Title: Employee's Right to Privacy versus the Employer's Right to Monitor Electronic Communication in the Workplace

Candice Padayachee

201501201

Supervised by: Darren Subramanien

DECLARATION

I, Candice Padayachee 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 …. day of ……..

Signature: ----------

Acknowledgements

To my husband, Enver and my two children, Kendall and Callum, thank you for your understanding, patience and love. Your continual support made it possible for me to complete this dissertation.

To my dearest friend, Dr Zaynab Essack, thank you for your invaluable input and for always making the time to listen to my challenges.

Lastly, to my supervisor, Darren Subramanien, thank you for the academic guidance in the production of this paper.

Abstract

This paper focuses on the employee's right to privacy versus the employer's right to access electronic communication in the workplace. This will be considered within the context of our common law and legislative provisions. The main aim of the dissertation is to determine the extent to which an employee's right to privacy is protected in the South African workplace given the significant advancements in technology.

ABBREVIATIONS

CCMA	Commission for Conciliation, Mediation and Arbitration
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedom
ECPA	Electronic Communications Privacy Act of 1986
EEA	Employment Equity Act 55 of 1998
IMPA	Interception and Monitoring Prohibition Act 127 of 1992
LRA	Labour Relations Act 66 of 1995
POPI	Protection of Personal Information Act, 4 of 2013
RICA	Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002
SALC	South African Law Commission

TABLE OF CONTENTS

CHAPTER ONE

1.1 BACKGROUND

The introduction of electronic communication into the workplace has permanently changed the way employers conduct their businesses and in turn the way employees are expected to perform their duties.[1] As a result of the increased electronic communication in the workplace, the physical employment environment has become infused with the electronic communication technology.[2] This has provided substantial benefits to employers such as cost effectiveness and enhanced productivity; however, the increased introduction of such communication also threatens to infringe an employee's right to privacy in the workplace.

The South African Constitution[3] guarantees an individual's right to privacy[4] including an individual's right not to have their communications infringed.[5] However, section 36 of the Constitution provides that all rights may be limited. The right to privacy is not an absolute right and has to be balanced with other rights. In this context it is argued that the employee's right to privacy has to be balanced with the employer's right to effectively manage the business in terms of business necessity and operational requirements. In the case of *Bernstein v Bester*[6] the Constitutional Court recognized the importance of the right to privacy but acknowledged that 'as a person moves into communal relations and activities such as business and social interaction the scope of personal space shrinks accordingly'.[7]

1.2 RESEARCH QUESTION

This dissertation will discuss the key question of whether an employee's right to privacy may be balanced against an employer's right to monitor its employee's electronic communication. In order to determine this issue, this dissertation will focus on the legal protection of the right to privacy within the constitutional and legislative framework, particularly in the workplace context.

[1] D Collier 'Workplace privacy in the cyber age' (2002) 23 *ILJ* 1743.
[2] T Pistorius 'Monitoring, interception and big boss in the workplace: is the devil in the detail?' (2009) *PER* 1.
[3] The Constitution of the Republic of South Africa, 1996.
[4] Ibid section 14.
[5] Ibid section 14(*d*).
[6] *Bernstein v Bester* 1996 (2) SA 751 (CC).
[7] Ibid at 789.

1.3 RESEARCH METHODOLOGY

The research methodology for this dissertation is desk-based. It involved a review and analysis of literature from journal articles, books, and case law that provide insight on the right to privacy as well as the employer's right to monitor and/or access its employee's electronic communication in the workplace. The material has been considered within the parameters of the constitutional and legislative framework and with due regard to the common law position on the right to privacy.

1.4 STRUCTURE OF DISSERTATION

Chapter one provides an introduction to the topic and describes the research question.

Chapter two examines the development of the legal protection of privacy in South Africa. The chapter commences by briefly focusing on the source of the right to privacy as protected in the international arena. It thereafter analyses the scope of the right to privacy in the South African context and considers the leading case law which illustrates the Courts' interpretation of the extent and limitation of this right.

Chapter three considers the primary focus of this dissertation, namely the extent to which privacy is protected in the workplace given the advancements in technology and the implications thereof. This chapter examines the key arguments in favour of employee monitoring. It then considers privacy within the context of the South African workplace and the legal precedents that have been established by the South African Courts.

Chapter four focuses on the extent to which an employer may monitor or intercept employees' electronic communication as regulated by South Africa's legislative framework. South African case law governing the application of such legislation is also considered.

Chapter five considers the scope and extent of the right to privacy in the United States with particular reference to the three primary sources of privacy protection: the US Constitution, Common Law, and Federal Statutes. The chapter examines the applicability of these sources of privacy in the employment context and analyses the dicta by the American Courts.

Chapter six sets out the conclusions of the dissertation.

CHAPTER TWO - THE RIGHT TO PRIVACY

2.1 INTRODUCTION

Privacy is considered a valuable and advanced aspect of an individual's personality.[8] It has been described as a basic human need that is fundamental to the development and advancement of both a free society and a mature and stable personality for an individual.[9] Moreover, the right to privacy is recognized by social scientists as essential for the preservation of an individual's human dignity including their physical, physiological and spiritual well-being.[10] An individual therefore has an interest in the protection of his or her privacy.[11]

The foundation of the right to privacy originates in the influential proclamations uttered, more than century ago by Brandeis and Warren, who described the right to privacy as an individual's 'absolute right to be left alone'.[12] Their thesis rests upon the fundamental notion that as society progresses and evolves, so to should the law.[13] This proclamation found resonance in many countries and as technological interventions began to emerge, from the introduction of the first hand-held camera to intervention of the internet, the interest in the right to privacy increased worldwide.[14] The concept of the right to privacy was extended from a simple right to be left alone to a much wider concept so as to include a person's right to have control over his or her personal information and affairs.[15]

However, as the right of privacy has evolved, it has been generally accepted that the concept of privacy is difficult to define due to it being vague and evanescent, or amorphous and elusive, often meaning strikingly different things to different people.[16] Nevertheless, according to most authors, privacy refers to that facet of a person's life in terms of which a certain 'measure of seclusion from others is maintained'.[17] Alan Westin reformulated the definition of privacy as: 'the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent

[8] SA Law Reform Commission Discussion Paper (Project 124 2005) *Privacy and Data Protection* at 49.
[9] GE Devenish *Commentary on the South African Bill of Rights* (1999) at 135.
[10] DJ McQuoid-Mason *The Law of Privacy in South Africa* (1978) xxxix.
[11] SA Law Reform Commission Discussion Paper op cit note 8 at 49.
[12] K Baum 'E-Mail in the workplace and the right to privacy' (1997) 42 *Vill. L. Rev*. 1011.
[13] K Kopp 'Electronic communications in the workplace: E-mail monitoring and the right of privacy' (1998) 8 *Seton Hall Const LJ* 861.
[14] SA Law Reform Commission Discussion Paper op cit note 8 at 39.
[15] A Roos 'Privacy in the Facebook era: A South African perspective' (2012) 129 *SALJ* 378.
[16] J Neethling 'The concept of privacy in South African law: notes' (2005) 122 *SALJ* 18.
[17] J Neethling et al *Law of Personality* (2004) 30.

information of them is communicated to others.'[18] Westin distinguishes measures of seclusion in four such states: 'Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical and psychological means, either in a state of solitude or small group intimacy or, when among larger groups, in a condition of anonymity or reserve.'[19] Accordingly, a person may not mind that another person knows a general fact about him/her, yet he may feel his privacy invaded if others know the details.[20]

Similarly, Gross defines privacy as that 'condition of human acquaintance with a person, or with affairs of his life which are personal to him, is limited'.[21] Moreover, Charles Fried, defined privacy as relating to the integrity of a person- furthering the ends of respect, love, friendship and trust. According to Fried, 'Privacy is not just an absence of information about ourselves; its a feeling of security in control over that information'.[22]

Having considered these definitions of privacy, Neethling argues that the crucial question is how to determine which facts regarding a person are private in nature. Neethling proposes that it is up to each person to determine this for himself, and in other words, he must cause the facts to be private[23]. In accordance with this principle, Neethling submits that the person must therefore also have the will, wish or desire that the facts should be kept private and, therefore privacy includes 'an individual condition of life characterised by seclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has himself [or herself] determined to be excluded from the knowledge of outsiders and in respect of which he [or she] has the will that they be kept private'[24]. From this definition, it is evident that a person determines the destiny of his private facts himself.[25]

This examination of a person's privacy has been increasingly deliberated over the last few decades as the fear in a technological age, of 'big brother' observing one's every activity, has captured the imagination of many authors.[26] Furthermore, the threat posed to personal privacy

[18] Roos op cit note 15 at 378.
[19] Westin in Neethling op cit note 17 at 30.
[20] J S Ressler 'Privacy, plaintiffs and pseudonyms: the anonymous doe plaintiff in the information age' (2004) 53 *Univ Kansas L Rev* 202.
[21] Gross in Neethling op cit note 17 at 30.
[22] Fried in J Burchell *Personality rights and freedom of expression: the modern actio injuriarum* (1998) at 366.
[23] Neethling op cit note 17 at 270.
[24] Ibid.
[25] Roos op cit note 15 at 396.
[26] Burchell op cit note 22 at 365.

has increased significantly due to the development of modern technology which has influenced the development of the right to privacy.

Consequently, the purpose of this chapter is to briefly focus on the source of the right to privacy as protected in the international arena. Thereafter, it will analyse the scope of the right to privacy in the South African context and consider a number of South African Court cases that illustrate the Courts' interpretation of the extent and limitation of this right.

2.2 INTERNATIONAL RECOGNITION OF THE RIGHT TO PRIVACY

The modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights[27], which also protects territorial and communications privacy.[28] Article 12 of the Declaration provides:

1 No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attacks on honour or reputation.
2 Everyone has the right to the protection of law against such interference or attacks.[29]

Following the Declaration, the right to privacy was also recognised in various other international instruments.[30] On a regional level, this recognition of the right to privacy was made legally enforceable by numerous treaties:

1 Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedom[31] ("ECHR")states that:

> '(1) Everyone has a right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country for the prevention of disorder or crime, for the protection of health of moral, or for the protection of the rights and freedoms of others.'

[27] Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 (III) of December 10, 1948.
[28] SA Law Reform Commission Discussion Paper op cit note 8.
[29] Op cit note 27.
[30] Recognized in instruments such as United Nations Conventions on the Rights of the Child, adopted by General Assembly resolution 44/25 of November 20, 1989, the International Covenant on Civil and Political Rights, adopted by General Assembly resolution 2200(A) XXI) of December 16, 1966; the United Nations Convention on Migrant Workers adopted by General Assembly resolution 45/158 of December 18, 1990.
[31] Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms open for signature November 4, 1950, entry into force September 3, 1950.

2 Articles V, IX and X of the American Declaration on Rights and Duties of Mankind.[32] The American Declaration of the Rights and Duties of Mankind was the first international human rights instrument adopted months after the Universal Declaration of Human Rights. This Declaration Article V states that 'Every person has the right to the protection of the law against abusive attacks upon his honor'. Article X states that 'Every person has the right to inviolability of the home'. Article XI states that 'Every person has the right to inviolability and transmission of his correspondence.

3 Article 11 of the American Convention on Human Rights.[33]This Convention is more elaborate than the American Declaration and provides for the protection of the individual's right to dignity and against arbitrary and abusive interferences of an individual's private life.
Article 11 states that 'Everyone has the right to have his honour respected and his dignity recognised. No one may be the object of arbitrary or abusive interferences with his private life, his family or correspondence, or of unlawful attacks on his or honour or reputation. Everyone has the right to the protection of the law against such interference of attacks.'

4 Protects individual honour, reputation, private life, the inviolability of the home and inviolability of correspondence.

Furthermore, it is important to note that the ECHR created the European Commission of Human Rights and the European Court of Human Rights to oversee the enforcement of the ECHR. Both these structures have made significant judgements on the meaning of protecting the right to privacy as articulated in Article 8.[34]

Finally, on a domestic level various countries have recognised the right to privacy either expressly or implicitly in their constitutions. These constitutional provisions differ by country but primarily protect the right to privacy of the home and communication. In this regard, countries such as Belgium, Finland, Namibia, Spain and Switzerland explicitly protect the right to privacy in their respective constitutions. By contrast countries such as Germany, the United States, Brazil Canada, Sweden, Denmark, Portugal and India recognise the existence of the right to privacy and implicitly protect the right to privacy by using other constitutional rights.

[32] Approved by the Ninth International Conference of America States, Bogota, Columbia, 1948.
[33] Pact of San Jose Costa Rica November 22, 1969 entered into force on July 18, 1978.
[34] SA Law Reform Commission Discussion Paper op cit note 8 at 51.

