states that it is doubtful that this Act was ever intended to be used in the civil litigation context. Section 3 (2) of the IMP Act provides that any application to a judge for a directive shall be made by a police officer, or an army officer, or to member of the intelligence service.[85] Hefurther states that it would seem to be a clear indication that the IMP Act was intended to be used by only the police or the military, including the intelligence services and is not concerned with the interception or monitoring in the private sphere but is rather concerned with the gathering of evidence by public agencies during the investigation of a crime.[86]

Section 8 of the IMP Act provides for offences and penalties to those who contravened the provisions of section 2(1) of this Act. Offences and penalties are there to prevent violation of the Act's general provisions (section 2) or the secrecy provisions. A fine or imprisonment for a period not exceeding two-years is contemplated for violating section 2, and in the case of the `secrecy clause' contravention, a fine or imprisonment not exceeding five-years can be imposed.[87] The importance of obtaining the proper authority to monitor or intercept with strict adherence to procedure has been stressed in our courts and the validity of the directive can be automatically vitiated if not lawfully issued. This would not only constitute a criminal offence in terms of the Act, but also constitute an infringement of the right to privacy, which includes the right not to be subject to "the violation of private communications", as set out above.[88]

The South African Law Commission was of the view that since the promulgation of the ((IMP) Act, 127 of 1992 on 1 February 1993, there had been an increase in the use of advanced telecommunications technologies, including cellular communications, satellite communications, computer communications through e-mail, as well as the electronic transfer of information and

[83]M Schönteich *African Security Review, Volume 9 No 2, 2000.* (2000): South Africa's arsenal of terrorism legislation, African Security Review,9:2, 39-51.
[84] Ibid.
[85] Act 127 of 1992: s 3 (2).
[86]Ibid.
[87]Act 127 of 1992: s 8.
[88]*S v Naidoo 1998 (1) BCLR 46 (D)* at 72 E-F and *Protea Technology Ltd and Another v Wainer and Others 1997 (9) BCLR 1225 (W).*

data.[89] Furthermore, the considerable legal developments across the world regarding the interception of communications made a review of the IMP Act necessary.[90] The SALC was of the view that even though the IMP Act compares favourably with its counterparts in other countries, it does not deal adequately with new technology (eg, the IMP Act does not deal with the monitoring of employees' e-mail by employers).[91] For that reason the SALC recommended that it be substantially repealed and replaced with new legislation.

2.2. The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

The Regulation of Interception of Communications and Provision of Communication – Related Information Act ("RICPCIA"), also known to others as (RICA), IMP's successor, is concerned with interception in both the private and public spheres and applies to private sector employees and employers.

The scope of the application of RICA:

• to regulate the interception of certain communications;
• to monitor signals, radio frequency spectrum and the provision of communication-related information
• to regulate the making of application for, and the issuing of, directions authorising the interception of communications, entry warrants and the provision of communication-related information;
• to prohibit the provision of telecommunication services that do not have the capability to be intercepted;
• to provide for the establishment of interception centres, the Office for Interception Centres and the Internet Service Providers Assistance Fund;

[89]SA Law Commission. Project 124: *Privacy and Data Protection Report.* (2009) pg 26.
[90]Ibid.
[91]Ibid.

• to create offences and to prescribe penalties for such offences.[92]

The objectives of RICA are more far-reaching when compared with the IMP. Unlike the IMP, section 1 of RICA defines 'communication' as including both a direct communication (non-electronic) and an indirect communication (electronic).[93]It is clear from the objectives contained in RICA that, although its primary focus is assisting law-enforcement officers in procuring information required to combat crime, it also regulates interception and monitoring in the private sphere.

Section 1 of RICA defines 'intercept' as

> the aural or other acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of the communication available to a person other than the sender or recipient or intended recipient of that communication and includes the
>
> • monitoring of any such communication by means of a monitoring device;
> • viewing, examination or inspection of the contents of any indirect communication; and
> • diversion of any indirect communication from its intended destination to another destination.[94]

Section 2 of RICA provides that, no person may intentionally intercept or attempt to intercept or authorise or procure any other person to intercept or attempt to do so, at any place in South Africa, any communication in the course of its occurrence or transmission.[95] Any interception in contravention to section 2 may constitute a criminal offence, which carries a maximum fine of two million rands or a maximum term of imprisonment of 10 years.[96]

The same with the IMP, section 3(a) of RICA allows authorised persons to intercept any communication in accordance with an interception direction issued by a judge. Other exceptions to the prohibition of interception include:

[92] The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.
[93] Act 70 of 2002 : s1.
[94] Ibid.
[95] Ac 70 of 2002: s 2.
[96]Act 70 of 2002: s 49 (1).

• unintentional interception[97]

• interception by a party to the communications[98]

• interception with the written consent of one of the parties to the communications[99]

• interception of indirect (electronic) communications in the carrying on of any business[100]

• interception by certain law-enforcement personnel to prevent serious bodily harm[101]

• interception by certain law-enforcement personnel to determine the location of a person in an emergency[102]

• interception in a prison[103]

• monitoring of signals by persons responsible for installing, operating and maintaining equipment in carrying out such duties[104]and

• monitoring of the radio frequency spectrum by Icasa[105]

Section 6(1) of RICA provides for exception and section 6(2) sets out conditions that have to be met before the exception applies. Section 6(1) states that any person may, in the course of carrying on any business, monitor, intercept or examine any indirect communications. This section limits the meaning of an indirect communication to, the means by which a transaction is entered into in the course of that business[106] ,which otherwise relates to that business, [107] which otherwise takes place in the course of carrying on that business and in the course of its transmission over a telecommunication system.[108]Although section 6(1)(a) specifically refers to communication 'by means of which a transaction is entered into' and section 6(1)(b) specifically refers to communication that 'relates' to a business, section 6(1)(c) refers generally to

[97] Act 70 of 2002:s 2.
[98] Act 70 of 2002:s 4.
[99] Act 70 of 2002:s 5.
[100] Act 70 of 2002:s 6.
[101]Act 70 of 2002: s 7.
[102]Act 70 of 2002: s 8.
[103]Act 70 of 2002: s 9.
[104] Act 70 of 2002:s 10.
[105] Act 70 of 2002:s 11.
[106]Act 70 of 2002:section 6(1)(a) .
[107]Act 70 of 2002: section 6(1)(b).
[108] Act 70 of 2002: section 6(1)(c).

communication that takes place 'in the course of carrying on of that business'.[109] It is arguable that most (if not all) personal indirect communication of employees, employees make use of employers' communications systems, fall within the exception set out in section 6(1)(c) of RICA.

Section 6(2) (b) provides that a person may intercept an indirect communication as indicated above only if, the interception is for purposes of monitoring or keeping a record of indirect communications, in order to establish the existence of facts, for purposes of investigating or detecting the unauthorised use of the employer's telecommunication system[110] , or where it is undertaken in order to secure, or is an inherent part of the effective operation of such system.[111] Furthermore, monitoring indirect communications made to a confidential voice-telephony counselling or support service which is free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that users thereof may remain anonymous if they so choose.[112] This does not place an onerous obligation on the employer, nor does it limit the exception very much. As long as an employer understands that it may intercept e-mail only for one or more of the stated purposes, there should be no problem in meeting the condition. Section 6 specifically deals with the interception that occurs in connection with the carrying on of a business hence that's why it's relevant to this dissertation because the employer is carrying on a business.

RICA was drafted in response to the increasing diversity and developments in communication technologies, globalisation of the telecommunications industry, and the convergence of the telecommunications, broadcasting and information technology industries, which inter alia include satellites, optical fibres, computers, cellular technology, e-mail, surveillance equipment, and the electronic transfer of information and data. RICA sets out circumstances under which government entities and other persons may or must intercept or monitor conversations, cellular text messages, e-mails, faxes, data transmissions and postal articles, and establishes that in all

[109]Ibid.
[110] Act 70 of 2002: section 2(1)(b)(i).
[111]Ibid.
[112]Ibid.

other circumstances, such interception or monitoring is prohibited. In permitting such interception and monitoring, it is arguable that RICA does not provide adequate safeguards to protect the privacy of employees in the workplace. This may result in a number of provisions of RICA being susceptible to constitutional challenge. There is also the danger that the invocation of the provisions of RICA, both in the employment context and by law-enforcement officers, may be abused in a manner that is inconsistent with the right to privacy and freedom of expression enshrined in the Constitution. RICA permits greater latitude for the interception and monitoring of communication than was permitted in the IMP Act. It makes detailed provision for the State to intercept and monitor communications. RICA also places onerous obligations (financial and otherwise) on the .private telecommunications industry to assist the State in its interception and monitoring of communications.

2.4. Electronic Communication and Transactions Act 25 of 2002

The main objective of the Electronic Communication and Transactions Act (ECTA) is 'to enable and facilitate electronic communications and transactions in the public interest'. [113] The definitions of this act are essential to the research paper. 'Electronic communications' is defined in the ECT Act as 'a communication by means of data messages'.[114] In addition, 'data' is defined as 'electronic representations of information in any form'.[115] 'Transaction' is defined as 'a transaction of either a commercial or non-commercial nature, and includes the provision of information and government services'.[116] The ECT Act does not limit the operation of any law that expressly authorizes, prohibits or regulates the use of data messages.

The aims of the ECT Act, as provided for in section 2(1) are, inter alia:

• to remove barriers to electronic communications and transactions in the Republic;

[113] Act 25 of 2002:s 2(1) .
[114] Electronic Communications and Transactions Act 25 of 2002.
[115] Ibid.
[116]Act 25 of 2002: s1.

• to promote legal certainty and confidence in respect of electronic communications and transactions;
• to promote technology neutrality in the application of legislation to electronic communications and transactions; and
• to ensure that electronic transactions in the Republic conform to the highest international standards.

'Data message' is defined as data generated, sent, received or stored by electronic means and includes voice where the voice is used in an automated transaction and a stored record.[117]Section 15 of the ECT Act provides that:

> (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence — on the mere grounds that it is constituted by a data message; or if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
> (2) Information in the form of a data message must be given due evidential weight.[118]

This signifies that e-mail messages have an evidential weight in both civil and criminal proceedings.[119] This is particularly important for employer — employee relations when the relationship terminates.[120] Archived e-mail messages may come in useful as evidence for either the employer or the employee in workplace-related disputes.[121]

Section 50(1) provides that the chapter on the protection of personal information applies only to personal information that has been obtained through electronic transactions.[122]

Section 85 defines 'cyber crime' as the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not authorised to access that data and still continues to access that data.[123] This is relevant to this discussion since cyber crime is one of the reasons why

[117]Ibid
[118]Ibid: S 15 (1).
[119] L Shumani. Gereda The Electronic Communications and Transaction ACT pg 271
[120] Lbid.
[121]L Shumani. Gereda The Electronic Communications and Transaction ACT pg 271
[122]Act 25 of 2002: s50 (1).
[123]Act 25 of 2002: s85.

employer monitors employee. Section 86(1) provides that, subject to the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.[124]In the case of *Douvenga*[125] the court had to decide whether an accused employee GM Douvenga of Rentmeester Assurance Limited (Rentmeester) was guilty of contravention of section 86(1) (read with sections 1, 51 and 85) of the ECT Act. It was alleged in this case that the accused, on or about 21 January 2003, in or near Pretoria and in the district of the Northern Transvaal, intentionally and without permission to do so, gained entry to data which she knew was contained in confidential databases and/or contravened the provision by sending this data per e-mail to her fiancée.[126] In the *Rabie*[127] case which was quoted by the *Douvenga* case it was held that, it seemed clear that an act done by a servant solely for his own interests and purposes, although occasioned by his employment, may fall outside the course or scope of his employment and that in deciding whether an act by the servant does fall within the course and scope of employment, some reference is to be made to the servant's intention. The *Douvenga* case went on to hold that the accused could not give any explanation to the Court when asked about her reasons to access and send the information to another computer.[128] The Court therefore concluded that the accused was on a frolic of her own when she gained access to Rentmeester's databases and that Rentmeester could therefore not be held responsible (vicariously liable) for her actions.[129] The Court observed that the information remained confidential information that only Rentmeester had exclusive use over.[130] It was further observed that the information and the data subject were attached to one another and had to be handled by the data controller in a manner that complies with section 51(4) of the ECT Act.[131] The accused was found guilty of contravening section 86(1) of the ECT Act and sentenced to a R1 000 fine or imprisonment for a period of three months

[124]Act 25 of 2002: s 86.
[125]*Die Staat v M Douvenga (née Du Plessis)* (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003, unreported).
[126] Ibid.
[127]*Minister of Police v Rabie1986 (1) SA 117 (A)*.
[128]*Die Staat v M Douvenga (née Du Plessis)* (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003, unreported).
[129] Ibid.
[130] Ibid.
[131] Ibid.