2.3 SOUTH AFRICA

2.3.1 PRIVACY PRIOR TO THE CONSTITUTION

In South Africa, the right to privacy enjoys substantial protection by both the common law and the Constitution.[35] However, this dual protection has not always been in place.[36]

Prior to the Constitution, there was no sophisticated concept of privacy.[37] The right to privacy was recognised by the common law in terms of the 'law of personality' and only emerged by implication in the 1950s.[38] In terms of the common law every person has personality rights that are protected by the law of personality, which in turn is regarded as part of the law of delict. [39]These personality rights include the right to physical integrity; the right to physical liberty; the right to good name or reputation; the right to dignity or honour; the right to privacy and the right to identity.[40] The available remedy in defence of these rights is *the actio injuriarum.*

However, the idea of an independent right to privacy, distinct from the general personality rights, in terms of the common law was initially not fully embraced by the South African Courts. It was evident from certain judgements that the Courts adopted a conservative approach, in recognising the right to privacy as being independent, by limiting the concepts of *dignitas* or honour and self-respect. [41] Furthermore, the limitation of the concept of *dignitas* resulted in insult being a requirement of the *injuria.*[42]

Notwithstanding this erstwhile position, this interpretation was altered by the Court in the case of O'*Keeffe v Argus Printing and Publishing Co Ltd and Other*[43], where the argument that the right to privacy should be equated with the right to dignity, was firmly rejected. Accordingly, this case became the *locus classicus* for the recognition of an independent right to privacy in South African law. In this case the plaintiff in O' Keefe, an unmarried woman, brought the *actio injuriarum* for the unauthorised use of her photograph and name in an advertisement for a company distributing rifles, pistols revolvers and ammunition. The plaintiff brought the action on the basis that the

[35] Op cit note 3.
[36] M Gondwe 'The Protection of Privacy in the Workplace: A Comparative Study' (unpublished PhD thesis, University of Stellenbosch, 2011) at 52.
[37] Burchell op cit note 22 at 372.
[38] Roos op cit note 15 at 378; *O Keeffe v Argus Printing and Publishing Co. Ltd & Others* 1954 (3) SA 244 (C).
[39] Neethling op cit note 17 at 3.
[40] Neethling op cit note 17 chapters 3-9.
[41] *S v A* 1971 (2) SA 293 (T) 297H, the defendants were accused of bugging the plaintiff's apartment. In his judgment, although Botha AJ recognized the right to privacy as an independent right, he restricted *dignita*s to dignity or honour; thus negating the existence of the independent right to privacy.
[42] Gondwe op cit note 36 at 54.
[43] *O'Keeffe* supra note 38.

advertisement had violated her dignity or *dignitas.* The defendant argued that insult had to be present in an *injuria.* In considering whether there had been an invasion of the plaintiff's privacy, Watermeyer AJ interpreted *dignitas* to include the whole legally protected personality except *corpus* (bodily integrity) and *fama* (reputation). Watermeyer AJ stated that as such *dignitas* includes not only a single right of personality, but all those rights in relation to dignity.[44]

Despite this decision, being criticised by scholars for failing to offer a comprehensive definition of privacy, and resulting in 'identity as a personality right [being] equated with privacy,'[45] this case signalled the start of the recognition of the right to privacy and the South African cases to follow began to fashion the concept of privacy.[46] For instance, in *S v A*[47] two private detectives placed a listening device under the dressing table of the complainant at the request of her estranged spouse. The Court found the two private detectives liable for invading the complainant's privacy. In reaching this decision, Botha AJ reiterated that the right to privacy is included in the concept of *dignitas* and further that the infringement of a person's privacy prima facie constitutes an impairment of his *dignitas*.[48] This principle was reaffirmed by the Court in the case of *S v I*[49] In this case, the appellants were held criminally liable for peeping through the complainants' bedroom window in an attempt to obtain evidence of infidelity. In reaching his decision, Beadle ACJ considered and applied the principles set out in *S v A*[50] and concluded that the protection of the right to privacy is subject to limitation and this would be determined by considering what is regarded as common to the community at a particular time. In addition, Beadle ACJ set out the elements that should be considered in protection of the right to privacy: 'the nature, incidence and occasion of the act or conduct and to the relationship, whether domestic or other, between the parties....'[51] The Court therefore found that the defendant's actions amounted to an invasion of privacy. However the invasion was seen to be justified given these actions were done with the *bona fide* intention of obtaining evidence against an adulterous husband.

Finally, in the case of *Kidson v SA Associated Newspapers Ltd*[52], the Court was called upon to consider the protection of the right to privacy in relation to the photographs of nurses taken by a journalist during their leisure time, without their permission. The photograph caption stated that

[44] Ibid at 248-249.
[45] Neethling op cit note 17 at 240.
[46] Roos op cit note 15 at 378.
[47] *S v A* supra note 41.
[48] Ibid at 297.
[49] *S v I* 1976 (1) SA 781 (RA).
[50] *S v A* supra note 41.
[51] Ibid at 297.
[52] *Kidson v SA Associated Newspapers Ltd* 1957 (3) SA 461 (W).

'97 Lonely Nurses want Boy Friends'. Kuper J determined that the publication on the alleged desire to meet persons of opposite sex because the nurses were lonely when they were off duty was an insult to the young married plaintiff, thus there had been an infringement of the right to privacy.

Consequently, it can therefore be concluded that the right to privacy is firmly established in the common law as an independent right of personality[53] and an infringement of dignity or insult plays no role in deciding whether there has been a violation of privacy.[54] Moreover, it is evident that the Courts are willing to have regard to the '*prevailing boni mores*' in deciding whether particular encroachments constitute an impairment of an individual's *dignitas*.

2.3.2 CONSTITUTIONAL RIGHT TO PRIVACY

In 1993, South Africa promulgated its first democratic Constitution of the Republic of South Africa.[55] The Bill of Rights contained within this constitution expressly recognised the right to privacy in terms of section 13:

> 'Every person shall have the right to his or her personal privacy, which shall include the right not to be subject to searches of his or her person, home or property, the seizure of private possessions or the violations of private communications.'

Subsequent to enactment of the Interim Constitution, in 1996 the Final Constitution was promulgated which entrenched the right to privacy within the Bill of Rights in terms of section 14 which states that:

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

(a) Their possession or home searched
(b) Their property searched
(c) Their possession seized or
(d) The privacy of their communication infringed.'

This enactment of the Constitution, with the express constitutional recognition of the right to privacy in this section and an independent right to dignity in section 10, furthermore confirms the independent existence of the right to privacy.[56]

[53] Neethling op cit note 17 at 219.
[54] Neethling op cit note 16 at 23.
[55] Act 200 of 1993.
[56] SA Law Reform Commission Discussion Paper op cit note 8 at 57.

Moreover, it is accepted that section 14 is interpreted has guaranteeing a general right to privacy as well as protecting against specific infringements of privacy.[57] According to McQuiod- Mason, section 14 can be divided into three groups:

a) Protecting privacy against intrusions and interferences with private life
b) Protecting privacy against disclosures of private facts
c) Protecting privacy against infringement of autonomy.[58]

For the purposes of this dissertation, it is the first and second groups that are of particular importance. However, it is should acknowledged that neither of these groups directly address the privacy challenges posed in the modern technology era.

Devenish[59] postulates that the use of the word 'include' in the second part of section 14 indicates that the specific breaches listed are not exhaustive and other unlisted breaches of privacy may be accommodated.

In addition, when considering section 14, it is of pivotal importance to consider the interrelated provision, section 2 of the Constitution. Section 2 provides that the Constitution is the supreme law of South Africa and any law or conduct inconsistent with it is invalid. This suggests that the Bill of Rights is applicable to all law, including the common law relating to the right to privacy and binds the state by vertical application. Furthermore the Bill also binds natural and juristic persons and for this reason has horizontal application. Both the vertical and horizontal application can be direct or indirect.[60]

- Direct vertical application requires the state to respect the fundamental rights contained in the Bill of Rights, in so far as such infringement is reasonable and justifiable in terms of the limitation clause (section 36 of the Constitution).
- Direct horizontal application requires the Court to give effect to applicable fundamental rights by applying and developing the common law to the extent that the legislation fails to do so, except where it is reasonable and justifiable to develop the common law to limit the relevant rights in accordance with the limitation clause.
- Indirect application of the Bill of Rights requires that all legal rules, principles or norms be subject to and must thus be content in accordance with the spirit , objects and purport of the Bill of Rights.[61]

[57] Ibid at 49.
[58] SA Law Reform Commission Discussion Paper op cit note 8 at 61.
[59] Devenish op cit note 9 at 138.
[60] J Neething *Law of Delict* (2006) 19-23.
[61] SA Law Reform Commission Discussion Paper op cit note 8 at 53.

2.3.3 INFRINGEMENT OF THE RIGHT TO PRIVACY

The constitutional right to privacy like its common law counterpart, is not an absolute right but may be limited in terms of the law of general application and has to be balanced with other rights entrenched in the Constitution.[62] This principle was confirmed in the case of *Case v Minister of Safety and Security*[63] where the Court stated that 'the protection accorded to the right of privacy is broad but it can also be limited in appropriate circumstances'.[64]

According to section 36 of the Constitution, the rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including:

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

The factors mentioned in section 36 are, however, not exhaustive.[65] They are key considerations, to be used in conjunction with any other relevant factors, in the overall determination of whether a limitation is justifiable.[66] Therefore, in each instance a careful balancing of the right to privacy and the opposing interests or rights will have to take place.[67] In order to establish an infringement of the constitutional right to privacy the plaintiff will have to show that he or she had a subjective expectation of privacy which was objectively reasonable.[68]

Essentially, the following enquiry is conducted:

a) Has the invasive law or conduct infringed the right to privacy in the Constitution?

b) if so, is such an infringement justifiable in terms of the requirements laid down in the limitation clause of the Constitution?[69]

[62] Ibid at 49.
[63] *Case v Minister of Safety and Security* 1996 (3) SA 617 (CC).
[64] Ibid at para [106].
[65] *S v Makwanyane* 1995 (3) SA 391 (CC) at 708.
[66] *S v Manamela & Another (Director-General of Justice Intervening)* 2000 (3) SA 1 (CC).
[67] SA Law Reform Commission Discussion Paper op cit note 8 at 65.
[68] Neethling op cit note 17 at 221.
[69] G Devenish 'The limitation clause revisited – the limitation of rights in the 1996 Constitution' (1998) *Obiter* 263.

According to De Waal, the scope of a person's right to privacy extends only to those aspects of his or her life or conduct about which a legitimate expectation of privacy can be harboured.[70] He states further that a 'legitimate expectation' means that one must have a subjective expectation of privacy that society recognises as objectively reasonable.[71] This test was developed by the South African Courts, following the decisions of courts in the United States and Canada.[72] The subjective component of the test recognises that a person cannot complain about an invasion of privacy if he or she has consented explicitly or impliedly to it. The objective component test, which is more important but difficult to assess, provides that the expectation must be recognised as reasonable by society.[73] This assertion was reinforced by the Constitutional Court, which noted, in its analysis that the continuum, on which the legitimacy of an expectation of having one's privacy respected may fall, that 'this inviolable core is left behind once an individual enters into relationships with persons outside this closest intimate sphere; the activities then acquire a social dimension and the right of privacy in this context becomes subject to limitation'.[74]

In terms of the common law, the test regarding whether there has been an infringement of privacy is a single enquiry: Has there been an unlawful and intentional interference with a legally protected interest.[75] For common-law action for invasion of privacy based on the *actio injuriarium* to succeed, the plaintiff must prove the following essential elements:

i) impairment of the applicant's privacy
ii) wrongfulness, and
iii) intention.[76]

In the case of *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another*[77], the Court held that a breach could occur by an unlawful intrusion upon the personal privacy of another, or by unlawful disclosure of private facts about a person. The Court held further that the unlawfulness of an infringement of privacy is adjudged 'in light of the contemporary *boni mores* and the general

[70] J De Waal, I Currie *The Bill of Rights Handbook* 5ed (2005) at 267.
[71] Ibid at 269.
[72] M McGregor 'The right to privacy in the workplace: general case law and guidelines for using the internet and e-mail' (2004) 16 *SA Merc LJ* 638 at 640.
[73] Ibid.
[74] *Bernstein* supra note 6 at para [77].
[75] Ibid.
[76] SA Law Reform Commission Discussion Paper op cit note 8 at 67.
[77] *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another* 1991 (2) SA 11 (W).

sense of the community as perceived by the Court[78]. Often a decision on the issue of unlawfulness will involve a consideration and balancing of competing interest.[79]

In accordance with the sentiments expressed in the *Financial Mail* case, our Courts have recognised examples of wrongful intrusion and disclosure at common law as being entry into a private residence[80], the reading of private documents[81] , listening to private conversations[82], the shadowing of person [83] and the disclosure of private facts acquired by a wrongful act of intrusion.[84]

2.3.4 THE RIGHT TO PRIVACY THROUGH COURT DECISIONS

Despite the right to privacy been given constitutional affirmation in terms of section 14, this section does not expressly define the concept of privacy. It has therefore been left to the South African Courts to shape the scope and extent of this right together with its corresponding limitations. In fact, it is submitted that it is in situations like this, where jurisprudence becomes relevant and important, since it is the task of jurisprudence to precisely describe those interests of personality that the law protects in order to render them dogmatically and practically manageable, and in this way to bring about legal certainty.[85]

The *locus classicus* of the interpretation of the right to privacy is the landmark Constitutional Court judgement of *Bernstein v Bester[86].* This decision has been acknowledged as representing the 'richest and most comprehensive interpretation of the right to privacy'.[87] In this judgement, Ackerman J reinforced the sentiment that the 'concept of privacy is an amorphous and elusive one which has been the subject of much scholarly debate'.[88] The issue before the Court was the constitutionality of sections 417 and 418 of the Companies Act 61 of 1973, providing for the examination of persons and the disclosure of documents on company affairs. The applicants contended that sections 417 and 418 were unconstitutional on several grounds, including the right to privacy. After considering and applying international law, Ackermann J found that 'the scope of privacy has been closely related to the concept of identity and it has been stated that

[78] Ibid at para [40].
[79] Ibid at para [45].
[80] *S v I* supra note 49.
[81] *Reid-Daly v Hickman & Others* 1981 (2) SA 315 (ZA).
[82] *S v A supra note 41*.
[83] *Epstein v Epstein* 1906 TH 87.
[84] *Financial Mail* supra note 77.
[85] Neethling op cit note 16.
[86] *Bernstein* supra note 6.
[87] De Waal & Currie op cit note 70 at 14.2 – 14.3.
[88] Ibid at paras [787]-[788].

rights, like the right to privacy, are not based on the a notion of the unencumbered self, but on the notion of what is necessary to have one's own autonomous identity'.[89]

In considering the extent of this right and potential infringement thereof, Ackermann J went further to state that:

> 'The truism that no right is considered to be 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 it is only the inner sanctum of a person such as his/her family life, sexual preference and home environment which is shielded from erosion by conflicting rights of the community...Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks'.[90]

This sentiment was subsequently echoed in the case of *National Media Ltd v Jooste*[91], where the Court reinforced the dictum in the *Bernstein* case and held that:

> Privacy is an individual condition of life characterised by exclusion from the public and publicity. This condition embraces all those personal facts which the person concerned has determined himself to be excluded from the knowledge of outsiders and in respect of which he has the will that they be kept private.[92] (translation from Afrikaans).

Likewise, in the case of *Mistry v Interim Dental Council of South Africa*[93], the Court illustrated that the 'degree of privacy that a citizen can reasonably expect would vary significantly according to the activity that bring him or her in contact with the state'.[94] In this case, the Court was called upon to consider the constitutionality of section 28 (1) of the Medicines and Related Substances Act 101 of 1965, which granted inspectors of medicines the authority to enter and inspect any premises, place, vessel or aircraft in which they reasonable believe medicines or substances regulated by the Act are housed. In terms of this section, the applicant's surgery was searched and numerous items were seized. In considering the nature of the right to privacy, the Court held that 'the existence of safeguards to regulate the way in which State officials may enter the private domains of ordinary citizens is one of the features that distinguish a constitutional democracy from a police state'.[95] The Court concluded that 'the more public the undertaking the more closely

[89] Ibid at para [788].
[90] Ibid at para [789].
[91] *National Media Ltd v Jooste* 1996 (3) SA 262 (A) at 271.
[92] Neethling op cit note 17 at 32.
[93] *Mistry v Interim Dental Council of South Africa* 1998 (4) SA 1127 (CC) at 1127.
[94] Ibid at 1142.
[95] Ibid.

regulated, the more attenuated would the right to privacy be and the less intense any possible invasion'.

Subsequently, the Court in the case of *National Coalition for Gay and Lesbian Equality v Minister of Justice*[96], considered the right to privacy as it extended to homosexuality. The Court held that 'privacy recognises that we all have a right to a sphere of private intimacy and autonomy, which allows us to establish and nurture human relations without interference from the outside community…'[97] In a separate concurring judgement, Sachs J went on to submit that privacy protects people and not places and imposes a duty in creating an environment in which personal realisation can thrive.[98] The principles in this judgement found support in the case of *S v Jordaan*[99], wherein the applicants contested the prohibition on prostitution. However, although the Court in this instance reinforced the dicta of Sach J in the *National Coalition* case it refused to afford the concerned sexual activity the same privacy protection. It went on to hold that the facts of this case were different, in that *Jordaan's* case concerned the commercial exploitation of sex which involves neither an infringement of dignity or unfair discrimination'. [100]
However, the above dictas relating to the extent of the right to privacy have been criticised by Neethling as being 'too restrictive'.[101] Neethling disagrees with this interpretation of privacy as he is of the view that it negates other private facts relating to a person worthy of protection. This applies particularly to the whole area of data protection where the information collected about a person is often not of a most personal nature, or some of the data, taken on their own, are not even private according to the above description of privacy, but the total picture thereof is usually of such a nature that the person concerned determines the destiny of the data to be private and therefore also has the will to keep them private.[102]

Neethling's criticism was subsequently validated in the decision of *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 Smith NO and Other.*[103] In this judgement, Langa DP found in contrast to the Bernstein case, stating that the right to privacy, in terms of the

[96] *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 (CC).
[97] Ibid at 6 30B.
[98] Ibid at 6 61A.
[99] *S v Jordaan* 2002 (6) SA 642 (CC).
[100] Ibid at 654 I.
[101] Neethling op cit note 17 at 32.
[102] Ibid at 20.
[103] *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 Smith NO and Other* 2011 (1) SA 545 (CC).

Constitution, should not be understood to mean that persons no longer retain such a right in the social capacities in which they act. Langa DP stated that:

> 'When people are in their offices, in their cars or on mobile telephones, they still retain the right to be left alone by the State unless certain conditions are satisfied. Where a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable, the right to privacy will come into play.'[104]

Langa DP stated further that privacy 'is a right which becomes intense the closer it moves into the intimate personal sphere of the life of human beings, and less intense as it moves away from the core'[105]. Consequently, this judgement confirmed that section 14 does not only relate to the 'truly personal realm' or 'inner sanctum' but individuals still retain this right to privacy when venturing outside of the 'truly personal realm'.

2.4 CONCLUSION

This chapter sought to explore the recognition and extent of the right to privacy in South African Law by focusing on the development of the legal protection of privacy in the country. Based on the preceding discussion, it is evident that despite the concept of privacy being difficult to define, the right to privacy has still been recognised, both internationally and domestically, as one of the most important human rights.

In South Africa, the right to privacy is protected by both the common law and the Constitution. Although, in the early centuries there was no sophisticated concept of privacy in terms of the common law and the Courts took a conservative approach equating privacy with the concept of *dignitas*. Notwithstanding, this position was transformed in the 1950's when the Court in the O'Keefe decision recognised the right to privacy as an independent right, distinct from general personality rights.

Subsequently, the enactment of the Constitution, with the express constitutional recognition of the right to privacy confirmed the independent existence of the right to privacy as well as the high premium to be placed on this right. However, clearly the right to privacy is not an absolute one and may be limited by having to be balanced with other rights entrenched in the Constitution. Moreover, the Constitution does not provide an express definition on the scope and extent of the right to privacy. This has culminated in the South African Courts being called upon to shape the scope of this right. In doing so, the Constitutional Court has reaffirmed the independent nature of

[104] Ibid at 545-557.
[105] Ibid.

the right to privacy and established various fundamental facets of privacy, the most pivotal being, the principle that 'the protection of privacy lies along a continuum, where the more a person inter-relates with the world the more the right to privacy becomes attenuated[106]. The continuum starts in the wholly inviolable inner self, then moves to the impervious sanctum of the home and the personal life and ends in the public realm where the right to privacy would only be remotely implicated'.[107]

In the subsequent chapter, this dissertation will focus on the right to privacy and its limitation in an employment context as well as the impact of modern technology on this relationship.

[106] *In re Hyundai Motor Distributors* supra note 103 at 556-557.
[107] Neethling op cit note 17 at 222.

CHAPTER THREE - RIGHT TO PRIVACY IN WORKPLACE

3.1 INTRODUCTION

The modern workplace has dramatically changed in the last two decades with the dawn of the technological revolution.[108]Today's workplace is now characterised by its reliance on computer technology, particularly the use of email and the internet to perform critical business functions.[109] This reliance has been further revolutionized by the introduction of social media, instant messaging and electronic communication devices, such as mobile devices and electronic notebooks, which has infused the physical employment environment with the home environment and has resulted in the border between the office and home becoming unclear.[110]

Consequently, this increased development and introduction of technology has significantly influenced the concept of the right to privacy in an employment context and has in turn, sparked widespread debate about the privacy of employees versus the employers' entitlement to monitor and regulate the employees' communication. On the one hand, there is the principle that employees are entitled to the right to privacy and this right is not ceded when employees sign an employment contract. [111] On the other hand, there is the right of the employers to enjoy their property and exercise their managerial powers of command to protect their property against abuse that may cause damage to the employer's business.[112] The key questions to be answered, therefore, are whether: employers should be entitled to have access or to monitor employees' electronic communication in the workplace? Conversely, should, or do, employees have a reasonable expectation of privacy?

Having said that it is noteworthy and of significance to this dissertation, that the monitoring of employee communications by employers is not a new phenomenon. [113] The monitoring of employees by employers definitely occurred before the introduction of electronic communication[114]. Nonetheless, in the information age employers have assumed other methods of monitor their business operations for the many reasons which will be expanded on below.

---

[108] L Court and C Warmington 'The workplace privacy myth: why electronic monitoring is here to stay' (2004) 29 *Okla. City U L Rev* 15.
[109] J Watt Electronic *Workplace Surveillance and Employee Privacy – A Comparative Analysis of Privacy Protection in Australia and the United States* (unpublished LLM thesis, Queensland University of Technology, 2009) at 55.
[110] Pistorius op cit note 2.
[111] Gondwe op cit note 36 at 144.
[112] Ibid at 144.
[113] Ibid at 258.
[114] In the past employers monitored use of company resources by using onsite managers at work to ensure that employees were being productive and efficient.

Accordingly, the goal of this chapter is to consider the issue that constitutes, the primary focus of this dissertation, namely the extent to which privacy is protected in the workplace given the advancements in technology and the implications for the right to privacy as such. In achieving this goal, this chapter will examine the key arguments made in favour of employee monitoring and the converse arguments relating to why employee privacy is important. It will then proceed to consider the South African context of 'Privacy in the Workplace' and the legal precedents that have been submitted by the South African Courts.

3.2 ARGUMENTS IN FAVOUR OF EMPLOYEE MONITORING

It is abundantly evident that technology has changed the landscape of the workplace environment. In many businesses, email has replaced the telephone for the purposes of casual electronic conversation and much employee communication, such as the inter-office memorandum, now takes place over private or public networks. [115] In addition, the use of the internet is unmistakably an imperative business tool which facilitates efficient work and often makes it easier for employees to perform their tasks.[116]

Nevertheless, the rise in technology has been a double- edged sword for employers. On the one hand, it is a vital business tool, but on the other it poses significant threats to employers' interest. Employers face serious risks from employee abuse of these communication mediums[117] and are forced to deal with the difficulty in trying to police the information which employees either access or disseminate in the business environment. [118] This has resulted in employers resorting to employee monitoring mechanisms in order to mitigate the risks.