2.5. The Electronic Communications and Transactions Act Amendment Bill 2012:

The Electronic Communications and Transactions Act, 2002, (ECT), has been in place for a decade. During all this time, the ECT Act has functioned well in all areas, providing for consumer protection ahead of the introduction of the Consumer Protection Act, 2008, and heralding the important notions of privacy and data protection. Be that as it may, in the decade since its introduction, the world has seen significant changes in the electronic communications sector, affecting use of the internet. Social media over the internet and other forms of communications have revolutionized communication, removing physical barriers to communications and the sharing of information.[132] As a consequence of the exponential growth in electronic transactions and our dependence on the internet, we have experienced a significant increase in hacking, security breaches, data mining for economic purposes, misuse of personal information, cyber security threats and cyber crime.[133]

Chapter VIII deals with the protection of personal information. Much work has been done in relation to new legislation to deal with personal information and privacy and the protection of state information for example the Protection of Personal Information Act 4 of 2013. As a result, this chapter has not been amended and awaits the new legislation. Section 50(2) of the ECT Act 25 of 2002 which provides that the principles governing the processing of electronically collected personal information are voluntary has been amended in order to make the principles obligatory because the voluntary principles do not give effect to the right to privacy provided for in the Constitution. In relation to definitions, "personal information" has been amended to reflect the proposed definition in the new Bill on personal information.[134]

2.6. Protection of Personal Information Act 4 of 2013:

Privacy and data protection legislation provides for the legal protection of a person in instances where his or her personal information is being collected, stored, used or communicated by another person or institution. The protection seeks to uphold the right to privacy as protected by

[132] The Electronic Communications and Transactions Act Amendment Bill 2012.
[133]Ibid.
[134]Ibid.

section 14 of the Constitution of the Republic of South Africa, 1996 (the Constitution), and other International Human Rights instruments. The Protection of Personal Information Act 4 of 2014 from here onwards written as (POPI) is, in many respects, similar to its United Kingdom (UK) counterpart, the Data Protection Act 29 of 1998 (DPA), which makes provision for the regulation of information relating to individuals, including the obtaining, holding and use or disclosure of such information. The DPA has dramatically affected the law in the UK and POPI is expected to have a similar effect in South Africa. Two of the main purposes of POPI are to give effect to the constitutional right to privacy(s 2(*a*)) and to regulate the manner in which personal information is processed (s 2(*b*)).[135] POPI is an attempt to bring South Africa in line with global trends of data protection.

Mention is only made to the definitions that are relevant to the scope of this paper. 'Personal Information' is defined as information relating to natural and juristic persons which includes:

•information relating to the race, gender, sex, pregnancy, marital status, nationality, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

•information relating to the education or the medical, financial, criminal or employment history of the person;

•any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person;

•the blood type or any other biometric information of the person;

•the personal opinions, views or preferences of the person;

•correspondence sent by the person that is of a private or confidential nature;

•the views or opinions of another individual about the person; and

•the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.[136]

[135]Protection of Personal Information Act 4 of 2013: s 2(a) and s 2(b).
[136]Protection of Personal Information Act 4 of 2013: s 1.

POPI only applies to Personal Information that is processed so the definition of processing is important. Processing includes collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alteration, use, dissemination, merging.[137]POPI will not apply in instances where processing of personal information is for purely personal or household activities. This is a broad application compared to what has been known throughout the years due to our case law that the right to privacy is mainly recognised in one's intimate sphere or private life. The Bill will also not apply to the state when it is involved in matters pertaining to national security, defence or public safety. POPI Act does not apply to journalistic purposes as long as it is subject to a code of ethics and has sufficient safeguards in place.

The POPI Act in brief─

(i) is a general information protection statute;

(ii) is applicable to both the public and private sector;

(iii) covers both automatic and manual processing; and

(iv) will protect identifiable natural and juristic persons.[138]

Chapter 3 of the Act deals with the conditions for the lawful processing of personal information and consists of Part A (processing of personal information in general), Part B (processing of special personal information) and Part C (processing of personal information of children).[139]Another welcome development is the formal introduction of information security to South African law with the introduction of Chapter 3: condition 7. This is the first time that information security has directly been addressed in any South African legislation. Condition 7 introduces requirement around security measures having to be introduced to secure the integrity of personal information as well as the requirement to notify third parties of a breach of security. This is the first of many evolving and current information security trends in our law.

[137] Ibid.
[138] C, Budricks. SAICA: Summary on the Protection of personal Information Bill of 2009. Published 14 August 2012.
[139]Protection of Personal Information Act 4 of 2013: Chapter 3.

The POPI Act is aimed at giving effect to South African citizens' constitutional right to privacy. This is going to be achieved through:

• Providing for the rights of data subjects with regard to their ability to protect their personal information as it is processed by public or private bodies, as well as giving data subjects remedies they can use should those rights be infringed.[140]

• Providing a framework that sets out the minimum conditions that must be met when personal information is processed by organisations, whether they are public or private.[141]

• Establishing an Information Protection Regulator, whose primary purposes will be to promote awareness of the rights of data subjects when it comes to protecting their personal information, as well as enforcing the requirements of the Bill.[142]

The POPI Act pursues a balanced approach to the protection of personal information, mandating due regard for the justifiable limitations of the right to privacy, the need to secure the interests of free flow of information and managing the tensions between the rights of access to information and protection of personal information.[143]

<u>The provisions of the Protection Of Personal Information Act 4 of 2013 that are relevant to this paper:</u>

The "pre-emption" provisions of the Act in section 3, state that any other legislation that is stricter than the Act must still apply, meaning that a Privacy Officer cannot rely solely on the Act for the development of their privacy program they must look to other stricter monitoring legislation to assert their privacy.[144] Consideration will have to be given to legislation such as the Consumer Protection Act, the Promotion of Access to Information Act, the Companies Act, to name just a few of the other pieces of legislation that make up the South African regulatory universe.

[140] Protection of Personal Information Act 4 of 2013: "long title".
[141] Ibid.
[142] Ibid.
[143] Opland R, Chetty P & Botton J. Protection of Personal Information Bill of 2009 Survey: The Journey to Implementation.www.pwc.com/za, November 2011 pg 1-40.
[144] Protection of Personal Information Act 4 of 2013: s 3

Section 10 requires responsible parties to obtain consent from a data subject prior to processing his information.[145] This can be achieved through privacy notices on websites and contracts.

Section 13 requires organisations to delete personal information that is no longer required, unless it needs to be retained by law, for the purposes of a contract between the organisation and the data subject or if the data subject has given his/ her consent to the information being retained.[146] This requirement has been conceived to be problematic in the future, given the multitude of legislation that requires records to be kept for differing periods of time.[147] Section 13(2) also states that personal information may be retained for "historical, statistical or research purposes".[148] It has been submitted that this wording may be open to interpretation, and that organisations may retain personal information for 'research', which may be their own marketing research.[149]

Section 17 of POPI requires organisations to explain to a data subject what his/ her information is being used for.[150] It has been argued that, given the many purposes for which organisations use personal information once it has been collected, how will this be meaningfully communicated to the data subject at the time of collection?[151]

Section 22 of POPI implies that data subjects will be able to ask organisations whether the organisation stores or processes any of their personal information, and can submit a request to have that information deleted.[152]Section 22 further allows a data subject to request access to his/ her information held by a responsible party.[153]

[145]Protection of Personal Information Act 4 of 2013: s 10.
[146]Ibid at s 13
[147]Opland R, Chetty P & Botton J. Protection of Personal Information Bill of 2009 Survey: The Journey to Implementation.www.pwc.com/za, November 2011 pg 1-40.
[148]Protection of Personal Information Act 4 of 2009: s 13 (2).
[149]Opland R, Chetty P & Botton J. Protection of Personal Information Bill of 2009 Survey: The Journey to Implementation.www.pwc.com/za, November 2011 pg 1-40.
[150]Protection of Personal Information Act 4 of 2013 : s 17
[151]Protection of Personal Information Bill of 2009 Survey: The Journey to Implementation. November 2011. pg 33.
[152]Protection of Personal Information Act 4 of 2013: s 22.
[153] bid.

Just like its counter parts for example RICA and the ECT Act which require consent for the interception of information, POPI under s71(1) prohibits using electronic communications for direct marketing unless the data subject has given his/ her consent or is a customer of the responsible party.[154] Section 71(2) permits an organisation to approach a data subject once in order to obtain their consent.[155]

Section 34 allows for the Regulator to authorise the processing of personal information even in situations where the processing does not comply with the requirements of the POPI Act.[156] Unlike in the RICA and other Acts on information privacy which grants discretion on the judge to decide when to allow an exception for interception, POPI awards this authority to the Regulator.

In conclusion the enactment of the POPI Act is going to bring a significant level of protection to individuals and organisations in South Africa with regard to how their personal information is handled. Unlike recent years legislation , individuals will have the ability to hold organisations to account for the actions that are taken regarding personal information. From the perspective of an individual, this legislation is welcome but from the perspective of the organisations that will have to amend systems, processes and policies in order to comply with the legislation, however, this Act may have a significant impact on the way that they do business. The Regulator has a task ahead of him, especially given the heavy compliance burden that organisations already carry to the extent that , it may initially be wise for the Regulator to focus on awareness and training of organisations, educating rather than enforcing in the beginning.

[154] Protection of Personal Information Act 4 of 2013: s71.
[155] Ibid.
[156] Ibid at s 34.

Chapter 3: Reasons why the employer monitors the internet, email and telephone corresponding of the employee

3. Introduction

The internet, telephone and email are indispensable tools of business in the workplace so the employer cannot do without them but he/she will have to guard against the potential risk of civil or criminal liability brought on by the employee through misuse of these tools. In certain circumstances the employer has a duty to monitor employee electronic transmissions but it must be for a legitimate purpose. There are various reasons why an employer may wish to monitor the internet and some of these reasons are discussed below.