To examine the legal implications of employee monitoring and interception of communication in the workplace and its effect on the employees' right to privacy, it is first necessary to consider the reasons motivating employers to monitor employees:

3.2.1 VICARIOUS LIABILITY

One of the foremost reasons for monitoring employee communication is in order to manage the risk of employer liability to third parties. [119] Given the nature of electronic communication,

[115] M Modiba 'Intercepting and monitoring employees' e-mail communication and internet access' (2003) 15 *SA Merc L* 365.
[116] D Subramanien and N Whitear-Nel 'A fresh perspective on South African law relating to the risks posed to employers when employees abuse the internet' (2013) 37 *SALJ* 10.
[117] J Yerby 'Legal and ethical issues of employee monitoring' (2013) 1 *Online Journal of Applied Knowledge Management* 44.
[118] V Etsebeth 'The growing expansion of vicarious liability in the information age (part 1)' (2006) 2 *TSAR* 564.
[119] Subramanien and Whitear-Nel op cit note 116 at 11.

whereby information can be transmitted instantaneously by a simple push of a button, employers are vulnerable and may be exposed to legal liability in cases of inappropriate use of the electronic communication tools.[120]This liability may extend from harassment, discrimination, defamation, copyright infringement, criminal liability and even liability under contract law.[121]

In South Africa, it is a principle of common law that an employer may be held jointly and severally liable with an employee for an employee's wrongful acts committed in the course and scope of the employee's duties.[122] This doctrine was first expressed in the case of *Feldman (Pty) Ltd v Mall*[123], wherein the Court held that

> '…a master who does his work by the hand of a servant creates a risk of harm to others if the servant should prove to be negligent or inefficient or untrustworthy….it follows that if the servant's acts in doing his mater's work of his activities incidental to or connected with it are carried out in a negligent or improper manner so as to cause harm to a third party the master is response for that harm…' [124]

This principle is based the doctrine of liability without fault in terms of which one person is held liable for the unlawful acts of another.[125] The most common reasoning behind this doctrine is the belief that a person who employs others to advance his own economic interest should in fairness be placed under a corresponding liability for losses incurred in the course of the enterprise.[126] Essentially it is based on the justification, that the victim should enjoy fair and just compensation (out of the deeper pocket of the employer), this is so because the employer is better equipped to spread the cost of compensating victims by taking out insurance and by price increases that employers will take measures to prevent employees from causing damage to third parties if they will be held liable for the acts of their employees.[127] The doctrine therefore is intended to encourage employers to take active steps to prevent their employees from harming others.[128]

In order for vicarious liability to be met, the following requirements must be present[129]:

---

[120] A survey by the American Management Association (at http//www.amanet.org) revealed that 68% of employers who monitor employees' emails and Internet use cite legal liability as their primary motivation.
[121] Etsebeth op cit note 118 at 565.
[122] C Mischke 'Workplace privacy, e-mail interception and the law' (2003) 12 (8) CLL 72.
[123] *Feldman (Pty) Ltd v Mall* 1945 AD 733.
[124] Ibid at 741.
[125] Etsebeth op cit note 118.
[126] K Calitz 'Vicarious liability of employers: reconsidering the risks as the basis of liability' (2005) 2 *TSAR* 215.
[127] Ibid.
[128] *NK v Minister of Safety & Security* 2005 (6) SA 40 (CC) at para [21].
[129] Etsebeth op cit note 118 at 578.

a) There must be an employment relationship
b) The employee's conduct must have been unlawful
c) The act of the employee must have led to a third person suffering damages
d) The act must have taken place within the scope of his or her employment. The test to determine whether or not an employee was acting in the course and scope of his employment was laid down in the case of *Minister of Safety and Security v Jordaan*[130], where Scott JA stated as follows:

> '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....'[131]

Similarly, in the case of *Boland Bank Bpk v Bellville Municipality*[132], the Court held that in order to determine whether an act was committed in the scope of employment, one must ask whether the act in question whilst busy with an act closely enough related to his employment tasks.[133]

However, having considered the aforesaid test, it is important to note that our Courts have grappled with the meaning of this requirement, especially in the cases of acts in contradiction of the employer's instruction.[134] In the earlier decisions, the South African Courts were reluctant to hold an employer vicariously liable for acts committed outside the employee's authority and not in furtherance of the employer's business.[135] Consequently, to deal with the difficulty, the Courts developed certain sub-rules, which included certain 'deviation cases'.[136] Accordingly, the Courts took the degree of deviation into account and although it was not possible to lay down hard and fast rules, the Courts developed the following principles:[137]

- The act would be regarded as having been done within the scope of employment of the employee did not deviate too far from acts authorised by the employer.
- If the employee subjectively completely abandoned his or her work, but there was objectively still a close connection between his or her employment and the act which caused the damage, the act would still be regarded as being within the scope of the employment.

[130] *Minister of Safety and Security v Jordaan* 2000 (4) SA 21 (SCA).
[131] Ibid at par [5].
[132] *Boland Bank Bpk v Bellville Municipality* 1981 (2) SA 437 (C).
[133] Ibid at 444-445.
[134] Calitz op cit note 126 at 216.
[135] Ibid.
[136] M Botha and D Millard 'The past, present and future of vicarious liability in South Africa' (2012) *De Jure* 225 at 230.
[137] Calitz op cit note 126 at 218.

These principles were demonstrated in the well-known case of *Viljoen v Smith*[138], wherein an employer was held liable for damages caused to a neighbouring farm by a veld fire. The employee had started the fire by lighting a cigarette on a neighbouring farm, despite the fact that the employer had specifically forbidden employees to go on the neighbouring farm. The Court held that the employer could only escape liability if the employee had entirely abandoned his employment.[139] The Court went on to consider the distance of the digression to the neighbouring farm and found that it could not be said that the employee abandoned his employment. [140]

Nevertheless, the position has been altered by the case of *Grobler v Naspers Bpk.*[141], which judgement has particular relevance to this dissertation. In this case, the Court re-examined the test for vicarious liability to include a circumstances where an employer may also be held vicariously liable even if the employee is engaged in activities other than the duties prescribed by his employer.[142] The facts of the case were that, the employee, a trainee manager, had sexually harassed his secretary resulting in the secretary suffering from emotional trauma. The secretary, in turn, claimed damages from the employer on the basis of vicarious liability. The Court concluded that that an employer may be held liable on the ground that the work relationship created a risk of harassment or enhances such a risk and that the harassment took place in the employment relationship.[143]

The outcome of this judgement therefore resulted in a shift away from the rigid test set down in the *Feldman* case towards favouring a 'sufficiently close connection' test.[144] The test ultimately provides that provided that the servant is doing his master's work or pursuing his employer's ends, he is acting within the scope of his employment even if he disobeys the employer's instructions as to the manner or the means to do the work.[145] This is important as it therefore rules out an employer's argument that the organisation should not be held liable to the claimant, because he or she did not authorise the inappropriate and harmful use of the workplace facilities.[146]

In the present context, the doctrine is therefore pertinent when considering circumstances relating to the viewing or circulating of racist material or pornography over the company's facilities and/or in sight of other employees thereby potentially causing harm to other employees.

---

[138] *Viljoen v Smith* 1997 (18) *ILJ* 61 (A).
[139] Ibid at 67.
[140] Ibid.
[141] *Grobler v Naspers Bpk* 2001 (4) SA 938 (LC).
[142] Ibid.
[143] Ibid.
[144] Etsebeth op cit note 118 at 579.
[145] Ibid.
[146] Subramanien and Whitear-Nel op cit note 116 at 12.

It is abundantly evident then that employers need to concern themselves with the activities of their employees as it stands to reason that the close connection test may also be used in the electronic communication domain.[147] An employer may, for instance, be held liable for various 'cyber liability' claims, which are discussed below.

3.2.2 SEXUAL HARASSMENT AND DISCRIMINATION

Sexual harassment and/or discrimination can occur by electronic communication where, for instance, an employee circulates electronic communication containing racist, derogatory or sexually offensive material.

In South Africa, in addition to the common law vicarious liability doctrine, in terms of the Employment Equity Act 55 of 1998 (EEA), an employer is compelled to combat unfair discrimination in the workplace, which includes harassment.[148] The Act goes further, in terms of section 60, to create a form of statutory vicarious liability for employers. According to this section, an employer would be rendered liable if an employee contravenes a provision of the EEA while at work in respect of another employee and if there is a failure by the employer to take the reasonable necessary steps to eliminate or prevent the contravention.

Sexual Harassment is the most widely reported form of Harassment.[149] In terms of the Code of Good Practice on the Handling of Sexual Harassment Cases in the Workplace [150], sexual harassment is defined as:

> '..unwelcome conduct of a sexual nature that violates the rights of an employee and constitutes a barrier to equality in the workplace, taking into account all the following factors:
>
> - Whether the harassment is on the prohibited grounds of sex and/or gender and/or sexual orientation;
> - Whether the sexual conduct was unwelcome;
> - The nature and extent of the sexual conduct; and
> - The impact of the sexual conduct on the employee.'

[147] Collier op cit note 1; Etsebeth op cit note 118 at 579.
[148] Section 5 and 6 of EEA.
[149] A Landman and MM Ndou 'The Protection from Harassment Act and its implications for the workplace' (2013) 22 (9) *Contemporary Labour Law* 81 at 89.
[150] Promulgated by Notice 1367 in GG 19049 of 17 July 1998.

The Code provides further that the harassment can include physical, verbal or non-verbal conduct.[151] Furthermore, a single incident of unwelcome sexual conduct may constitute sexual harassment.[152]

Our Courts have been called upon to consider the extent of an employer's liability in terms of the EEA relating to sexual harassment in the workplace:

In the case of *Ntsabo v Real Security*[153], which was the first case of sexual harassment under the EEA, the Labour Court had to consider a claim for compensation for an automatically unfair dismissal and damages for pain and suffering, humiliation, impairment of dignity and trauma. Briefly, the facts of the case were that Ms Ntsabo was repeatedly sexually harassed by her supervisor. After bringing the incidents to the attention of the employer, the employer attempted to resolve the matter by transferring Ms Ntsabo to another site to work at night. Ms Ntsabo subsequently resigned and thereafter brought an action of automatic constructive dismissal against the employer.

The Court found that the employer's conduct constituted a contravention of the EEA as the employer failed to consult and take reasonable steps to eliminate the harassment. As a result, the employer was vicariously liable for the damages in terms of section 60 (2) of the EEA. Significantly, in reaching its decision, the Court held that an employer will not be held liable in terms of section 60 of the EEA, where there is one incident of sexual harassment, which is brought to the attention of the employer immediately after the incident.[154] Similarly, in the case of *Mokoena & Another v Garden Art (Pty) Ltd*[155] the Court held that an employer may not be held liable for a single incident of harassment because it could not had been prevented by the employer.

As an aside - in addition to the EEA and the Code of Good Practice, South Africa further enacted the Protection from Harassment Act.[156] This Act came into force on 27 April 2013 and affords victims of harassment an effective remedy against such behaviour and introduces measures which will enable the relevant organs of state to give effect to the provisions of the Act.[157] Essentially, the Act permits any person who alleges that that he or she is being subjected to harassment to apply to a Magistrate's Court for a protection order against the harassment.

---

[151] Item 4.
[152] Section 3(2) *(a)-(c).*
[153] *Ntsabo v Real Security* (2003) 24 *ILJ* 2341 (LC).
[154] Ibid at 2347 B-G.
[155] *Mokoena & Another v Garden Art (Pty) Ltd* (2008) 29 *ILJ* 1190 (LC).
[156] Act 17 of 2011.
[157] Landman and Ndou op cit note 149 at 89.

Thus, the impact of the provisions of this Act on employers is essentially in the instances where the harasser is employed at the same worksite as the 'complainant'. In such cases, the employer may be obliged to take measures to ensure compliance with the protection order.[158] Furthermore, should the harasser be an employee and use the employer's electronic facilities in the course of the alleged harassment, the employer could be faced with a request for the disclosure of information which accompanies the harasser's communication.[159] Section 18 (5) of the Act makes the failure to provide, such information an offence.

3.2.3 DEFAMATION

Defamation has been defined to be the 'wrongful, intentional publication of words or behaviour concerning another person which [have] the effect of injuring his status, good name or reputation'.[160] As a result, an employer may be liable for a defamatory email or electronic posting sent by an employee in the course of his or her employment, provided that the requirement of 'publication' has been met.[161] In determining whether the content of an email is defamatory, it must be ascertained:

> 'Whether a reasonable person of ordinary intelligence may reasonably understand the email to convey a defamatory meaning as regards the plaintiff'[162]

The question of what would exactly constitute a publication on the internet was considered in the case by the Supreme Court of Appeal in the case of *National Media v Bogoshi*[163]. In this case, the Court submitted 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. Consequently, the requirement of publication will be met when a defamatory statement that impairs the reputation of a third party is spread and read by others through an employer's electronic communication.[164]

Based on this definition of 'publication', it can be inferred that acts of postings to a newsgroup, sending an email, making a website available on the internet, internet relay chat and file transfer – will amount to publication.[165]

---

[158] Ibid at 87.
[159] Ibid.
[160] Neethling, et al *Law of Delict* (2006) 307.
[161] M Van Jaarsvel 'Forewarned is forearmed: some thoughts on the inappropriate use of computers in the workplace' (2004) 16 *SA Merc LJ* 651 at 663.
[162] Ibid.
[163] *National Media v Bogoshi* 1998 (4) SA 1995 (SCA).
[164] Van Jaarsvel op cit note 161.
[165] V Etsebeth 'The Growing Expansion of Vicarious Liability in the Information Age (part 2)' (2006) (4) *TSAR* 755.

An example of a case concerning a derogatory email sent by an employee, is the case of *CWU v Mobile Telephone Networks (Pty) Ltd*.[166]The facts of the case were briefly that the employee had circulated two emails that alleged that MTN's management was corrupt and bias towards a certain temporary employment agency. MTN retaliated by charging the employee with abusing company tools and privileges, in that he had used the tools to circulate an email that exposed MTN to liability by its clients. In turn, the employee instituted an urgent application against MTN to compel it to have his suspension uplifted.

In casu, the Court found that by sending the email the employee waived the protection offered to him by the Protection of Disclosure Act[167] and by his actions he increased the reputational damage to MTN. Furthermore, the Court held that in the circumstances, there were grounds on which MTN's clients could institute a vicarious liability claim against MTN.