3.1 Vicarious liability

Our law recognises the doctrine of vicarious liability in terms of which one person can be held liable to a third party for the edictal acts performed by another which caused loss to that third party.[157]Vicarious liability is a doctrine of liability without fault in terms of which one person is held liable for the unlawful acts of another.[158] It is a strict liability, or liability without fault, on the part of the defendant and is additional to that of the other person's delict. Vicarious liability is based on social policy regarding what is fair and reasonable and amounts to an expression of a society's legal convictions that victims of a delictual conduct should be able to recover damages from someone who has the ability to pay.[159]For vicarious liability to be incurred there must be a special relationship between the two persons and one such important relationship is the employer-employee relationship. Under this doctrine an employer may be held liable to a third party for the delictual acts performed by employees.[160]The rational for this doctrine is for the third party to enjoy fair and full compensation for his loss by suing the person who is able to compensate him properly and who should have taken adequate measures of competence not to employ the employee who has caused loss to the third party.[161]Although vicarious liability has its origin in the law of delict it has developed as a general labour law principle that the employer

[157]JC Van der Walt & JR Midgley .*Principles of Delict*.3ed. (2005) pg 36.
[158]Ibid.
[159]Ibid.
[160]ME Manamela. *Vicarious liability: paying for the sins of others:case comments*. (2004) 16 (1) SA *Merc LJ* pg126.
[161]K Calitz. *Vicarious liability of employers: reconsidering risk as the basis for liability*. (2005) 2 *TSAR* pg 215.

will be liable for the delicts committed by its employees. Basson[162] states the following as issues that should be considered in order to constitute employer's liability;

a) there must be a contract of service between the employee and the employer at the

time the employee carries out an unlawful act,

b) the conduct of the employee must have been unlawful to the extent that the requirements for a delict must be meet and,

c) the employee must have acted in the course and scope of the employee's duties orservice. [163]

For these requirements to be satisfied, especially the third requirement, these acts must be committed by the employee in the exercise of the functions to which he/she was appointed, including such acts as are reasonably necessary to carry out the employer's instructions. This is further explained by,

> The standard test for vicarious liability of a master for the delict of a servant is whether the delict was committed by the employee while acting in the course and scope of his employment. The enquiry is frequently said to be whether at the relevant time the employee was about the affairs, or business, or doing the work of the employer…[164]

According to Mischke[165]it is a principle of our common law that an employer may be held jointly and severely liable with an employee for an employee's wrongful acts committed in the course and within the scope of the employees' duties. The issue is clearly illustrated by Rycroft[166]when he states that, the employer may not be able to escape liability merely because the act was intentional on the part of the employee, amounted to criminal conduct or was specifically prohibited by the employer. Paterson, states that activities that may create legal liability include the downloading or distribution of copyright material, the posting of defamatory material on

[162] Basson et al Essential Labour Law (vol l) Individual Labour Law (1998) pg 50.
[163] Ibid.
[164]*Minister of Law and Order v Ngobo1992 4 SA 822 (A)* see also *Minister of Safety & Security v Jordaan t/a Adre Jordaan Transport 2000 (4) SA 21 (SCA)* at 24H-25E.
[165] C Mischke. "Disciplinary action and the internet: responding to employee abuse of e-mail, network access and internet access". (1999) 12 *CLL* pg 46.
[166] Rycroft & Jordan. A Guide to SA Labour Law2 ed (1992) pg 86.

bulletin boards and the circulation of defamatory material on bulletin boards.[167] To substantiate his position he refers to a case in which a Chevron Corporation paid out $2.l2 million to settle a sexual harassment case brought by female employees as a result of an email titled 'why beer is better than women'.[168]An employer stands to be held liable for wrongful activities committed by an employee's internet and network related acts regardless of the fact that an employer had specifically prohibited those acts. The question that begs to be answered is whether an employee acted within the scope of his or her duties.

The question whether the act falls within or outside the scope of employment is not without problems and the answer has been described as a question of law, but it has also been said that each case will depend on its own facts. In determining whether an employee's actions fall within the scope of his or her employment and therefore renders the employer vicariously liable, both a subjective test and an objective test may be applied.[169]The consequence of these tests is that an employer will be able to escape liability only if the employer can prove that the employee's intention was to solely promote his or her own interests (the subjective test) and that the employee had completely disengaged himself or herself from the affairs of the employer when committing the delict (the objective test).In *Viljoen v Smith*[170]the employee, although prohibited by his employer, climbed through a fence and walked some 70 meters onto the third party's farm to relieve himself. While doing so, he lit a cigarette and caused a fire. The Court held that the employee had not abandoned his place of work and that he was still acting within the course and scope of his employment.[171] This indicates that the mere existence of a digression does not automatically result in the employer not being found vicariously liable for the delict of an employee.[172]Although the employee had disobeyed the employer's instruction, the employer was held to be vicariously liable because employee was still engaged in the business of the employer. The employer's liability depends on the nature of the digression and the surrounding circumstances.

3.2 Defamation:

[167]M Paterson . "Monitoring of Employee Emails and Other Electronic Communicatins" (2002) 21 (1)University of Tasmania: Law Review 1, 2.
[168]Ibid.
[169]*Minister of Police v Rabie (1986 (1) SA 117 (A).*
[170]1977 (1) SA 309 (A).
[171]Ibid.
[172]Ibid.

Defamation is the unlawful, intentional, publication of defamatory words or conduct referring to the plaintiff which causes his reputation to be impaired.[173]In order to determine whether the contents of an e-mail are defamatory, it must first be ascertained whether a reasonable person of ordinary intelligence may reasonably understand the e-mail to contain a defamatory meaning as regards the plaintiff.[174]For an employer to be liable for defamatory e-mail sent by an employee in the course of his or her employment, the requirement of publication must be met. As to what constitutes publication on the Internet was illustrated in *National Media v Bogoshi*[175] which stated that publication is the act of making known a defamatory statement or the act of conveying an imputation by conduct, to a person or persons other than the person who is the subject of the defamatory statement or conduct.[176] It has been submitted that, it can be inferred from this statement that the following acts will amount to publication: postings to a newsgroup, sending an email, making a website available on the internet, internet relay chat and file transfer by file transfer protocol.[177]In*CWU v Mobile Telephone Networks (Pty) Ltd*[178] it was evident that liability for defamation can result in vicarious liability for a company. This case concerned a derogatory e-mail sent by one of the employees of MTN. The e-mail contained allegations that MTN's management was corrupt and that they show favouritism to a certain temporary employment agency. MTN charged the employee with: (i) intentional circulation of an email insinuating that MTN management was corrupt; (ii) intentionally and disrespectfully engaging in abusive and insulting language in that he insinuated that management were fat cats; (iii) making unfounded allegations against management by insinuating in the email that management was benefiting from recruitment processes; (iv) bringing the company's image into disrepute in that he circulated the email to MTN employees; and (v) intentionally conducting himself in an insubordinate manner in that the email contained derogatory remarks against MTN management

[173]C Mischke. "Disciplinary action and the internet: responding to employee abuse of e-mail, network access and internet access". (1999) 12 *CLL* pg46.
[174]JM Burchell. *The Law of Defamation in South Africa* (1985) pg35.-: The meaning of the words published , allegedly defamatory material is determined by establishing whether: ― a reasonable person of ordinary intelligence might reasonably understand the words to convey a meaning defamatory to the plaintiff … The test is an objective one … the reasonable person of ordinary intelligence is taken to understand the words alleged to be defamatory in their natural and ordinary meaning… the Court must take account not only of what the words expressly say , but also of what they imply.
[175]1998 4 SA 1195 (SCA).
[176]Ibid.
[177]V Etsebeth. *The growing expansion of vicarious liability in the information age (part 2)*. (2006) 4 *TSAR* pg755.
[178]2003 8 BLLR 741 (LC).

and clients.[179] The court found that the employee had failed to comply with the procedure established by MTN for reporting allegations of fraud, and that he was seeking a wider audience in the form of MTN management and employees.[180] His email therefore increased the damage to the reputation of MTN and his actions therefore justified a defamation suit against him. The court held that in addition, there were grounds on which the clients of MTN could institute a vicarious liability suit against MTN.[181]A court can find that in providing an employee with tools to access the internet and email facilities, the employer is directly liable as a publisher or disseminator of the offending statement. Employers that decide not to regulate publication of material on the internet by their employees could be potentially exposing themselves to a possible claim for negligence on grounds that they owed a duty of care to their employees and third parties to impose some restrictions. From the above therefore it is accurate to conclude that if a defamatory statement is posted on a Usenet newsgroup or where the email is sent to a person other than the person who is defamed in the message, the requirements of publication would have been met.[182] Where an e-mail/s is used as the medium for defamatory remarks in the workplace it is important to remember that the defamation will probably occur at the place where the offending material is accessed.

3.3 Sexual Harassment and Discrimination

It is a well known fact that sexual harassment can occur through electronic means therefore creating a need for the employer to monitor employees' electronic transactions. Sexual harassment may take the form of coarse jokes sent via e-mail, pornographic screen-savers and crude graphics. Racial and religious discrimination cases can also be based on offensive electronic content, regardless of the sender's intentions.[183] Parliament and our courts have sought to protect employees who are victims of sexual harassment by imposing certain obligations that may render the employers liable as to curb the rising of sexual harassment claims in the workplace. [184] Employers are under a legal duty to prevent discriminatory acts being

[179] Ibid.
[180] Ibid.
[181] Ibid.
[182] V Etsebeth. *The growing expansion of vicarious liability in the information age (part 2)*. (2006) 4 *TSAR pg*755.
[183] Ibid.
[184] S Gule. *Employers'vicarious liability for sexual harassment*. (2005) 13 (2) *JBL* pg 66.

perpetrated against their employees. This was illustrated in the case of *Media 24*[185], where Farlem JA held that an employer has a legal duty that is dictated by public policy to prevent harm such as sexual harassment to its employees. In terms of section 5 of The Employment Equity Act 55 of 1998 (EEA) an employer is under an obligation to combat unfair discrimination in the workplace which is stated by, "Every employer must take steps to promote equal opportunity in the workplace by eliminating unfair discrimination in any employment policy or practice."[186]

Harassment can generally be defined as any humiliating or degrading treatment of a person because of their personal characteristics.[187] Harassment is a form of unfair discrimination and is prohibited in the workplace. [188] Harassment in any form is treated in the EEA as a form of unfair discrimination. The most common form of harassment in the workplace is sexual harassment.[189] An employer who fails to prevent or put an end to a sexual harassment complaint may be held liable.[190] The Code of Good Practice on the Handling of Sexual Harassment Cases states that sexual attention will become harassment if it is,

(a) persistent, although a single incident of harassment can constitute sexual harassment; and/or,

(b) the recipient has made it clear that the behaviour is considered offensive; and/or,

(c) the perpetrator should have known that the behaviour is regarded as unacceptable.[191]

---

[185] 2005 JDR 738 (SCA) pg 741.
[186] Employment Equity Act 55 of 1998: s 5.
[187] Ibid.
[188] Act 55 of 1988: s 6 (3).
[189] M Van Jaarsveld. *Forewarned is Forearmed: Some Thoughts on the Inappropriate Use of Computers in the Workplace*. (2004) 16 (4*) SA Merc LJ* pg 661.
[190] Section 60 of the EEA 55 of 1998 - which regulates the liability of employers for the conduct of their employees committed while the employees are at work. If the conduct complained of is brought to the employer's attention, the employer is obliged to take the necessary steps to eliminate the alleged conduct and to comply with the EEA. Section 60(3) renders the employer vicariously liable for the conduct of an employee who contravenes the provisions of the EEA. It states: "If the employer fails to take the necessary steps referred to in sub-section (2), and it is proved that the employee has contravened the relevant provisions, the employer must be deemed to have contravened that provision." Section 60(3) deems the employer to have contravened the provisions of the applicable section if he/she fails to take the necessary steps referred to in subsection (2), and if it is proved that the employee has contravened the relevant provision. An employer is not liable for the conduct of an employee ―if that employer is able to prove that it did all that was reasonably practicable to ensure that the employee would not act in contravention of this Act (section 60(4)). Steps that may be taken are set out in sub-section (2) – that is, the relevant parties must be consulted and the ―necessary steps taken.
[191] Code of Good Practice on the Handling of Sexual Harassment Cases, section 3 (2) (a- c).

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

In the case of *Ntsabo v Real Security CC*[192]; Ms Ntsabo was employed as a guard with Real Security CC. Ms Ntsabo, a single mother, found herself stationed at Khayelitsha Day Hospital. She reported to a supervisor who turned out to be worse than a mere groper.[193] On one occasion the supervisor all but raped her, and then threatened to shoot her if she told anybody about the incident. After resigning, she approached the Labour Court for relief, claiming compensation for an automatically unfair dismissal and damages for future medical costs and humiliation, impairment of dignity, pain, suffering, emotional trauma and the loss of the normal amenities of life.[194] All this relief was sought against her former employer.[195] The court had to consider whether the employer Real Security was liable for making the continued employment of Ms Ntsabo intolerable, even though the cause of the intolerable situation was due to the conduct of an employee of Real Security (the supervisor), who, while he may have harassed the employee during working hours, could hardly be said to have been acting in the course and scope of his duties.[196] The court held that an employer can only be held liable for the conduct of one of the employees if the employer created an intolerable situation by failing to prevent one of its employees from creating and perpetuating an intolerable situation for another and further that an employer can only be held to have failed to prevent an employee from creating and maintaining an intolerable situation for another if it (or its management) was aware of the situation and did nothing about it.[197] Pillay AJ held that Ms Ntsabo had done all that could reasonably be expected of her to attempt to hold onto her employment and avoid being sexually harassed.[198] The employer had brushed aside her complaint. This inaction was held to be unfair and had created an intolerable working environment for Ms Ntsabo.[199] Her resignation accordingly constituted a constructive dismissal.[200] The EEA now gives the Labour Court power to grant compensation and/or damages to employees who are victims of discrimination on various grounds cited in the

[192][2004] 1 BLLR 58 (LC).
[193]Ibid.
[194]Ibid.
[195]*Ntsabo v Real Security CC [2004] 1 BLLR 58 (LC).*
[196] bid.
[197]Ibid para 98 H-I.
[198]Ibid.
[199]Ibid.
[200]*Ntsabo v Real Security CC [2004] 1 BLLR 58 (LC)* para 93 A-C.

Act.[201] On the sexual harassment issue, the court found that the senior employee of the corporation had contravened section 6(3) of the EEA and that the corporation was liable for the conduct of such employee in contravening the Act.[202] The Labour Court exercised its power in terms of section 50 to award compensation and damages in respect of unfair discrimination, it awarded Ntsabo R20 000 for future medical costs, and R50 000 as general damages.[203]

3.4. Gender and Racial Issues

If an employee engages in sending material which has gender or racial sensitive contents it may have serious implications for both the company and the employee who sent the mail. A sexual harassment claim and a racial discrimination claim can be directed to both the employee and employer. In *Cronje* v *Toyota Manufacturing* [204]an employee was dismissed as a result of a racist cartoon distributed at the workplace. The applicant received an e-mail which he printed out to other colleagues at a meeting.[205] The e-mail consisted of a cartoon depicting an adult and a young gorilla, both with the head of President Mugabe of Zimbabwe superimposed on them.[206] The caption stated 'we want to grow more bananas'.[207] He defended himself by stating that he did not regard the cartoon as racist but rather as a depiction of Zimbabwe as a banana republic.[208] The human resources manager deposed that the respondent's internet and e-mail usage code specifically outlawed the display and or transmission of any offensive racial, sexual, religious or political images documents on any company system.[209] The factory employed 3500 blacks and 1000 whites so race related issues were very important on the factory floor and black employees were upset by the cartoon.[210] The Commissioner found that it was reasonable to include a rule prohibiting the distribution of racist and inflammatory or offensive material in the company's

[201]Employment Equity Act 55 of 1998 (see sections 50(1) (d) and (e), read with sections 50(2) (a) and (b)), which specifically includes ―harassment‖ (section 6(3)).
[202]*Ntsabo v Real Security CC [2004] 1 BLLR 58 (LC).*
[203] Ibid.
[204]*Cronje v Toyota Manufacturing (2001)22 ILl735 (CCMA).*
[205] Ibid.
[206] Ibid.
[207] Ibid.
[208] Ibid.
[209] Ibid.
[210] Ibid.

code and that the applicant was aware of the rule which was consistently applied.[211] The Commissioner found the dismissal to be fair.[212]

3.5. Viewing of Pornography

Pornography is easily accessible on the Internet. Certain forms of on-line pornography (also referred to as cyber porn) constitute cyber crime and may be prosecuted in terms of the Films and Publications Act 65 of 1996 (hereafter referred to as the Act).[213] The Act is the principal statute governing online pornography in South Africa.[214] Section 2 of the Act outlines the objects of the Act as follows:

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

(b) to make the exploitative use of children in pornographic publications, films or on the Internet punishable. [215]

Section 1 of the Act defines publication as inter alia (i) computer software which is not a film; and (ii) any message or communication, including a visual presentation, placed on any distributed network including but not confined to the Internet.[216] Most forms of pornography on the Internet can be classified as publications, with the exception of a pornographic video clip, which could rather be classified as a film due to the fact that the definition of film includes ―images (that) can be capable of being seen as a moving picture.[217] Section 27 of the Act specifically deals with child pornography and the offences under it have been categorised into three types :(a) Offences dealing with the actual perpetrator; (b) failure to report knowledge of the commission of an offence referred to in paragraph (a); and (c) failure to prevent access to

[211]Ibid.
[212]Ibid.
[213] M Watney. *Regulation of Internet pornography in South Africa (1)*. 2006 (69) *THRHR* pg 227-228.
[214] Ibid.
[215] Films and Publications Act 65 of 1996; s 2.
[216] Film and Publications Act 65 of 1996; s1.
[217] Ibid.

certain materials. [218] In most cases the employer will be held liable under offences b and c. Section 27 (1) makes it an offence for any person to be in possession of, create, distribute, import or knowingly export or takes steps to export a film or publication which contains child pornography or which advocates, advertises or promotes child pornography or the sexual exploitation of children.[219] In terms of s 30 (1A) contraventions of s 27 (1) are punishable with a fine or imprisonment for a period not exceeding 10 years. [220] Section 27 (2) (b) places a duty upon any person who has knowledge of an offence under section 27 (1) or has reason to suspect that such an offence has been or is being committed to report that offence or suspicion of that offence to the South African Police Service. Internet Service Providers (ISP's) have a vital role to play with regards to the accessibility of the Internet because failure to do so the wrong will be imputed on them. Ignorance is not a defence to the ISP whose services are used for the hosting or distribution of child pornography. Section 27 A is specifically aimed at regulating the duties and responsibilities of ISPs in relation to child pornography and was placed in the statute book by the second Films and Publications Amendment Act 18 of 2004. Every ISP is required to take all reasonable steps to prevent the use of its services for the hosting or distribution of child pornography.[221] Section 30B (l) (b) provides that if in any prosecution in terms of the Act access was gained or attempted to be gained to child pornography on a distributed network, including the Internet, by means of access provided or granted to a registered subscriber or user, it shall be presumed, in the absence of evidence to the contrary which raises reasonable doubt, that such access was gained or attempted to be gained by the registered subscriber or user.[222]Section 30B maintains that employers must ensure that their employees are not engaged in the creation, production, distribution and possession of pornographic material because the unlawful conduct can be imputed on the company itself although in actual fact it's not the actual wrongdoer but due to the fact that it owns the tools it is responsible for the material on company computers and e- mail systems. It is submitted that the implications of s 30 B (1) and S 30 B (1) (b) are crucial

[218] Act 65 of 1996; s 27 (a) – (c).
[219] Ibid.
[220] Act 65 of 1996; s 30 (1A) & s 27 (1).
[221] s 27 A (2) (a) – (c).
[222] Inserted by the second Films and Publications Act 18 of 2004.

to the business and reputation of the company because the company brand is ultimately tarnished.[223]

3.6. Intellectual Property

Electronic content is subject to copyright. In terms of South African copyright law, copyright is the right given to the owner of certain types of works not to have his/her work copied without authorisation.[224] Work is copyrighted when it has been created by the author's original skill and effort and has been reduced to material form and is therefore not merely an idea.[225]Copyright is protected in South Africa in terms of the Copyright Act 98 of 1978 (hereafter referred to as the Act). Copyright gives the owner the right to prevent the unauthorised reproduction of his/her work as well as protection against the commercial exploitation.[226] In terms of the Act, two forms of copyright infringement can take place, namely direct and indirect infringement.[227] In South Africa, one does not have to register copyright (as is the case with other forms of intellectual property, such as patents or trademarks). A copyright situation will arise automatically as soon as something tangible is produced as a result of the author's original skill and effort.[228] Once an expression is entered into a computer in a form that can be read on a screen, it is considered fixed in a material medium even if it is never printed out or saved to a disk.[229] Therefore employees surfing web sites are not entitled to freely copy and distribute content obtained from those web sites owned by companies without obtaining prior permission.[230] This extends to copying images and text found on the web site. The World Wide Web now makes it possible to download magazine articles, reports, song titles, videos and photographs, all of which are protected by copyright. A computer software program placed on the Internet can also be downloaded at sites around the world and re-posted.[231] This has obviously created numerous problems for publishers and a potential nightmare for the creators of articles, songs, software and films, as the owners

[223] M Watney. ―Regulation of Internet pornography in South Africa (2) ‖. 2006 (69) *THRHR* 385-386.
[224] GJ Lidovho. *The internet and the piracy of copyrightable computer software in South Africa: some comparative perspectives*. (2006) 123 (2) *SALJ* 339.
[225] Ibid.
[226] V Etsebeth. *The growing expansion of vicarious liability in the information age (part 2)*. (2006) 4 *TSAR* 755 at 761.
[227] Ibid.
[228] Ibid.
[229]Ibid.
[230]Ibid.
[231] V Etsebeth. *The growing expansion of vicarious liability in the information age (part 2)*‖. (2006) 4 *TSAR* 755 at 761.

will want to protect their materials. While there are steps and measures being put in place by operators and creators to protect the content of their web sites against indiscriminate copying, there is a large amount of online content that is not technically protected against copying.[232] This being the case, there is a serious potential for loss that could arise for corporate employers where such copying is conducted by their employees.[233] If an employee ignores these stipulations, he/she will expose the company to vicarious liability for copyright infringement.