Finally, other instances where an employer may face vicarious liabilities claims include:

- Copyright infringements, where an employee, in the course of business, breaches the intellectual property rights of another through his or her online activities, even though the employer was unaware of the breach. It is of particular relevance to note, that in terms of the survey conducted by Dancaster,[168] 15.69 % of employees admitted to violating copyright laws or posting information in the name of their company that defames other companies or individuals.
- criminal activity and or civil liability, where an employee disseminates child pornography and/or other unlawful obscene material.

3.2.4 PRODUCTIVITY AND EFFICIENCY

Although, tools such as the Internet and email are integral parts of the typical worker's daily routine, they are also tools which possess capacity for distraction to employees[169]. This capacity of distraction has been significantly increased by the advent of social networking sites.[170]. It is contended then that the computer has usurped gossiping in the coffee room or talking on the telephone as the leading waste of corporate time.[171] It is therefore contended that giving employees' open, unmonitored access causes productivity and efficiency to suffer[172]. The argument is based generally on the premise that employees who abuse electronic communication

[166] *CWU v Mobile Telephone Networks (Pty) Ltd* (2003) 8 BLLR 741 (LC).
[167] Act 26 of 2000.
[168] Collier op cit note 1 at 1766.
[169] Subramanien and Whitear-Nel op cit note 116 at 10.
[170] Ibid.
[171] R Freeman and K Martin, 'Some problems with employee monitoring' 2003 (43) *Journal of Business Ethics* 353.
[172] Yerby op cit note 117 at 45.

tools for purposes other than work lower the business's productivity level because if they are 'surfing the web' or engaging on social network sites, they are not doing the job that they were hired to do.[173]

This argument is firmly advanced by Westin who contends that privacy- based objections against the use of monitoring devices in the workplace is really a disguise protests against worker supervision and poses a threat to 'central societal interests in quality of work'.[174] Westin postulates that in this context, the concept of 'Privacy' is one that has been exploited 'as emotionally-charged weapon in the ongoing power struggle between management and unions.[175]

This argument also appears to be supported by various international research surveys which have revealed that:

- 30% to 40% of Internet use in the workplace is not business related[176]
- 37% of workers say that they surf the web constantly at work on personal rather than business matters[177]
- Many employees report using the Internet to read the news each day and make travel arrangements, check stocks and to shop for gifts.[178]

Additionally, the survey by Vault.com revealed that Email is also a productivity culprit, with half of the employees surveyed admitting to sending and/or receiving one to five non-work related emails each work day.[179]

From a South Africa perspective, a similar sentiment was revealed in a survey which was conducted with 644 companies listed on the Johannesburg Stock Exchange.[180] According to this survey, which had a response rate of 25.4%: 68.63% of employees admitted to 'loafing' on the internet. As a result, the impact on employers can be significantly detrimental. In fact, it has been estimated that a company with 500 Internet users could lose almost a million dollars in productivity annually from just a half hour of daily Internet surfing by employees.[181] Consequently, it stands to reason that employers will favour employee monitoring and actively

[173] GFI White Paper 'Internet Monitoring not 'Big Brother' but 'Wise Management'" available at *http://www.gfi.com/whitepapers/Internet_Monitoring.pdf,* accessed on 21 November 2014 at 3.
[174] K Conlon 'Privacy in the workplace' (1996) 72 *Chicago-Kent Law Review* 292.
[175] Ibid.
[176] GFI White Paper op cit note 173.
[177] Vault.com. 'Survey Internet Use in the Workplace' Fall 2000 available at http://www.vault.com/surveys/internetuse2000/results/2000, accessed on 21 November 2014.
[178] Results from Vault.com Survey ibid.
[179] Ibid.
[180] L Dancaster 'Internet Abuse: a survey of South African companies' (2001) 22 *ILJ* 862.
[181] Court and Warmington op cit note 108 at 18.

seek to monitor electronic communication of employees in order to maintain and enhance productivity and efficiency.

This was illustrated in the decision of *Bamford & Others/ Energiser SA Ltd* [182] where employees was dismissed after being charged for abuse of the email. The employer had circulated an email instructing employees to refrain from sending chain emails on the company network and on company time. The employees had ignored the instruction and were subsequently dismissed for abusing company time. At the CCMA, the Commissioner held that the dismissal was substantively and procedurally fair.

However, it is noteworthy that many employee groups and privacy advocates have disagreed with the contention that the monitoring of workers results in enhanced work quality. [183] Opponents advocate that employee monitoring and interception of employee communication is pervasive in nature and severely negatively impacts employees' privacy interests.[184] Moreover, studies have demonstrated a link between monitoring and psychological and physical health problems increased boredom, high tension, extreme anxiety and severe fatigue.[185] Consequently, it is submitted that the adversarial atmosphere created by monitoring undermines employee self-esteem and dignity, which decreases job commitment and results in lower productivity and competitiveness.[186] Employee monitoring can therefore create a hostile workplace environment, possibly eliminating the whole point of monitoring in the first place.[187]

3.2.5 PROTECTING COMPANY PROPERTY

Generally, the electronic communication tools are the property of the employer and have been distributed to employees in order to promote the employer's business interests and to enhance efficiency. The employer as the owner of these tools, has the inalienable right to decide the manner in which they are to be used as to well as regulate their use.[188] In line with this right, the employer may want to ensure that these tools are not abused by the excessive non-work related usage.

Instances of such abuse relate to excessive misuse of the employer's internet and email network which can result in clogging the network by taking up space on the bandwidth intended for

[182] *Bamford & Others/ Energiser SA Ltd* 2001 (12) BALR 1251 (P).
[183] Yerby op cit note 117 at 47.
[184] Conlon op cit note 174 at 293.
[185]Freeman and Martin op cit note 171 at 354.
[186] Conlon op cit note 174 at 293.
[187] Yerby op cit note 117 at 47.
[188] L Michalson 'The use of e-mail and the Internet in the workplace' (1999) available at http://www.comp.dit.ie/rfitzpatrick/The%20use%20of%20email%20and%20the%20Internet%20in%20the%20Workplace.pdf, accessed on 21 November 2014 at 196.

business. This was acknowledged in the decision of *Bamford & Others/ Energiser SA Ltd*[189], where the commissioner stated that objectively speaking the trafficking in chain mail and in pornography was damaging to the business of the employer and that the most obvious damage was in clogging up the system and running up costs. Furthermore, the Dancaster survey revealed that 64.71% of the companies reported problems with clogged bandwidth or degraded system performance through the abuse of the internet.[190]

Another significant reason why employers wish to enforce employee monitoring is security. With greater reliance on computer systems, information assets are seen as a vulnerable point of attack by would-be saboteurs.[191] In this context, it is evident that the simple opening of an unsolicited email at work could create a danger as attached files could contain a virus, wreaking havoc on a workstation hard drive and then spreading through a business' entire computer network.[192]One hacker or virus can therefore bring operations to a halt. This was evident, for instance, with 'the Melissa' virus or the 'iloveyou' virus which went around the world in a matter of hours and is estimated to have cost North American business millions.[193] Consequently, proponents argue that the monitoring of employees protects the safety and security of the company or organisation.[194]

Therefore from an employer's perspective, there are a number of counter-balancing arguments considerations which support the employer's argument of employee monitoring. Employees argue that employee monitoring should therefore not be seen as 'Big Brother' but rather as 'Wise Management'.[195]

The next part of this chapter is to explore to what extent the South African Law framework protects employees' right to privacy.

3.3 SOUTH AFRICAN CONTEXT

In a South African context, as stated in Chapter 1, section 14 of the Constitution guarantees the right to privacy as a fundamental human right. This section guarantees a general right to privacy with specific protection against search and seizures and infringement of communication.[196] Some commentators have therefore divided this constitutional right into 'substantive privacy' rights, which are the rights enabling persons to make decisions about personal interests, and

[189] *Bamford & Others / Energiser* supra note 182.
[190] Dancaster op cit note 180 at 865.
[191] Freeman and Martin op cit note 171 at 353.
[192] Yerby op cit note 117 at 48.
[193] McGregor op cit note 72 at 646; *Bernstein* supra note 6.
[194] Freeman and Martin op cit note 171 at 354.
[195] GFI White Paper op cit note 173.
[196] Modiba op cit note 115 at 365.

'informational privacy rights', which limit the ability of persons to gain, publish disclose or use information about others without their consent.[197] De Waal denotes that information privacy should be construed as safeguarding the interest of an individual to restrict the collection, storage and use of personal information concerning him or her.[198]

Moreover, the scope of the right to privacy has been defined as extending only to aspects of his or her life or conduct in regard to which a legitimate expectation of privacy can be harboured.[199] According to McGregor, a '*legitimate expectation'* connotes that one must have a subjective expectation of privacy. However, at the same time society must recognise this as objectively reasonable.[200] Further, in terms of the limitation clause of the Constitution, the infringement of the right to privacy can sometimes be justifiable, including in the context of the employment relationship.[201] To determine justifiability, it is necessary to balance the competing interest of the employer and the employee.

Consequently, this constitutional safeguard of privacy, in terms of section 14, protects a wide range of overlapping and inter-related right which is particularly relevant in the workplace where employees share offices and where computers, the internet and email are used as means of communication to perform activities of varying nature in the employer's interest, but often also in the employee's private interest.[202] Viewed from the employer's perspective, it may be argued that privacy is not an absolute right and an employee's right to privacy should be balanced with the employer's business necessities or operational requirements.[203] Proponents of this view, postulate that employer as the 'owner' of the computer facilities has a right to control the working life of the employee and has a right to protect his or her business interests and the integrity of his or her computer equipment.[204]

3.4 CASE LAW ON THE CONCEPT OF PRIVACY IN THE WORKPLACE

The Constitutional Court of South Africa has not yet been called upon to make a ruling regarding the application of section 14 in the workplace.[205] However, as discussed in the earlier Chapter, the Constitutional Court, in the Bernstein decision has laid down guiding parameters pertaining

[197] Roos op cit note 15 at 395.
[198] De Waal & Currie op cit note 70 at 323.
[199] McGregor op cit note 72 at 640.
[200] Ibid.
[201] A Dekker 'Vices or devices: employee monitoring in the workplace' (2004) 16 (4) *SA Merc LJ* 624 at 625.
[202] McGregor op cit note 72.
[203] Pistorius op cit note 2 at 3.
[204] Ibid.
[205] H Schoeman and M Jones 'Legality of monitoring E-Mail at the workplace: a legal update' available at http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/078.pdf, accessed on 16 August 2013.

to the scope of the right to privacy, i.e. while privacy is acknowledged in respect of a person's inner sanctum (such as family life, sexual preference and home environment), protection erodes as he or she moves into communal relations and activities such as business and social interaction.[206] Further to this principle, the lower Courts have also been called on to consider the parameters of the right to privacy in the workplace. A brief overview of these cases is set out below:

In one of the earlier decisions relating to telephone tapping, *Goosen v Caroline's Frozen Yogurt Parlour*[207], the Court discussed the need to engage in a balancing of interests in great detail. In this case, an employee recorded telephone conversations between the chairman of the disciplinary enquiry and the employer in order to prove bias on the part of the chairman. Startlingly, the employer argued that its right of privacy, in terms of the Interim Constitution, had been infringed by the recording of the conversation, without the employer's consent or knowledge. The Court concluded that the interception of the communication was indeed an infringement of the employers' right to privacy. However, in arriving at the aforesaid conclusion, the Court considered the limitation clause in terms of the Interim Constitution, which provided that 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.

To determine the meaning of 'reasonable' the Court looked at the Canadian Charter of Human Rights, which stated that it should firstly be determined whether there had been an infringement of a fundamental right and if so, whether the infringement was reasonable. According to the Canadian law, an infringement limitation must be of sufficient importance to outweigh the constitutionally protected right and the means must be proportional to the objective of the limitation'.[208]

A few years after this decision, two significant judgements were laid down pertaining to the tape recording of the employee's telephone conversations and which were decided in terms of the final Constitution. The first of these decisions was the case *Protea Technology Ltd & Another v Wainer & Others.*[209] In this case the Court had to consider whether the interception of a telephone conversation by an employer infringed the employee's right to privacy. The Court affirmed that in this case the scope of a person's privacy extends only to those aspects in regard to which a legitimate expectation of privacy can be harboured. The Court went further to state that whether there is a legitimate expectation of privacy depends on a 'subjective expectation of privacy which

[206] *Bernstein* supra note 6 at para [67].
[207] *Goosen v Caroline's Frozen Yogurt Parlour* 1995 (16) *ILJ* 396 (IC).
[208] Ibid at 404 D.
[209] *Protea Technology Ltd & Another v Wainer & Others* 1997 (9) BCLR 1225 (W).

society recognizes as objectively reasonable'.[210] The Court held that where an employee has conversations relating to the employer's affairs, the employer is entitled to demand and obtain a full account as the employee can furnish and these conversations did not enjoy constitutional protection. In arriving at this decision, the Court relied on the Bernstein judgement and stated that:

> 'Thus he may receive and make calls which have nothing to do with his employer's business. The employee in making such calls has a legitimate expectation of privacy. Although he must account to his employer if so required for the time so spent, the employer cannot compel him to disclose the substance of such calls. The content of the conversations involving his employer's affairs (whether indirectly or indirectly) is a different matter. The employer is entitled to demand and obtain from his employee as a full an account as the latter is capable of furnishing. In this sense also, the company can fairly be regarded as the owner of the knowledge in the employer's mind.'[211]

Following the *Protea* judgement, was the leading judgement of *Moonsamy v The Mailhouse*[212]*.* In this case an employee was dismissed as a result of the tape recording of his telephone conversations at work having been made by the employer without his consent. After his dismissal, the employee referred the matter to the CCMA, alleging that the tape recordings were obtained in contraventions of the Interception and Monitoring Prohibition Act (IMPA) 127 of 1992 and that his right to privacy, as guaranteed by the Constitution was breached through the actions of the employer.