3.7. Performance Monitoring

It is alleged that surveillance of usage of the e-mail and internet usage serves the purpose of monitoring performance as well as enhancing productivity.[234] It is further stated that such commonly used software programme will not only monitor the usage of the internet and e-mail but also has the ability to record every stroke programme used and file opened or copied so as to incorporate such information into a searchable report.[235]

3.8. Personal use

Working people spend a great deal of their working time at the workplace. They therefore expect some kind of privacy at the workplace even though they are utilising the company's property. The big challenge is where the employer can draw the line between permitting personal use (that is non-company related use) of e-mail facilities and other communication facilities by its employees which might be harmful to the company's business interests. Buys[236] maintains that there are those who hold the view that if all personal use is totally prohibited then no employee would have any possible expectation in any stored material (for example computer or e-mail) . He further articulates that the better practice is to permit restricted personal use of e-mail either internally or externally and then incorporate other policies such as privacy expectation and misuse of company resources around this pragmatic acknowledgement.[237] Personal use should entail some articulated constraints on such use and should not be allowed to consume a significant amount of the employee's workday. Employers do have a vested interest in promoting

[232] Ibid.
[233] Ibid.
[234]M Paterson . "Monitoring of Employee Emails and Other Electronic Communications" (2002) 21 (1)University of Tasmania: Law Review 1, 2.
[235] Ibid.
[236]R Buys . *The Law of the Internet in South Africa*. (200) pg 197.
[237]Ibid.

good communication and strong relationships between employees. Thus, employers are willing to compromise and are of the view that as long as the number or length of personal calls is not excessive. An employee may make calls that have nothing to do with employer's business affairs and that employee is justified to have a legitimate expectation to privacy.[238] Although an employee must account to employer for time spent, employer cannot compel employee to disclose information of such correspondence.[239]Electronic facilities at work are primarily for the employer's business and are to be used in the course and scope of the employee's functions.[240]There is a contrast argument that states that, the opportunity for some personal use of the internet may in fact enhance an employee's skills in the effective use of the electronic medium and reduce the amount of time required for personal, face to face transaction so it is to the employer's advantage to promote employee personal use of company property.[241] It has been further alleged that a more logical approach is to monitor employees' productive output rather than their electronic transaction and to confine surveillance to situations where there is reason to believe that this may be implicated in a low or reduced level of productivity.[242]

In conclusion, the internet and telephone is the property of the employer and hence should be used as such. To create a balance and avoid abuse of employer's property, the employer must put in place policy clearly setting out the rights and obligations of the employer as well as the employee so as to eliminate many misconceptions. If the employee is aware of the contents of the policy disciplinary action for non compliance is justified. There is no question that in an employment relationship the computer or telephone would be the property of the employer. The employer may therefore wish to monitor the internet and telephone use such as the size of the message, attachments, the frequency and volume of e-mail sent by an employee, number of calls, web-sites often visited by the employee, and the frequency of hits of those.The law places no significant restrictions on the employer's right to monitor electronic transmissions for legitimate purposes but the methods used must not be unduly intrusive and/or reduce employee

[238]*Protea Technology Ltd & another v Wainer &others 1997 (9) BCLR 1225 (W).*
[239]Ibid.
[240]Ibid.
[241]M Paterson . "Monitoring of Employee Emails and Other Electronic Communicatins" (2002) 21 (1)University of Tasmania: Law Review 1, 2.
[242] Ibid.

productivity, and must comply with relevant legislation.[243] Each time an employee uses the internet for a private purpose he or she should know that he or she is taking up the employer's space on the bandwidth intended for business.

[243]Subramanien D & Whitear – nel N. *A fresh perspective on South African law relating to the risk posed to employers when employees abuse the internet*. (2013)SAJLR Vol 37 Issue 1 pg 9-23.

Chapter 4: Case law on the monitoring of employees in the workplace

4. Introduction

Ample cases have surfaced in the law reports to indicate that abuse of electronic communications facilities is a problem for employers. Most of these cases involve illicit use of the internet, telephone taping and use of company email systems. Through this case law we learn how the courts have approached the issue of privacy in the workplace and whether they has been a change over the years on how courts have tackled the conflict between the employers right to monitor and the employees right to privacy.

4.1 Cases heard under the Interception and Monitoring Prohibition Act 127 of 1992

In *Protea Technology Ltd & Another v Wainer & Others*[244] (decided under the Final Constitution), the employer had recorded phone calls made by the employee in the workplace without his consent. These calls were used in court to prove that the employee was acting in breach of a restraint of trade agreement.[245] The employee argued that the recording invaded his right to privacy and contravened IMPA and that the court had no discretion to admit the evidence.[246] The Court considered two issues: first, whether the employer's conduct amounted to a breach of privacy and, secondly, whether the common law power of a court to admit evidence irrespective of the means by which it is obtained, that is the relevance test in *Goosen v Caroline's Frozen Yoghurt Parlour*[247] remained valid under the new Constitutional dispensation. *Goosen*[248] was decided under the Interim Constitution and concerned the dismissal of an employee who after a disciplinary hearing sought to rely on telephone transcripts that he obtained without the consent of the employer to show that the chairperson of the disciplinary hearing was biased. At issue was the admissibility of the recordings. The Industrial Court found the recordings admissible and reasoned in this regard that the test to be applied when determining the admissibility of the evidence is whether the evidence is relevant to the matters in

[244] *Protea Technology Ltd & another v Wainer &others 1997 (9) BCLR 1225 (W).*
[245] Ibid.
[246] Ibid.
[247] 1995 16 ILJ 396 (IC).
[248] Ibid.

issue (the relevance test).[249] The Industrial Court in considering the privacy provision in section 13 of the Constitution and the limitations clause in respect to the first issue, the Court held that the right to privacy requires a subjective expectation of privacy which society recognizes as objectively reasonable.[250] The court held that the 1992 Information Act did not expressly or by necessary inference render the production of recordings made in contravention of its terms inadmissible in a civil action.[251]*Protea Technology* was followed in *Tap Wine Trading CC v Cape Classic Wines*[252], and was even extended to the criminal context in *S v Dube*[253] where court held that, a recording of a conversation between car thieves was held to be not "confidential" and hence excluded from protection under the 1992 Act.

In *Protea Technology*, the court observed:

> The scope of a person's privacy extends only to those aspects in regard to which a legitimate expectation of privacy can be harboured. Whether it exists requires a subjective expectation of privacy which society recognises as objectively reasonable.[254]

More significantly, the Court also held that the employee's subjective expectation of privacy not to be objectively reasonable in light of the fact that the employee was in a position of trust and the telephone calls were made from the employer's premises within business hours.[255] The Court concluded that, because the parties were in an employment relationship, the conversations relating to the employer's affairs were not private and therefore not protected by the Constitution.[256] With respect to the second issue, the Court found that the discretion to admit illegally obtained evidence had to be exercised with reference to the substance of section 36(1) of the Constitution, meaning that, the competing interests had to be balanced. The Court accordingly concluded the relevance test in *Goosen*[257] was inconsistent with the Constitution, but still recognised discretion to be exercised on a case-by-case basis to admit illegally obtained evidence.

---

[249] Ibid.
[250] Ibid.
[251] Ibid.
[252] 1999 (4) SA 194 (C).
[253] 2000 (2) SA 583 (NPD).
[254]1997 (9) BCLR 1225 (W).
[255] Ibid.
[256] Ibid.
[257]*Goosen v Caroline's Frozen Yogurt Parlour (Pty) Ltd 1995 16 ILJ 396 (IC).*

At issue in *Moonsamy v The* Mailhouse[258] was whether the employer was entitled to use evidence at a disciplinary hearing which it had obtained by intercepting and recording the employee's telephone calls in his office and which subsequently contributed to the employee's dismissal. The employee argued that the evidence contravened IMPA and the Constitution. As mentioned above, the arbitrator established that IMPA applied only to interception or monitoring carried out by the police and the Defence Force.[259] The tribunal based this on the fact that section 3(2) of IMPA provides that any application to a judge for a directive shall be made by a police officer, or an army officer, or a member of the intelligence services.[260] The arbitrator concluded that the recording was in violation of section 14(d) of the Constitution and proceeded to consider whether the infringement was justified in terms of the limitations clause contained in the Constitution.[261]

In considering whether the infringement was justified, the tribunal considered the following issues: the nature of right ; the importance of the purpose of the limitation; the extent and nature of the limitation; the relation between the limitation and its purpose; and whether less restrictive means to achieve the purpose were available.[262] In respect of the nature of the right, the tribunal held that the employee had a reasonable expectation of privacy in respect of calls made at his employer's premises.[263] With reference to the importance of the purpose of the limitation, the tribunal reasoned that the employer considered its actions necessary for financial preservation and therefore the employee's right to privacy had to be qualified.[264] The arbitrator observed that the court in *Protea Technology*[265] identified the competing interests to be the employee's right to privacy versus the employer's right to economic activity. The right to economic activity is no longer guaranteed in terms of the Final Constitution and has been replaced by section 22 of Constitution guaranteeing freedom of trade, occupation and profession.[266] The introduction of section 22, according to the tribunal, seemed to indicate that the framers of the Constitution preferred "the employee's personal right to the more amorphous (consequently controversial)

[258]*Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA).*
[259] Ibid.
[260] Ibid.
[261] Ibid.
[262] Ibid.
[263] Ibid.
[264] Ibid.
[265]*Protea Technology Ltd & another v Wainer &others 1997 (9) BCLR 1225 (W).*
[266]*Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA).*

right to economic activity".[267] In considering the nature and extent of the limitation, the arbitrator opined that an employer might have a right to ask an employee to disclose the number of personal calls he or she made during working hours.[268] With regard to the relationship between the limitation and its purpose, the tribunal reasoned that if an employer showed that telephone tapping was the only method through which it could secure essential evidence against an employee, its use may be justified.[269] As regards less restrictive measures to achieve the purpose, the tribunal reasoned that if the only method to obtain evidence was telephone tapping, the employer should have sought prior authorization.[270] Leaving aside the question whether the constitutional limitations are indeed applicable to the assessment of specific acts of employees, the test adopted in *Moonsamy*[271]was as good as any that might be chosen. However, it still begs the wider question: what are the limits of the employee's right to privacy?[272]

In *Moonsamy*[273], the commissioner conceded that this question cannot be answered *in vacuo*. Following the American case of *Katz v US* 389 US 347 (1967), he observed:

> Office practices and procedures, and legitimate employer regulations, might reduce the employee's expectations of privacy in their offices, desks and filing cabinets. Given the great variety of work environments, the question of whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.

The commissioner held that by continually tapping Moonsamy's telephone with the express purpose of monitoring all his conversations, the employer had gone further than "rummaging in [his] desk or filing cabinet".[274] Importantly, the commissioner found that the assessment of the reasonableness of the infringement did not depend on the nature of the evidence uncovered by the tap; the method chosen must be assessed in advance. Telephone conversations, said the commissioner, are a "very private affair". Therefore:

> An employer might have the right to ask an employee to disclose the number of personal as opposed to business calls he or she makes during working hours, but the right to disclosure ends there, unless the employer can show, when seeking prior authorisation [which the

[267] Ibid.
[268] Ibid.
[269] Ibid.
[270](1999) 20 ILJ 464 (CCMA).
[271] (1999) 20 ILJ 464 (CCMA).
[272] Ibid.
[273] (1999) 20 ILJ 464 (CCMA).
[274] Ibid.

> commissioner suggested might be obtained from the Labour Court], that there are compelling reasons within the context of business necessity, that the contents of those conversations are disclosed.[275]

In *Moonsamy,* [276] the commissioner therefore recognised that employees cannot in all circumstances invoke their right to privacy to prevent employers from using the contents of their personal communications against them in disciplinary proceedings. Everything depends on the reasonable operational needs of the employer.