In adjudicating this matter, the Commissioner referred to the earlier cases of *Goosen* and *Protea Technology* and thereafter reaffirmed that the question before the Court 'involves a balancing of competing interests, and in this respect the honourable Court identified these as the employer's right to economic activity versus the employee's right to privacy'. [213] Consequently, the Commissioner structured its reasoning on the five premises as set out in the limitation clause, section 36, of the Constitution:

1) <u>The nature of the right</u> – The Commissioner acknowledged that 'it is extremely difficult to clarify, at least with any degree of precision, the nature of the right to privacy of an employee on the premises of the employer during working hours.'[214] Upon relying on the

[210] Ibid at 1226 F.
[211] Ibid at 1240 D.
[212] *Moonsamy v The Mailhouse* 1999 (20) *ILJ* 464 (CCMA).
[213] Ibid at 470.
[214] Ibid.

American case of *Katz v US*[215], the Commissioner held that a person is entitled to a 'reasonable expectation' of privacy, which expectation only exist when (a) the individual has a subjective expectation of privacy and; (b) where society recognised the expectation as reasonable. The Commissioner held further that within the employment context, this expectation was largely determined by the operational requirements of the workplace and given the great variety of working environment that expectation must therefore be addressed on a case-by-case basis. In respect of the facts of *Moonsamy*, the Commissioner found that whilst one may argue that the telephone conversation took place on the employer's telephone on the employer's business premises and was related to the employer's business, telephone conversations by their nature demanded a higher degree of privacy than the employee's office or desk.[216] The Commissioner stated further that it could be argued that if a telephone call related to the employer's business, the employer was entitled to be privy to that conversation. But if the employer were allowed to make that initial decision regarding the nature of the call (personal v business), the right to privacy would be meaningless.[217] The right would then amount to a having a tribunal decide, after the interception of the call that did not relate to the business of the employer and so was confidential.

2) <u>The importance of the purpose of the limitation</u> - In a nutshell, the employee's right to privacy regarding work-related matters had to be qualified on the basis of fiduciary relationship between the employee and employer that entitled the employer to loyalty and honesty.[218] The employer argued that it considered its actions necessary for its financial self-preservation, as the employee conducted business that was damaging to the employer. However, the Commissioner held that a person's work or occupation was pivotal to his life, personal and professional. The rights to which a citizen was entitled in his personal life could not simply disappear in his professional life as a result of his employer's business necessity. At the same time, the employer's business necessity could legitimately impact on the employee's personal right in a manner not possible outside the workplace. Consequently, the Commissioner found that there had to be a clear balancing of rights. The Commissioner held that section 22 of the Constitution emphasized the employee's personal right and was to be preferred to the more 'amorphous (and consequently controversial) right to economic activity.[219]

[215] *Katz v US* 389 US (1967).
[216] Ibid.
[217] Op cit note 212 at 470 I.
[218] Op cit note 212 at 470 I.
[219] Op cit note 212 at 471 G-H.

3) The nature and extent of the limitation – The Commissioner stated that telephone calls were considered to be very private.[220] An employer might have the right to ask an employee to disclose the number of personal as opposed to business calls made during working hours. But the right to disclosure ended here, unless the employer could show, when it sought authorisation, that there were compelling reasons within the context of business necessity for the content of those conversations to be disclosed.[221]
4) The limitation and its purpose – The interception of telephone calls was intended to provide evidence against the employee. The commissioner stated that there must have been other methods to accumulate evidence of wrongdoing. If an employer could show that telephone interception was the only method of securing evidence, in circumstances where the employee was clearly causing harm to the employer, the telephone tapping might be justified. In this instance the employer still had to seek prior authorisation.[222]
5) That less restrictive means had to be used to achieve the purpose – If an employer actually could have used other more conventional methods of obtaining incriminating evidence against an employee, it should have done so. Put differently, other less restrictive means had to be considered. If there were none, the employer had to seek prior authorisation to tap the telephone. Prior consent could be obtained by way of employee consent as a condition of the employment contract, or by authorisation by the Labour Court.

Based on this reasoning the Commissioner found that the employer's actions in intercepting the employee's telephone calls, without prior authorisation or the consent of the employee, contravened section 14 (*d*) read with section 36 of the Constitution.

Subsequent to these decisions and as the use of the internet and email increased exponentially within the workplace, the Courts were called upon to effectively address the issue of employee privacy in relation to the employer's email and internet facilities. The following cases shed some light on the development of boundaries to the use of technology in the workplace.

In the case of *Bamford & Others/Energiser (SA) Limited*[223], the company Energiser summarily dismissed a group of employees for violating the company email policy. It was discovered that the employees had forwarded and received inappropriate emails during working hours. The issue before the Court related to the fairness of the dismissal. The company argued that the dismissal was justifiable based on the following charges: a) the repeated violation of company policies and procedure regarding the use of the company email; b) the repeated receipt and forwarding to

[220] Op cit note 212 at 471 I.
[221] Op cit note 212 at 272 A.
[222] Op cit note 212 at 472 D.
[223] *Bamford & Others / Energiser* supra note 182.

colleagues of obscene pornographic; racist and sexist material and jokes; c) the violation of the company procedures regarding the work environment. In response to the charges, the employees did not deny receiving or forwarding the material. However, they claimed that there was no clear rule against the receipt or transmission of such material and that their right to privacy had been infringed. They argued further that the company had acted inconsistently and discriminately in perusing disciplinary action against them.

In considering these arguments, the Arbitrator found that although the company's standard policy did not explicitly provide for the prohibition about email use in the workplace; there was enough contained in the policy to suggest such prohibition. The Arbitrator stated that the company's directives left no room for doubt that the circulation of such material was forbidden. Employees had also been warned against the downloading of foreign material into the company system, and had been told that office computers were for business use only.[224]

The arbitrator held further that the background of the employees left him convinced that the employees should have known that the circulating of such material was socially unacceptable. The arbitrator went on to conclude that apart from the fact that material was 'contrary to what would circulate amongst self-respecting people', such material also damaged the business of the company by clogging the computer system and carried the risk of the company domain name becoming associated with messages in its system. The abuse of trade names constituted a trademark violation, and demonstrated how frivolous use of office computers by untrustworthy employees exposed businesses to risk. Furthermore, there was a distinct likelihood that the material might have offended other employees if they had chanced upon it.[225]

With regard to the employees' argument that their privacy had been infringed, the Arbitrator rejected their claim. The Arbitrator found that the material concerned could not be described as personal in nature, the personal dignity or personal affairs of the employees had not been affected in any way, and the material concerned were stored in the employees' computers and could not be considered personal information.[226] Consequently, *Bamford's* case is precedent of the fact that even where there is no explicit policy regulating employee use of email in the workplace, employees cannot argue that they had a reasonable expectation of privacy in respect of all received and forwarded communications in that workplace.[227]

[224] Ibid at 1268 B-H.
[225] Ibid at 1268.
[226] Ibid at 1271 A.
[227] Gondwe op cit note 36 at 276.

The reasoning of the *Bamford* case was adopted in the case of *Toker Bros (Pty) Ltd & Keyser*[228]. In this case the employee was charged with dishonesty in that she excessively misused the company computer for personal use during working hours and without the consent of the employer. She was further charged with making defamatory remarks about the employer in a personal email to a friend, which was sent from the company computer. The employee argued that the manner in which her email was accessed contravened her right to privacy in terms of the Constitution. The Commissioner held that the right to privacy, in terms of section 14 (d) can be limited where consent has been given or a clear policy on monitoring and intercepting of communication in the workplace is implemented.

Another case which involved the misuse of the internet by employees at the workplace, is the case of *Smuts/Backup Storage Facilities & Others*[229]. In this case a managerial employee was dismissed for viewing pornographic material on the company computer while at work. The employee was ultimately dismissed on the grounds of the use of company time and resources and excessive use of the Internet. The arbitrator found that the manager was guilty of viewing pornography during working hours on the company computer and for using the Internet for purposes other than company business. The arbitrator concluded further that whilst there was no rule in place prohibiting such conduct, the employee (at a managerial level) should have known better and should not have engaged in this type of activity at the workplace.[230] The arbitrator therefore ruled that the employee abused the employer's facility and had failed to act in the best interest of the employer.

Subsequent to these decisions is the case of *Cronje v Toyota Manufacturing*[231] which dealt with the dismissal of a managerial employee of the company for, inter alia, distributing racist or inflammatory material via the company email. The email in question pertained to a cartoon depicted a picture of a gorilla with the head of President of Zimbabwe, Robert Mugabe. This carton version of Mugabe was holding another small gorilla and was captioned 'Mugabe and his right hand man. We want the farms to grow more bananas.' The employer argued that it was necessary to dismiss the employee as the company had to take strict action against racism and email abuse at the workplace. The employee, on the other hand, argued that he did not consider himself or the cartoon as racist, which is why he distributed the cartoon to others. He submitted further that he was unaware of the cartoon fell within the prohibitions contained in the company's email policy.

[228] *Toker Bros (Pty) Ltd & Keyser* (2005) 26 *ILJ* 1366 (CCMA).
[229] *Smuts/Backup Storage Facilities & Others* [2003] 2 BALR 219 (CCMA).
[230] Ibid at 224 A-G.
[231] *Cronje v Toyota Manufacturing* 2001 (3) BALR 213 (CCMA).

The Commissioner rejected the employee's claim and after analysing the evidence, the Commissioner found the cartoon to be racist and inflammatory:

> '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.'[232].

The Commissioner submitted further that the cartoon had to be evaluated in the context in which it was published, that is a factory that employs 3500 black workers in a new independent South Africa, in the year 2000. The fact that sterotyping is a matter of deep moral, cultural and social sensitivity to blacks. Stereotyping cartoons offend people's cultural and racial self-image. The Commissioner also considered the existence of the company's rule, the contravention thereof, the employee's awareness of the rule and the consistent application of the rule. The substantive fairness of the dismissal was accordingly confirmed.

Similarly, in the case of *Dauth & Brown & Weirs Cash & Carry*[233], an employee was dismissed for sending racist email to a large number of employees via the company's email facility. In this email the employee made a number of inflammatory and derogatory anti-Semitic comments with reference to certain Jewish shareholders and directors of the company. The employee argued that he could not be held responsible for the contents of the email as he was in a state of diminished responsibility because of a drug prescription intake for depression and related illnesses. However, the Commissioner found that the employee was not influenced by his medication intake when he sent the email.[234] The Commissioner found further that the email remarks relating to Jews was 'a gross and sickening example of racism'.[235] The Commissioner ruled that the dismissal of the employee was justifiable.

In the case of *Philander/CSC Computer Sciences*[236], an employee was dismissed after he had contravened the employer's electronic communication policy by accessing and forwarding pornographic material via the employer's electronic communication system. In this case the employer had a policy in place that clearly stated that the company was serious in combating the

---

[232] Ibid at 222.
[233] *Dauth & Brown & Weirs Cash & Carry* 2002 (8) BALR 837 (CCMA).
[234] Ibid at 842 G-J.
[235] Ibid.
[236] *Philander/CSC Computer Sciences* 2002 (3) BALR 304 (CCMA); See also *Singh and Island View Storage Ltd* (2004) 13 CCMA 8.32.1. In this case the employee was dismissed for forwarding sexually explicit emails to 3 colleagues. The employee argued that he was not aware that the email was inappropriate and in contravention of the employer's electronic communication policy. However, the Commissioner found that the employee's motive was to offend and insult his colleagues and that he was well aware of the consequences of his action.

inappropriate use of the electronic system. In arriving at his decision, the Commissioner considered the attitude of the employee towards the employer. The Commissioner noted that the employee showed no appreciation of the potential harm of his conduct, nor did he repent for what he had done:

> 'I have great difficulty in finding a reason why an employer should tolerate such an attitude from an employee and how an employee can expect the employer to tolerate a continuation of the relationship in such circumstances'. [237]

Consequently, the Commissioner found the dismissal to be fair as the appropriate sanction.