In *Sugreen v Standard Bank of SA*[277]the commissioner came to an opposite conclusion. In this case, the employer had obtained a tape recording of a conversation between one of its managers and a service provider which revealed evidence of a bribe. The tape recording was made and given to the employer by the alleged briber.[278] The commissioner distinguished *Moonsamy*[279]on the basis that there were few other methods by which evidence against the employee could be acquired, that the recording had not been part of a continual monitoring and was not made by the employer itself, that this was a case of 'participant monitoring', that the recording was made during business hours, using the employer's telephone. Given all these factors, it was fair to admit the recording as evidence.[280]It is ample to recognise that the use by the employee of the employer's telephone and e-mail are legitimate areas of interest to the employer where it suspects that the employee is guilty of misconduct.[281]

Prior to IMPA coming into effect, "all relevant evidence which was not rendered inadmissible by an exclusionary rule was admissible in a civil court irrespective of how it was obtained".[282] This unrestricted use of evidence resulted in abuse and violations of privacy. IMPA restricted the manner in which evidence was obtained and further introduced penalties for obtaining evidence in a manner contrary to the Act's requirements. The language of IMPA further points to the fact that the legislation was intended to apply to state agencies which were in the business of

[275] Ibid.
[276] Ibid.
[277]*Sugreen v Standard Bank of SA [2002] 7 BALR 769.*
[278]Ibid.
[279] (1999) 20 ILJ 464 (CCMA).
[280]Ibid.
[281] C Mischke. 'The monitoring and interception of electronic communications' (2001) 10 *Contemporary Labour Law* pg 91.
[282]*Protea Technology Ltd & another v Wainer &others 1997 (9) BCLR 1225 (W).*

intelligence gathering for purposes of investigating and ultimately combating criminal activities. Before the tribunal's reasoning in *Moonsamy v The Mailhouse*,[283] it appears as if courts were quite willing to find that the application of IMPA was wide and that the Act applied to interception and monitoring in the private sphere. One reason for this is that certain terms in IMPA and its general prohibition were couched widely enough for the argument to be made that the Act could well regulate the interception and monitoring in places such as the workplace.

4.2 Cases herd under The Regulation of Interception of Communications and Provision of Communication – Related Information Act (RICPCIA)

Bamford & Others/Energizer (SA) Limited,[284] is one of the earliest decisions to put into perspective or effectively address the issue of employee privacy in the workplace, particularly in relation to the use of the employer's e-mail and Internet facilities. In this case Energizer, a leading manufacturer of batteries for electrical appliances, summarily dismissed a group of its female employees for violating the company's e- mail policy.[285] The company dismissed the applicants on the following charges:

- The repeated violation of company policies and procedure regarding the use of company e-mail.
- The repeated receipt and forwarding to colleagues of obscene pornographic, racist and sexist material and jokes.

The applicants did not deny receiving and forwarding the said material and jokes. However, they contended that there was no clear rule against the private use of e-mail, that their right to privacy was invaded, and that there was a discriminatory application of discipline by the respondent.[286] In respect of last-mentioned claim, the applicants argued that the standard of behaviour required by the respondent as regards company e-mail use was flawed because, were it applied across the board in business and industry, almost every employee would be at risk of losing their jobs.[287] Meaning the receipt and forwarding of pornographic, racist and sexist material and jokes rule was not consistently applied.

[283](1999) 20 *ILJ* 464 (CCMA).
[284]*Bamford & others v Energiser (SA) Limited [2001] 12 BALR 1251*.
[285] I bid.
[286] I bid.
[287] I bid.

The arbitrator had scarce sympathy with this argument. He said:

> The material which has been the subject-matter of this arbitration has not been 'personal' in any respect. The proper label may be non-business or even 'private' but nevertheless it consists entirely of material generated by anonymous third parties and distributed for the consumption of interested parties on the internet. In no sense whatsoever has the personal dignity or personal affairs of any of the individual applicants in the least been disturbed. Furthermore, all the information which was the subject matter of the proceedings was derived from storage facilities in the company's own e-mail system. It can hardly be said; even in respect of genuinely 'personal' communications that individuals are entitled to deposit intimate material in their employer's storage facility and require their employer not to examine it in order to determine whether there is any point to it being kept.[288]

In considering these arguments the arbitrator found that although the standard policy document did not explicitly prohibit e-mail use in the workplace, there was enough wording in the document to suggest such prohibitions. The background of the applicants, which the arbitrator described as 'middleclass…not bereft of education', convinced the arbitrator that the applicants should have known that their conduct was not socially acceptable.[289] The arbitrator further stated that some of the materials received and forwarded by the applicants were 'contrary to what would circulate amongst self-respecting people.'[290] Lastly, the arbitrator stated that even if the policy was silent on prohibitions against e-mail use in the workplace, common sense should have directed the applicants that the grotesqueness of the material they were receiving and forwarding had no place in the workplace.[291] The dismissals were found to be fair because of:

- The risks posed by the trafficking;
- The grotesqueness of the images;
- The danger of the outside world becoming aware of the exchanges of these messages and the further risk of the domain name of the respondent being associated with such material and jokes;
- The respondent's exposure to trademark violations as the applicants resorted to entertaining themselves with trademark parodies ;

[288] Ibid.
[289] Ibid.
[290] Ibid.
[291] Ibid.

- The offence that could be taken to the material and jokes by other staff members and
- The embarrassment to the employer by the exchange of such material and jokes.[292]

The arbitrator found that the material and jokes concerned could not be described as personal in nature, the personal dignity or personal affairs of the applicants had not been affected in any way, and the material and jokes concerned were stored in the respondent's computers and could not be considered personal communications hence they was no violation of the right to privacy.[293]*Bamford*[294] broke new ground in that it made clear that, even where there is no (explicit) policy regulating employee use of e-mail in a workplace, employees cannot argue that they had a reasonable expectation of privacy in respect of all received and forwarded communications in that workplace.

The applicant in *Cronje v Toyota Manufacturing*[295] had been dismissed for circulating a cartoon he received via company e-mail. The cartoon superimposed President Mugabe of Zimbabwe head's on a gorilla's body. The bigger gorilla depicted in the cartoon was holding a smaller gorilla, also with Mugabe's features, with a caption alongside worded "Mugabe and his right hand man. We want the farms to grow more bananas."[296] Although privacy considerations did not play a role in this case, the respondent argued that it found it necessary to dismiss the applicant based on the following:

- race and race related issues are familiar and important issues on the shop floor;
- the employer's factory employed a total of 4500 employees and 77 percent of these employees were black. This means one had to take extra care and display extra sensitivity towards the race issue, especially in light of the country's past;
- concern that the incident would cause serious problems such as industrial action on the shop floor;
- the employer had dealt harshly with race related incidents in the past;
- employees knew that racially offensive remarks and the distribution of racially offensive material or sexually explicit material would be dealt with in a very serious light;

[292] Ibid
[293] Ibid.
[294] Ibid.
[295][2001] 3 BALR 213 (CCMA).
[296] Ibid

- the employer's internet and e-mail code specifically prohibited the display and/or transmission of any offensive racial, sexual, religious or political images, documents and images on the company system;
- the depiction of a black person as an ape is racist and there is still a section of the white population that associated black people with apes; and
- the respondent's shop stewards and black employees found the cartoon very offensive in that it portrayed black people as apes.[297]

The employee argued that he did not regard himself or the cartoon as racist, which is why he readily distributed the cartoon to others. The applicant also acknowledged that he was aware of the company's e-mail policy, but was not aware of the fact that the cartoon fell within the policy's prohibitions.[298]

On analysis of the evidence and argument, the presiding commissioner found that the cartoon was racist and inflammatory. He held,

> "The subject of the crude superimposition is President Mugabe, but the picture and to no lesser extent, the caption, fall square into the crude, offensive, racist stereotype developed over centuries by white people that associate black people with primates, beings of lesser intelligence and lower morality…The fact that the offensive, racist stereotype associating black people with apes exists is not disputed. This is a matter of deep moral, social and cultural sensitivity to black people, and this sort of offensive racial stereotyping is not by any means limited to black people ...These caricatures were and are still are, deeply offensive.... They offend people's self-image as a cultural racial entity. The depiction of an Islamic leader as a pig would be found to be deeply reprehensible by Muslims in this and in many countries. In the same way the depiction of a black person as an ape is racist, inflammatory and inherently wrong."[299]

The employee in *Singh and Island View Storage Ltd*[300] had been dismissed for sending a sexually explicit e-mail to 3 of his colleagues on the company's intranet. The employee admitted

[297][2001] 3 BALR 213 (CCMA).
[298] Ibid.
[299] Ibid.
[300] Singh and Island View Storage Ltd (2004) 13 CCMA 8.32.1.

that he was aware that the e-mail he had sent was inappropriate and contained sexually explicit material and also that he was aware of the company's electronic communications policy and that his conduct could result in his dismissal.[301] The employee argued that he had intended no harm in sending out the e-mail but had done so as a joke.[302] The employee further argued that the company's electronic communications policy had not been consistently applied.[303] Although the commissioner agreed that this was probably the case, the commissioner also reasoned that what was of paramount importance was the employee's motive in sending out the e-mail. In this respect, the commissioner found that the employee's motive was to embarrass and cause offence as he had admitted that he had a hostile and less than amicable relationship with his colleagues. The commissioner concluded that the employee was well aware of the consequences of his actions and his intention in sending the e-mail was to offend and insult his colleagues and, as such, found his dismissal to be justified.

The decision of *Toker Bros (Pty) Ltd and Keyser*[304] adopted the reasoning in *Bamford*.[305] In *Toker Bros (Pty) Ltd and Keyser* an employee was charged with dishonesty in that she excessively misused the company computer for personal use during working hours and without permission.[306] The employee was further charged with making defamatory remarks about her employer in an e-mail to a friend she sent from the company computer.[307] The employee argued that her employer was aware that she was accessing the Internet to arrange a 20th school reunion, that her access to the Internet was mostly work related and that she was not told by her employer about a policy or rule against personal use of the Internet.[308] The employee further admitted the defamatory remarks about her employer in her e-mail to a friend, but challenged the manner in which the e-mail was retrieved by her employer.[309] The employer argued that it had advised the employee not to download from the Internet and denied giving her permission to use the Internet to arrange her school reunion.[310] The arbitrator found that at issue was whether, in the absence of

[301] Ibid.
[302] Ibid.
[303] Ibid.
[304] Toker Bros (Pty) Ltd and Keyser(2005) 26 ILJ 1366 (CCMA).
[305] Bamford & others / Energiser (SA) Limited [2001] 12 BALR 1251.
[306](2005) 26 ILJ 1366 (CCMA).
[307] Ibid.
[308] Ibid.
[309] Ibid.
[310] Ibidd

a written and clear policy against personal use of Internet, the employee could be reasonably expected to know or be aware of the rule.[311] The arbitrator further found that "not all rules and policies have to be made known to employees as some common sense... [has] to be weighed against reasonableness".[312] As such, the employee "could reasonably have been expected to know the rules as she was cautioned at the start of her employment and due to her experience as an employee."[313] More importantly, the arbitrator pointed out that the charge was not for using Internet for personal use, but for using the Internet excessively for personal use.[314] This implies that employers reasonably expect their employees to make personal use of company Internet facilities, but the employee has to ensure that such use is within reasonable limits and not excessive.

With regard to the employee's challenge to the manner in which her defamatory e- mail was accessed, the employer had argued that the manner in which the e-mail was obtained was not illegal in that the e-mail was obtained during an investigation into the employee's excessive Internet usage. [315]The arbitrator stated that the right to privacy in the Constitution particularly section 14 (d) prohibiting the monitoring and interception of employee communications, can be limited where consent has been given or a clear policy on monitoring and intercepting of communications in the workplace is implemented.[316] The arbitrator found that the e-mail was not obtained with malicious intent but its discovery was incidental to the investigation into the employee's abuse of the company's Internet facility.[317] The arbitrator also considered the fact that the employee's e-mail to her friend could have resulted in her employer being held vicariously liable in civil law, given that the e-mail could be regarded as offensive and insensitive by some of its recipients.[318]

In *Van Wyk v Independent Newspapers Gauteng (Pty) Ltd & Others*[319] the Labour Court reinforced the principle that personal e-mails sent from a company's e-mail system are not private as they can be read by other recipients, especially where the intended recipients also use

[311] Ibid.
[312] Ibid.
[313] Ibid.
[314] Ibid.
[315] Ibid.
[316] Ibid.
[317] Ibid.
[318] Ibid.
[319]Van Wyk v Independent Newspapers Gauteng (Pty) Ltd & Others (2005) 26 ILJ 2433 (LC).

the company e-mail system. The applicant had been employed as chief sub-editor by a newspaper when she had a heated argument with her editor and two other employees while on night duty.[320] The employee sent an e-mail to her superior a day later in which she vented her feelings and frustrations about work and further referred to her editor and his deputy as that 'arse hole' and 'his overbearing cohort'.[321] This second e-mail landed on her editor's desk in an unmarked envelope, even though the employee and her superior had not forwarded the e-mail to anyone else.[322] The employee argued that the second e-mail to her superior should not be admitted by the arbitrator because of its private nature.[323] The arbitrator found the employee should have been reasonably aware that the second e- mail would be read by people other than its intended recipient given that: a) when her superior received her e-mail, two of her colleagues were standing behind her superior; b) the first and second e-mail were sent within a short time of each other and both dealt wholly or partly with work related issues; c) the second e-mail was not marked private or confidential; d) the company's e-mail policy stipulated that all information stored on the company system belongs to the company and cautions employees not to assume that their e-mails will not be read by others; and e) the e-mail had been sent to a communal computer which belonged to the company. [324]

Case law relating to staff abuse of company e-mail and Internet suggests that courts and commissioners are unlikely to accept the argument that the employee was unaware of a policy regulating such abuse, particularly where the concerned employee held a managerial or leadership role in a company and, of course, where the abuse is of an excessive nature.

The employer in *Kalam and Bevcap (Nampak)*[325] established that over a period of 5 months the employee had visited thousands of Internet sites, most of which contained pornographic material. The employer found that the employee had spent approximately 285 hours per week visiting 14802 non - work related sites.[326] The employer further ascertained that the employee had visited and downloaded sexually explicit images using the company's Internet access.[327] The employee

[320] Ibid.
[321] Ibid.
[322] Ibid.
[323] Ibid.
[324] Ibid.
[325] *Kalam v Bevcap (2006) 15 MEIBC 8.32.1.*
[326] Ibid.
[327] Ibid.

was dismissed for this reason. The employee contended that his actions could not be considered unacceptable because he was aware of the company's IT policy document, but had not read it because it was bulky document.[328] The commissioner found the latter argument to be unacceptable and also found that the employee knew of the policy and its content because he ignored the popup messages that warned that the sites he was accessing were prohibited.[329] The commissioner added that even if the employee was unaware of the policy and its contents, his common sense should have prevailed.[330] The commissioner found the employee's dismissal to have been both substantively and procedurally fair.

The employee in *Latchmiah and Billiton Aliminium SA (Pty) Ltd t/a Bayside Aliminium*[331] the employee was also dismissed for repeatedly accessing pornographic websites via the employer's Internet. Unlike the employee in Kalam, the employee in this case argued that he had a "dependency problem", which employer had failed to explore. The employee, who had been employed as a process superintendent, further argued that his accessing of pornographic websites did not interfere with his work and that the rules in place restricting the accessing of pornographic sites, was not consistently applied.[332] The employee further disputed the employer's argument that his repeated access interfered with the company's information systems as he did not access the sites with malicious intent.[333]

The arbitrator found that, the existence of a well-established rule in the employer's workplace; the employee admission to being aware of the rule; the rule was lawful and reasonable because it was aimed at dissuading unethical conduct, keeping the company information systems free from viruses and outside intrusion, preventing the slowing down of the system due to traffic, as well as preventing sexual harassment claims; the rule had been breached by the employee's conduct and the "dependency problem" defence could not be considered because the employee failed to take steps to bring the problem to the attention of the employer.[334]It was further held that, the rule was consistently applied; the company's Internet and access policies had evolved because of the

[328] Ibid.
[329] Ibid.
[330] Ibid.
[331]*Latchmiah and Billiton Aliminium SA (Pty) Ltd t/a Bayside Aliminium (2006) 13 MEIBC 8.32.2.*
[332] Ibid.
[333] Ibid.
[334] Ibid.

increase in Internet access in the workplace; and dismissal was an appropriate sanction because of the excessive nature of the employee's conduct.[335]

From the foregoing discussion of case law decided since the enactment of RICPCIA, it appears as if South African courts have taken the following observation towards employee privacy in the workplace. The employer is justified in protecting its business interests by regulating the use of e-mail and Internet in the workplace, because it owns the e-mail and Internet facilities in the workplace. Secondly, the absence of an explicit policy or no policy is no excuse for forwarding racist or offensive e-mails using the employer's Internet facilities. Case law decided under IMPA addressed the issue of privacy in the context of the interception of communications and it was decided that telephone calls in the workplace were not protected by the Act by virtue of the nature of the relationship between the employee and employer (Protea Technology[336]).

Case law decided after the enactment of RICPCIA has not really dealt with the application of that Act, nor in much detail with the balancing required where employer policies relating to e-mail and Internet clash with the privacy concerns of employees. Even so, and even though most cases have dealt with the fairness of dismissal of employees who abused e-mail and Internet systems, these cases already make it clear that an employer has an important interest in the integrity of its information systems and that these interests typically will trump those of the employee.

4.3 Most recent cases on monitoring pending the implementation of the Protection of Personal Information Bill of 2009:

Fredericks v Jo Barkett Fashions [2012] 1 BALR 28 (CCMA)

An employee working as an administrative assistant for a fashion company was dismissed after the respondent's witness, Ms Alex Barkett, General Manager, testified under oath that it was brought to her attention that the applicant was publishing derogatory statements on her facebook page.[337] She opened the applicant's page and found that it was indeed true.[338] The applicant made several remarks which were horrific and disturbing in that the applicant even went to an extent of

[335](2006) 13 MEIBC 8.32.2.
[336]*Protea Technology Ltd & another v Wainer &others 1997 (9) BCLR 1225 (W).*
[337]*Fredericks v Jo Barkett Fashions[2012] 1 BALR 28 (CCMA).*
[338] Ibid.

calling her names.[339] It was argued that, the remarks were made known to the general public and the implications would have affected 90 employees and key customers which generates the revenue for the company.[340] It was further argued, the applicant did not show any respect to her as the manager and the company itself.[341] After a thorough investigation, as facebook is a new concept, the applicant was charged and an independent chairperson conducted the hearing fairly which led to a dismissal of the applicant.[342]The respondent moreover, argued that, the applicant contravened the provisions of her contract although there was no specific policy concerning Facebook usage in the company, in that she published derogatory statements about the company and the general manager.[343]

The applicant counter argued she felt that the dismissal was unfair and the company was supposed to use corrective measures other than to dismiss her as she feels that it was too harsh.[344] The employee argued her total circumstances were not considered since she asked for an apology for using facebook as a platform as she had issues in as far as what the General Manager (Alex) said about her after she lost a child.[345] It was her evidence that her constitutional right of privacy was infringed. The dismissal of Nadia Fredericks by Jo Barkett Fashions was held to be substantively fair.[346]

Sedick& another v Krisray (Pty) Ltd CCMA WECT13321-10, [2011] JOL 27445 (CCMA)

Employees (De Reuck and Sedick) were employed by a fashion accessories company (Krisray (Pty) Ltd) as an Operations Manager and Bookkeeper respectively.[347] The company's Marketing Manager (Ms Coetzee) logged into her Facebook account and navigated to De Reuck's facebook page, because she wanted to send her a friend request.[348] She was able to see everything on the employee's Facebook wall without being given access as a friend and what she saw included posts by Sedick and other employees.[349] Ms Coetzee found offensive comments about the

[339] Ibid.
[340] Ibid.
[341] Ibid.
[342] Ibid.
[343] Ibid.
[344] Ibid.
[345] Ibid.
[346] Ibid.
[347]*Sedick& another v Krisray (Pty) Ltd CCMA WECT13321-10, [2011] JOL 27445 (CCMA).*
[348] Ibid.
[349] Ibid.

company and its management in posts on the employees' Facebook walls.[350] Another employee referred to Ms Coetzee and her brother in a post as, *"2 dumb brats runnin a Mickey Mouse business"* Sedick referred to the Director of the company as, *"a very ugly man with a dark soul".*[351]

After having gone through the comments as per the bundle, it was clear that the applicant knew what she was doing and had negatively impacted on the image of the company and it's General Manager.[352] As to her claims of her right of privacy being infringed, the Regulation of Interception of Communication Act 70 of 2002 provides that any person may intercept any communication unless the person is intercepting that information or communication for committing an offence.[353] It was held that Facebook can be accessed by any person who has an account and it is up to the Facebook user to restrict access to their pages.[354] The applicant did not do so, her page was open to the public and anybody could access it.[355] It was further held that corrective measures in circumstances of this case would not be a viable decision, her actions were not justifiable and she used the wrong platform to address her grievance, therefore, dismissal was fair. [356]

Smith and Partners in Sexual Health (Non-Profit) CCMA (WECT 13711-10)

An employee, Ms Smith, was employed as the administration assistant, one of her duties was to check the company Gmail account and forward emails to the company's new email address.[357] The company CEO (Ms de Lora) wanted to log into the company Gmail account to check whether any emails had come in while Ms Smith was on leave.[358] Ms Smith forgot to sign out of her personal Gmail account and the CEO ended up looking at Ms Smith's personal account instead.[359] The CEO did not realise that she was looking at the employee's personal emails at

[350] Ibid.
[351] Ibid.
[352] Ibid.
[353] Ibid.
[354] Ibid.
[355] Ibid.
[356] Ibid.
[357] *Smith and Partners in Sexual Health (Non-Profit) CCMA (WECT 13711-10).*
[358] Ibid.
[359] Ibid.

first; however, she worked it out once she tried to look at them again and ended up logging into the business account.[360]

Ms De Lora dismissed Ms Smith because she found emails in her personal account in which the employee complained about her job, complained about Ms De Lora and told people outside of the organisation about its daily activities.[361]

Ms Smith took her employer to the CCMA for unfair dismissal. She argued that her employer had intercepted her private Internet based emails on Gmail unlawfully; the employer's actions were not justified by our monitoring law, the Regulation of Interception of Communication and Provision of Communication-Related Information Act, 70 of 2002 ("RICA"); employer's actions infringed her Constitutional right to privacy; and that the emails that her employer sought to rely on were not admissible as evidence.[362]

The question answered by this case was, when can an email be considered the "private" property of the employee and not be capable of being monitored by the employer?[363] The answer to the question was held to be 'when it's your own email'.[364] It was further held that, viewed from the employee's perspective your own email is that email that is stored or hosted with a service provider with whom you have a contract.[365] Secondly, where an employer: owns its email infrastructure (e.g. owns its own hardware and runs its own email exchange server) and provides a user with an email address to use at work; or does not own its own email infrastructure, but instead uses a hosted email infrastructure which it pays a fee per user to use, and provides each user with an email address, the default position would be that all emails that a user sends or receives are not private.[366]

In conclusion, South Africa now has legislation directly regulating the monitoring of employees in the workplace. This was not always the case, as IMPA did not specifically provide for such interception and monitoring, although it arguable was broad enough to include Internet and e-mail communications in its scope of application. This is a clear indication of the challenges

[360] Ibid.
[361] Ibid.
[362] Ibid.
[363] Ibid.
[364] Ibid.
[365] Ibid.
[366] Ibid

technological developments create for the law in general, and privacy in particular .In the Smith case, the court appeared to be leaning in the direction of drawing a distinction between whether the employer owns the hardware that makes up the email infrastructure (where the email would not be private) and where the employer does not own that hardware (where the email would be private).