Furthermore, the increased usage of electronic communication in the workplace has also impacted the prevalence of corruption in the workplace[238]. This was illustrative in the case of *Sugreen v Standard Bank of SA*[239]. In this case the employee, Mr Sugreen was dismissed for alleged corruption. The primary piece of evidence against her was a tape recording of a telephone conversation with one of the respondent's service providers. The recording was made by the service provider who had allegedly offered a bribe to Mr Sugreen in order to keep his company on the panel of service providers. The employee denied receiving a bribe and claimed that the tape was a compilation of a series of actual telephone conversations. In addition, the employee claimed that the tapes were inadmissible because the recording of her conversation had breached her right to privacy. [240] The Commissioner submitted that the use by employees of their employer's telephone and email facilities are of legitimate interest to the employer if there is reason to suspect that the employee is guilty of misconduct. The Commissioner concluded that there was no constitutionally cognisable breach of privacy.[241]

Finally, more recently Commissioners have been called upon to consider employee privacy rights in terms of communication posted on social media forums. Although, not directly relevant to this dissertation and the issue of employee privacy in respect of electronic communication, it is still interesting to note the Court's approach:

In the cases *of Sedick & Another v Krisray (Pty) Ltd[242] and Fredericks v Jo Barkett Fashions[243],* in both matters the employees were dismissed as a result of derogatory comments posted on 'Facebook'. The employees challenged the fairness of the dismissals. In both cases the

[237] Ibid at 316 D.
[238] R Le Roux 'Aspects of South African law as it applies to corruption in the workplace' (2004) 17 *SACJ* 158.
[239] *Sugreen v Standard Bank of SA* 2002 (7) BALR 769 (CCMA).
[240] Ibid at 772 A-B.
[241] Ibid.
[242] *Sedick & Another v Krisray (Pty) Ltd* 2011 (8) BALR 879 (CCMA).
[243] *Fredericks v Jo Barkett Fashions* 2011 JOL 27923 (CCMA).

Commissioners found that the employees were fairly dismissed as their privacy had not been infringed when their employers accessed their Facebook posts. The Commissioners reasoning was based on the fact that the employees had not restricted their Facebook privacy settings and the updates could be viewed by anyone, even those with whom they were not 'friends' on the website. The Commissioners took the view that the employers were entitled to intercept the posts in terms of the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 (RICA). The Commission decided that the employer was entitled to access the wall posts as the employees had 'open' Facebook profiles.

3.4.1 ANALYSIS OF CASE LAW PRINCIPLES

Based on the preceding discussion of the case law, it is evident that the following principles have emanated from the judgements:

a) The employer, as the owner of the electronic communication systems in the workplace, is justified in regulating employee communication in order to protect its business interests.
b) The employee has a legitimate expectation of privacy, however this expectation is determined and dependant on the operational requirements of the workplace.
c) The employer should respect the rights of the employers and exercise care and discretion when intercepting the contents of employee email communication.
d) In certain circumstances, an employee maybe justified in intercepting or monitoring the employee's electronic communication without his or her knowledge or consent.
e) The employee's right to privacy regarding work related matters has to be qualified on the basis of the fiduciary relationship between the employee and employer that entitled the employer to loyalty and honesty.
f) In balancing the interests of the employer and employee, the Courts will consider:
    - the manner in which the communication is intercepted
    - the intention or motive of the employee
    - the consequences of the employee's action i.e. Could the employees action result in the employer being vicarious liable
    - whether the employer could employ other methods of obtaining the information or evidence required, which were less restrictive.
g) Even in cases where there is no explicit policy regulating employee use of email in the workplace, employees cannot argue that they had a reasonable expectation of privacy in respect of all received and forwarded communication in the workplace.

Notwithstanding these principles, however, it is evident that the question of balancing the employee's right to privacy with the employer's right to economic activity has only been primarily

considered in a minority of the cases thus far. Furthermore, these cases involved the elementary electronic communication platforms such as telephone networks, email facilities and internet networks. Our Courts still have some way to go in developing the law in light of the recent technological advancements.

3.5 CONCLUSION

It is trite that the right to privacy enjoys constitutional protection. However, this constitutional safeguard protects a wide range of overlapping and interrelated rights, which is particularly pertinent in the workplace where the advancement of technology has made it difficult to draw a distinct line between the employee's right to privacy and the employer's right to economic activity. It is therefore a right, in the context of the employment relationship, which is extremely difficult to clarify.[244] It must therefore be balanced, in terms of section 36, with the employer's business necessity and operational requirements.

Nevertheless, it has been argued whilst employers may have a legitimate business interest, employees should be afforded with an 'inviolable zone of privacy' upon which employers should not intrude.[245] Proponents of this argument contend that the protection of the right to privacy in the workplace preserves employee's autonomy and fosters respect and trust in the employment relationship. It also argued that employee privacy enhances productivity and improves employee morale and loyalty.

Conversely, employers argue that the employees do not have an absolute right to privacy and this should be balanced with the employer's business necessity. This argument is premised on the view that the employer is the owner of the property and has a right to 'control' the working life of the employee. Moreover, there are important reasons why employers favour employee monitoring with the most significant being employer liability, protecting company property and employee productivity. Employers are therefore more at risk than ever before and are forced to take effective steps to deal with these risks.

Consequently, a balancing of interests is ultimately required, which sentiment was succinctly expressed in the *Moonsamy* case:

> '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

[244] *Moonsamy* supra note 212 at 469.
[245] McGregor op cit note 72 at 639.

personal rights in a manner not possible outside the workplace. Therefore there is a clear balancing of interest.'[246]

In South Africa the Constitutional Court has yet to consider the application of section 14 in the workplace. Nevertheless, although the decisions of the lower Courts have not left clear guidelines indicating where the right to workplace privacy ends and the right to monitor begins[247], they have provided a basis of principles relating the employer's right to intercept and monitor employee's electronic communication in the workplace. This position will be expanded on in the upcoming chapter, which will explore the legislative framework promulgated in South Africa pertaining to electronic communication in the workplace.

[246] Moonsamy supra note 212 at 471G.
[247] Collier op cit note 1 at 1759.

CHAPTER FOUR - SOUTH AFRICAN LEGISLATION REVIEW

4.1 INTRODUCTION

The preceding chapters have dealt with the nature and scope of the right to privacy in South Africa, as well as the extent of the right to privacy in the employment context. This chapter will now focus on the extent to which an employer may monitor or intercept employee electronic communication as regulated by the legislative framework in South Africa.

4.2 INTERCEPTION AND MONITORING PROHIBITION ACT 127 OF 1992

The Interception and Monitoring Prohibition Act[248] (IMPA) came into effect in February 1993, prior to the enactment of the Interim Constitution and was arguable one of the most important statutory provisions relating to monitoring and interception of communication.[249]The primary focus of the Act is to deal with issues of monitoring and intercepting relating to telephonic communications and postal communications. It is said, therefore, that the Act aims to protect confidential information from illicit eavesdropping.[250]

The objective and purpose of the IMPA is:

> 'To prohibit the interception of certain communications and the monitoring of certain conversations; to provide for the interception of postal articles and communications and for the monitoring of conversations in the case of a serious offence or if the security of the Republic is threatened; and to provide for matters connected therewith.'

In terms of the IMPA, the following definitions are noted:

> 'monitor' includes the recording of conversations by means of a monitoring device;
>
> 'monitoring device' means any instrument, device or equipment which is used or can be used, whether by itself or in combination with any other instrument
>
> 'telecommunications line' includes any apparatus, instrument, pole, mast, wire, pipe pneumatic or the receiving of signs, signals, sounds, communications or other information.

[248] Act 127 of 1992.
[249] Pistorius op cit note 2.
[250] N Bawa 'The Regulation of the Interception of Communications and Provision of Related Information Act': telecommunications law in South (2006) 296 available at http://thornton.co.za/resources/telelaw13.pdf, accessed on 21 November 2014.

It is noteworthy that the term 'intercept' is not defined in the Act. Beech contends that it should bear its ordinary meaning of 'seize, catch or stop' (a person, message, vehicle etc.) from one place to another.[251] Furthermore, it is generally accepted that a monitoring device would include a computer and computer related equipment which records communications.[252]

Section 2 (1) provides that no person shall a) intentionally and without the knowledge or permission of the dispatcher intercept communication transmitted by telephone or in other manner b) intentionally monitor a conversation by means of a monitoring device in order to gather confidential information of a person/organisation.

Section 2 (2) goes on to provide that notwithstanding subsection (1), a judge may direct that a) a particular postal article or communication which has been transmitted by telephone or over a telecommunications line may be intercepted b) all postal articles or communications to or from a person transmitted by telephone or over a telecommunications line may be intercepted; c) conversations by or with a person may be monitored by means of a monitoring device.

In summary, the IMPA is aimed at the prohibition of the interception and monitoring of telephonic conversations or the interception of postal articles and communication. However, it does provide for a designated judge [253] to consider applications for interception and monitoring of 'a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line'. Bawa explains that this Act therefore deals with concepts of interception and monitoring separately.[254] With regard to interception, it does not prohibit interception of a communication:

- If the interception is not intentional;
- If the dispatcher knows that his or her communication is being intercepted or gives proper permission for such interception;
- If the communication is not electronic (i.e. 'transmitted by telephone or in any other manner over a telecommunication line').[255]

On the other hand, the prohibition regarding monitoring goes beyond electronic communication and includes 'direct conversations'. The prohibition on monitoring however, does not apply:

- If the monitoring is not intentional; and

[251] W Beech 'The right of an employer to monitor employees electronic mail, telephone calls, Internet usage, and other recordings' (2005) 26 *ILJ* 650.
[252] Ibid.
[253] The Act provides that it is a Judge in a Local or Provincial Division of the High Court.
[254] Bawa op cit note 250.
[255] Ibid at 308.

- If the monitoring is for any reason other than to 'gather 'confidential information'.[256]

Furthermore, section 2 (1) places emphasis on confidential information concerning any person, body or organisation. It also allows the state to intercept and monitor conversations and communications under certain conditions and in accordance with the directives of issued in terms of the Act.

Section 8 of the IMPA provides for offences and penalties to those who contravened the provisions of section 2 (1) and these provisions have been considered by our Courts in a number of judgements:

In *Tape Wine Trading CC v Cape Classic Wines (Western Cape)*[257], the Court dealt with the admissibility of telephone recordings which had been obtained at the instance of one of the parties. It was alleged that the recorded conversation had breached the provisions of the IMPA and the right to the privacy. The Court drew the distinction between participant surveillance and third party surveillance. According to the Court, participate surveillance was surveillance by one of the parties to the communication without the knowledge of the other. In this instance, the Court concluded that the recorded conversation fell within the ambit of participant surveillance and was therefore not in contravention of the IMPA and did not breach the constitutional right to privacy.

Similarly in *S v Kidson*[258] and *S v Dube*[259], the Court concluded that the intention of the legislation was for section 2(1) (b) of the IMPA to apply to third party surveillance and not participant surveillance. In both cases, one party to the conversation recorded the conversation without the knowledge or consent of the other party. The Court concluded in both instances, that the party's conduct in recording the conversations were not prohibited by the IMPA as it amounted to participant surveillance. In this regard, Cameron J, in his judgement in the case of Kidson, stated that the legislature's primary purpose was to 'protect' confidential information from 'illicit eaves-dropping'[260]. Cameron J stated further that the IMPA prohibited the conduct of third persons acting in relation to a conversation between others and not in respect of a person monitoring a conversation in which he or she participates in.[261] The Court concluded therefore that it is not

[256] See *Protea Technology* supra note at 209 at 603, the Court remarked that 'that expression must surely means such information as the communicator does not intend to disclose to any person other than the person to whom he is speaking and any other person to whom the disclosure of such information is necessary or implied to be restricted. I think that there is a distinction between 'confidential' information and 'private' information.
[257] *Tape Wine Trading CC v Cape Classic Wines (Western Cape)* 1999 (4) SA 194 (CC).
[258] *S v Kidson* 1999 (1) SACR 338 (W) at 348.
[259] *S v Dube* 2002 (2) SA 583 (NPD).
[260] *Kidson* supra note 258 at 344 F.
[261] Ibid at 344 H-I.

necessary for a person, who is a participant to the conversation, to apply for authority to conduct the recording 'because the monitoring they are most likely to engage in, namely participate monitoring, is not prohibited at all'.[262]

In *Protea Technology Ltd & Another v Wainer*[263], one of the issues before the Court was whether telephone recordings which was made by the employer of the employee's conversations, amounted to a contravention of the IMPA. In reaching its decision the Court considered the interpretation of various definitions contained in the IMPA in great depth. Following this consideration, the Court held that 'In any case where section 2 (1) (b) is invoked, it will be necessary to consider why the conversation was monitored in order to ascertain whether the purpose was to gather confidential information, and it may be necessary to examine the contents of the conversation in order to establish that purpose.'[264] The Court held further that, although the IMPA does not define 'confidential information', that 'expression must surely mean such information as the communicator does not intend to disclose to any person other than the person to whom he is to speak and any other person to whom the disclosure of such information is necessarily or impliedly intended to be restricted.' [265] The Court ultimately concluded that recordings obtained in this case, fell within the ambit of 'confidential information' and was therefore in contravention of the IMPA. However, this did not render the production of recordings inadmissible before the Court in a civil matter.[266]