Chapter 5

5.1 Conclusion

The right to privacy has developed over time because in the beginning it used to be recognised under the ambit of the right to dignity but now it is a right with its own self recognition. The right to privacy in South Africa is recognised in the Bill of Rights specifically section 14 of the Constitution of the Republic of South Africa. Although recognised by the Constitution it is not an absolute right because it can be limited through application of section 36 of the Constitution which is the limitation clause. Case law over the years has also established that for one's right to privacy to be upheld one must have had a legitimate expectation of his/her privacy right not being infringed.

There are a number of legislative provisions which protect the right to privacy by regulating monitoring of employees internet, telephone and email correspondence in the workplace directly and indirectly. The interception and Prohibition of Monitoring Act came into effect before the interim Constitution and it was the first piece of legislation which concerned monitoring of email and internet communications. Its purpose was both to prohibit and authorise the monitoring of communications and conversations. The main aim and purpose of this piece of legislation was the monitoring and prohibition of interception of telephone conversations. The shortfall that led to its repeal was that it did not deal adequately of monitoring of new technology especially email. The IMPA Act was succeeded by the Regulation of the Interception of Communications and Provisions of Communications Related Information Act. RICPCIA recognises three instances where interception of communications can be lawful, where one of the parties to the communication have given their consent, where one party to the communication is involved in the interception and if the interception is carried out in the ordinary course of business. This legislation highlighted that employees did not have a legitimate expectation of privacy in the workplace and if they do their employer interests can outweigh privacy. Cases heard under this Act seem to be pointing to the fact that the employer's right to protect the integrity of its information trumps the employees right to privacy. The Protection Of Personal Information Act 4 of 2013 enactment is going to bring about a significant protection of individuals and organisations protection of personal information. Individuals will have the ability to ask

organisations to account for the exploitation of their personal information unlike in recent years legislation.

The reasons formulated as to why employers monitor the internet, telephone and email correspondence of their employees is aimed at ensuring productivity and efficiency in the workplace. Monitoring of employee email, internet and telephone correspondence in the workplace brings about into play two competing interests which are, the employers need to run his business as he/she sees fit and the employees right to privacy. Restrictions on privacy in the workplace also serve to create an increase in economic performance. The law treats both the employee's right to privacy and the employer's right to monitor as important. It is not set in stone that the courts will rule in favour of the employer or employee in a given case but as to which right is to be limited depends on the facts of each case. The invention of new technology each day increases the need for the employer to put in place measures for the monitoring of employee email, telephone and internet so as to curb the risk brought about by these devices. So as to create a balance between the two conflicting rights of the employer and employee new statutory laws are implemented to regulate monitoring so as to provide for both the needs of the employer and employee for example the Protection of Personal Information Act is said to be the employees champion because it is going to make organisations more accountable for the exploitation of the employee's right to privacy.

Although it is not law many cases as discussed in this paper make it clear that an employer has an important interest in the integrity of its information systems and that these interests typically will trump those of the employee.

BIBLIOGRAPHY

ARTICLES:

Basson et al Essential Labour Law (vol l) Individual l Labour Law (1998) pg50.

Bawa N. The Regulation of the Interception of Communications and Provision of Communication Related Information Act. (2008) pg 296- 332.

Beech W. "Right of Employer to Monitor Employees' Electronic Mail, Telephone Calls, Internet Usage and other Recordings" 2005 (26) *Industrial Law Journal* pg655.

Calitz K. Vicarious liability of employers: reconsidering risk as the basis for liability. (2005) 2 TSAR pg 215.

Chatfield C. & Hakkila J. 2005. 'It's like if you opened someone else's letter — User perceived privacy and social practices with SMS communication'. In*Proceedings of the seventh international conference on human computer interaction with mobile devices and services*, Salzburg, Austria, pg 219-222.

Collier D. 2002. 'Workplace privacy in the cyber age', *Industrial Law Journal*, 23: pg 1743-1759.

Dekker A. Vices or Devices" Employee Monitoring in The Workplace (2004) 16 SA Merc LJ pg 622- 637.

Etsebeth V. The growing expansion of vicarious liability in the information age (part 2). (2006) 4 TSAR pg755.

Gule S. Employers'vicarious liability for sexual harassment‖. (2005) 13 (2) JBL pg 66

Hunter P. 2007. 'Is now the time to define a mobile security policy', *Computer Fraud and Security*, 6: pg10-12.

Lidovho GJ. The internet and the piracy of copyrightable computer software in South Africa: some comparative perspectives. (2006) 123 (2) SALJ pg339.

Manamela ME. Vicarious liability: paying for the sins of others: case comments. (2004) 16 (1) SA Merc LJ 126.

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

Paterson M. "Monitoring of Employee Emails and Other Electronic Communications" (2002) 21 (1)University of Tasmania: Law Review 1, 2.
Pistorious T. Monitoring, interception and Big Boss in the workplace: is the devil in the details? (2009) PER vol.12 no.1 Potchefstroom. pg 3.

Schönteich M. *African Security Review, Volume 9 No 2, 2000.* (2000): South Africa's arsenal of terrorism legislation, African Security Review, 9:2, 39-51

Shumani L. Gereda The Electronic Communications and Transaction ACT pg 271.

Subramanien D & Whitear – nel N. A fresh perspective on South African law relating to the risk posed to employers when employees abuse the internet. (2013)SAJLR Vol 37 Issue 1 pg 9-23.
Tavani HT. 2007. 'Philosophical theories of privacy: Implications for an adequate online privacy policy', *Metaphilosoph,* **38**(1): 1-22. Pg 10.
Van Jaarsveld M . Forewarned is Forearmed: Some Thoughts on the Inappropriate Use of Computers in the Workplace. (2004) 16 (4) SA Merc LJ 661.
Watney M. ―Regulation of Internet pornography in South Africa (2)‖. 2006 (69) *THRHR* 385-386.

BOOKS

Basson A, Christianson M, Garbers C, Le Roux PAK, Mischke C and Strydom EML Essential Labour Law (2003).
Burchell JM. The Law of Defamation in South Africa (1985) 35.
Cockhead A. "A Critical Analysis of Law of Privacy with Reference to Invasion of Privacy of Public Figures. 1990 5.
Currie & de Waal (2005) Bill of Rights Handbook. Juta & Co Ltd , Cape Townpg 317 - 318.

Eiselen S. Roos A , Pistorius T & Van der Merwe D. (2006). *Information and communications technology law*. Durban: LexisNexis pg 353.
McQouid – Mason. *The Law of Privacy in South Africa* (1978) Juta and Company Ltd Cape Town 98 – 99.
Neethling et al Neethling's Law of Personality (1996) Butterworths: Durban.pg 36.
Remp Ann, M. The 2/" Century: Meeting the Challenges to Business Education (1999) pg117.
Rycroft & Jordan. A Guide to SA Labour Law2 ed (1992) pg86.

Van der Walt, JC & Midgley, JR .*Principles of Delict*.3ed. (2005)pg 36.

TABLE OF CASES:

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

Bernstein v Bester NO 1996 (2) SA 751 (CC) 784.
Case v Minister of Safety and Security1996 (3) SA 617 (CC).
Cronje v Toyota Manufacturing (2001)22 ILl735 (CCMA).

Die Staat v M Douvenga (née Du Plessis) (District Court of the Northern Transvaal, Pretoria, case no 111/150/2003, 19 August 2003, unreported).

Fredericks v Jo Barkett Fashions [2012] 1 BALR 28 (CCMA)

Goosen v Caroline's Frozen Yogurt Parlour (Pty) Ltd 1995 16 ILJ 396 (IC).
Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors 2000 (10) BCLR 1079 (CC).

Kalam v Bevcap (2006) 15 MEIBC 8.32.1.
Latchmiah and Billiton Aliminium SA (Pty) Ltd t/a Bayside Aliminium (2006) 13 MEIBC 8.32.2.
Minister of Law and Order v Ngobo1992 4 SA 822 (A).
Minister of Police v Rabie1986 (1) SA 117 (A).
Minister of Safety & Security v Jordaan t/a Adre Jordaan Transport 2000(4) SA 21 (SCA) at 24H-25E.
Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (CC) ;1998 (7) BCLR 880 (CC).
Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA).
National Coalition for Gay and Lesbian Equality v Minister of Justice1999 (1) SA 6 60 D – E.
National Media Ltd v Jooste 1996 (3) SA 262 (A).
Ntsabo v Real Security CC[2004] 1 BLLR 58 (LC).
O'Keeffe v Argus Printing and Publishing Co. Ltd and Others 1954 (3) SA 244 (C).
Olmstead v The United States 277 US 4381927.

Others: In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others2001 1 SA 545 (CC).
Protea Technology Ltd & another v Wainer&others 1997 (9) BCLR 1225 (W).
R v Umfaan 1908 TS 62.
S v A 1971 (2) SA 293 (T)
S v Bhulwana (1996) 1 (SA) 388 (CC) para 18.
S v Dube 2000 (2) SA 583 (NPD)
S v Jordan and Others (Sex Workers Education and Advocacy Task Force and Others as Amici Curiae 2002 6 SA 642 (CC).

S v Makwanyane 1995 (3) SA 391 (CC); 1995 (6) BCLR 665 (CC).
S v Naidoo 1998 (1) BCLR 46 (D) .
Sedick & another v Krisray (Pty) Ltd CCMA WECT13321-10, [2011] JOL 27445 (CCMA).

Smith and Partners in Sexual Health (Non-Profit) CCMA (WECT 13711-10).

Sugreen v Standard Bank of SA [2002] 7 BALR 769.
Tap Wine Trading CC v Cape Classic Wines 1999 (4) SA 194 (C).
Toker Bros (Pty) Ltd and Keyser(2005) 26 ILJ 1366 (CCMA).
Van Wyk v Independent Newspapers Gauteng (Pty) Ltd & Others (2005) 26 ILJ 2433 (LC).
Viljoen v Smith 1977 (1) SA 309 (A).

TABLE OF STATUTES

Electronic Communications and Transactions Act 25 of 2002.
Employment Equity Act 55 of 1998.
Films and Publications Act 18 of 2004.
Films and Publications Act 65 of 1996.
The Interception and Monitoring Prohibition Act 127 of 1992.
Protection of Personal Information Act 4 of 2013.
The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

BILLS:

The Electronic Communications and Transactions Act Amendment Bill 2012.

Internet Sources:

Budricks C. SAICA: Summary on the Protection of personal Information Bill of 2009. Published 14 August 2012.

Buys R. The Law of the Internet in South Africa. (200) at 197.

Gondwe M. *The Protection of Privacy in the Workplace: A Comparative Study.* (2011) Published dissertation for a Degree of Doctor of Law at Stellenbosch University. page 1-448.

PWC. Protection of Personal Information Bill of 2009 Survey: The Journey to Implementation. November 2011 pg 1-40.

SA Law Commission. Project 124: *Privacy and Data Protection Report.* (2009).

Shumani L. Gereda The Electronic Communications and Transaction ACT pg 271.

PRESENTED PAPERS:

Le Roux PAK. "Employment Practices in the Age of the Internet" (Unpublished paper delivered at the E-commerce and Current Commercial Law Workshop on 29 August 2003 at Sandton Johannesburg) pg 5.

Lease D. 'Balancing productivity and privacy: Electronic monitoring of employees.' Paper presented at the European Management and Technology Conference, Rome, Italy, June 2005.