Based on the case law, it is evident that the Courts have determined that the IMPA, and therefore the prohibitions on interception and monitoring, does not apply to the interception and monitoring of a party to the communication or conversation (i.e. participant participation).[267] In this regard, Beech contends that in employer-employee related cases, this aspect is particularly important where the interception and monitoring forms part of an investigation being conducted by an employee. In addition, where the investigation has been conducted, the information may not be 'confidential information' on the basis that it was information intentionally disclosed during the investigation.[268]

Consequently, although the IMPA was the most statutory provision with regard to monitoring, in that it prohibited the interception of confidential information, it contained potential difficulties. Firstly, it is apparent that the IMPA was not applicable to the private sphere such as the

[262] Ibid at 346 F-G.
[263] *Protea Technology* supra note 209.
[264] Ibid at 603.
[265] Ibid.
[266] Ibid at 606.
[267] Bawa op cit note 250.
[268] Beech op cit note 251 at 654.

workplace; and secondly, the IMPA does not take into account the vast array of communications which have been possible in recent times.[269]

As a result of these difficulties during October 1999, after extensive public consultation the South African Law Commission (SALC) submitted a report to the Minister of Justice and Constitutional Development. This report included an extensive review of the IMPA. The SALC expressed the view that even though the IMPA compared favourably with its international counterparts, such as France, Netherlands, Belgium, Germany, and many other countries, it did not deal adequately with new technology. Particularly, relating the monitoring of employees' email by employers[270]. To this end, the SALC recommended a new draft bill, which culminated in the promulgation of the Regulation of the Interception of Communications and Provisions of Communication-Related Information Act, 70 of 2002 (RICA).

4.3 REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION RELATED INFORMATION ACT 70 OF 2002

The President assented to RICA on 30 December 2002.[271] The Act was primarily 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.[272] As a result, the primary purpose of this Act is to prohibit the interception of communication, direct or indirect, unless it is intercepted by a party to the communication, or if an author of the communication has consented thereto. Law enforcement officers may intercept under certain conditions.[273] RICA therefore regulates virtually every aspect pertaining to the interception and monitoring of telecommunications both in the workplace and private sector.[274] Importantly and of relevance to this paper, this includes monitoring and interception of employee electronic communication by employers.[275] Accordingly, this discussion will consider the workplace environment and the regulation of employee communications by an employer as regulated by RICA.

RICA defines the following pertinent terms as follows:

'Business' as any business activity conducted by a person or private or public body.

[269] Ibid at 651.
[270] Bawa op cit note 250 at 298.
[271] GG 24286, 22 January 2003.
[272] Bawa op cit note 250 at 298.
[273] Schoeman and Jones op cit note 205 at 2.
[274] Bawa op cit note 250 at 298.
[275] Ibid.

'Intercept' as being the acquisition of any communication through the use of any means, including an interception device in order to make the contents of the communication available to a person other than the sender or recipient or intended recipient of that communication. This includes the monitoring of the communication by a monitoring device; viewing, examination or inspection of the contents of any indirect communication; diversion of any indirection communication from its intended destination.

An 'Interception Device' as any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to intercept any communication.

'Direct Communication' as oral communication between two or more persons which occurs in the immediate presence or all the persons participating in that communication; or the utterance by a participant in indirect communication if the utterance is audible to another person who is in the immediate presence of the participating persons in the direct communication.

'Indirect Communication' as the transfer of information, including a message or any part of a message, whether in the form of speech, music or other sounds; data; text; visual images, whether animated or not; signals; or radio frequency spectrum; or in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication systems.

'Monitor' includes to listen to or record communications by means of a monitoring device, and 'monitoring has a corresponding meaning.

'Monitoring Device' as any electronic, mechanical or other instrument, device, equipment or apparatus which is used or can be used, whether by itself or in combination with any other instrument, device, equipment or apparatus, to listen to or record any communication.

Based on these definitions, it is apparent that RICA permits greater latitude for the interception and monitoring of communication than was permitted by the IMPA.[276] For instance:

- Unlike the IMPA, RICA defines 'communication' as including both direct and indirect communication. For purposes of this paper, the definition relating to indirect communication is of greater relevance and is broadly defined to include a number of communications that occur through the media, telephone calls, music, visual images and data or text.[277] This means then that the content of email communication would constitute a form of indirect

[276] Bawa op cit note 250.
[277] Mischke op cit note 122 at 77.

communication as envisaged in the Act. Further, telephone conversations, SMS, postal communication and the downloading of information from the Internet are also within the ambit of indirect communication.

- The IMPA does not define intercept or interception, which is explicitly defined in RICA, to include monitoring communication by a monitoring device (as defined). The effect of such a definition of 'intercept' is, in essence, a wide definition – it refers to the acquisition of the contents of any communication by any means: it is not only limited to the use of interception or monitoring devices.[278]
- RICA defines 'monitoring' to include the listening to, or recording of, communications by means of a monitoring device – which is an extension to the meaning provided in IMPA – which defines 'monitor' to include the recording of conversations or communications by means of a monitoring device. It further defines 'monitoring device' more precisely, to include electronic, mechanical or other instrument, device equipment or apparatus, to listen or record any communication. In terms of this definition, a computer would constitute a monitoring device.

4.3.1 PROHIBITION ON INTERCEPTION AND MONITORING

Section 2 of RICA contains the general prohibition. In terms of this section:

> '..no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept at any place in the Republic, any communication in the course of its occurrence or transmission.'

Any interception in contravention of this section may constitute a criminal offence, which carries a maximum fine of R2 million or a maximum term of imprisonment of 10 years.[279]

In terms of this section then, it is evident that no person may intentionally acquire the contents that is, intercept any email communication in the course of that email message's occurrence or transmission by using an interception or monitoring device.[280] However, it is noted that RICA does not define 'transmission' for the purposes of section 2. In this regard, Mischke contends that it is safe to assume that the entire transmission process, from the point where a computer user clicks the send button in respect of a single email message to the point where the email message appears on the computer screen of the recipient is intended.[281]

[278] Ibid.
[279] Section 49(1) of RICA.
[280] Mischke op cit note 122 at 78.
[281] Ibid at 77.

Similarly, the term 'occurrence' is also not defined in the Act. The use of this word raises the question of whether the email message 'occurs' on the employee's computer or on the employer's network server? According to Mischke, in many instances an email message is not transmitted to an employee's computer or stored on the hard drive of the computer; the message is stored (and often remains) on the central mail server of the employer, where that email message may be accessed by any users with access privileges to the server.[282]

Essentially, it is contended that the scope and purport of section 2 is wide and seeks to protect communications from interception regardless of how, when and where they are transmitted, and irrespective of where, the email message is stored on the computer network.[283] Mischke contends that it would be safer to assume that section 2's prohibition encompasses the entire transmission process and protects the contents of the email message no matter where it is situated.[284]

Nevertheless, it is important to note that RICA does provide for the interception of communication in certain instances. These exemptions are discussed below, with specific reference to the employee – employer relationship.[285]

4.3.2 INTERCEPTION OF COMMUNICATION BY A PARTY TO THE COMMUNICATION

Section 4 (1) of the RICA provides that

> 'any person, other than a law enforcement officer, may intercept any communication if he or she is a party to the communication, unless such communication is intercepted by such person for purposes of committing an offence.'

This means therefore that any person who is a party to the communication may intercept such communication, unless it is being done for purposes of committing an offence. [286] In this regard, Beech contends that as the term 'party' is not defined, it bears its ordinary meaning and therefore includes the sender, recipient and any other person to whom the communication is copied.[287] There is also potential argument that the employer, by providing the relevant systems, is a party to any communication which is sent or received on the system.[288]

[282] Ibid.
[283] Ibid.
[284] Ibid.
[285] It is noted that outside of the employer-employee relationship, Section 3 of RICA provides that an authorized person may execute an interception. An authorized person as defined in the Act is a law enforcement officer from the South African Police Services, the Defense Force, the Independent Authority of South Africa, the National Prosecuting Authority or the National Intelligence Agency (NIA), or other persons in terms of section 26.
[286] Section 4(1) of the RICA.
[287] Beech op cit note 251 at 656.
[288] Ibid.

4.3.3 INTERCEPTION OF COMMUNICATION WITH CONSENT OF PARTY TO COMMUNICATION

Section 5 (1) of the IMPA provides that:

> 'Any person, other than a law enforcement officer, may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception, unless such communication is intercepted by such person for purposes of committing an offence.'

This provision is undoubtedly the most important provision in respect of the issue of workplace privacy and the interception of communication by employers. It is noteworthy that this provision is similar to that contained in the IMPA. However, unlike the IMPA, RICA provides that this consent must be given prior to the interception occurring and that the consent must be in writing. Furthermore, the consent maybe given by either one of the parties to the communication. It follows then, that a general consent obtained by employers as part of the terms and conditions of employment to intercept personal employee communication may be construed as prior consent, as contemplated in section 5 (1).[289]

Having said that, however, an argument maybe raised that the wording of the provision 'consent in writing to such interception' implies that the consent must be obtained each time an interception is sought.[290] It is for this reason that employers are advised to ensure that the scope of the 'general consent for interception' contained in the employment contract or policy, is drafted in a manner which ensures that at the time the employee agreed to the interception, the employee understand the ambit of what he or she agrees to.[291]

4.3.4 INTERCEPTION OF INDIRECT COMMUNICATION PERTAINING TO CARRYING ON OF A BUSINESS

Section 6 provides that:

> '(1) Any person may, in the course of the carrying on of any business, intercept any indirect communication –
>
> (a) by means of which a transaction is entered into in the course of that business;
> (b) which otherwise relates to that business; or
> (c) which otherwise takes place in the course of the carrying on of that business,
>
> in the course of its transmission over a telecommunication system.
>
> (2) A person may only intercept an indirect communication in terms of subsection (1) –
> (a) if such interception is effected by, or with the express or implied consent of, the system controller;
> (b) for purposes of-

[289]Bawa op cit note 250.
[290]Ibid; Beech op cit note 251.
[291]Bawa op cit note 250 at 296.

(i) Monitoring or keeping a record of indirect communications-

(aa) in order to establish the existence of facts;

(bb) for purposes of investigating or detected the unauthorised use of that telecommunication system; or

(cc) where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system; or

(ii) 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 of they so choose

(c) If the telecommunication system concerned is provided for use wholly or partly in connection with that business; and

(d) If the system controller has made all reasonable efforts to inform in advance a person, who intends to sue the telecommunication system concerned, that indirect communications transmitted by means thereof may be intercepted or if such indirect communication is intercepted with the express or implied consent of the person who uses that telecommunication system'.

This section has particular relevance to the employer-employer relationship in respect of the monitoring and/or accessing of employee's emails, monitoring of internet usage and recordings of telephone calls.[292] The purpose of this section is to permit employers to intercept indirect communication; provided that such communication relates to a transaction entered into in the course of business.[293] However, the section goes further, in terms of section 6(2), and sets certain requirements that must be met before the interception of indirect communication will be permitted:

Firstly, the interception must be with the expressed or implied consent of the 'system controller'.[294] Secondly, the system controller must either have made all reasonable efforts to inform in advance all persons who intend to use the telecommunication system concerned of the fact that interceptions may take place, or the interception must take place with the express or implied consent of the person who uses the telecommunications system. [295] Thirdly, the telecommunications system must be provided for the use 'wholly or partly in connection with that business'. Finally, such interception must be carried for defined purposes, namely:

[292] Ibid at 313.
[293] Schoeman and Jones op cit note 205 at 9.
[294] System Controller is defined in section 1 to mean the chief executive officer or equivalent officer of the juristic person, or any person duly authorized by such person.
[295] Pistorius op cit note 2 at 9.

- to establish the existence of facts. Beech notes that includes the traditional recording of the terms and conditions of a transaction.[296]
- to investigate or detect the unauthorised use of the telecommunication system. This would include monitoring or intercepting for the purpose of detecting unauthorised use of the internet system or email system.[297]
- to secure or to ensure the effective operations of the system. This could include spamming, unusable email traffic to and from persons.[298]

Essentially, section 6 means that an employer may, on prior notice to the employee and with the employee's consent, monitor email communication sent and/or received on its network in order to keep records of email transactions[299]. It is also of relevance that this section includes the interception to determine whether pornography, defamatory and/or sexually offensive emails are being sent and received. This is premised on the fact that the section refers to the 'detection of unauthorised use'.[300] Bawa supports this contention and submits that the legitimate purpose provisions of RICA are aimed at balancing employees' rights to privacy with the need for employers to prevent the misuse and abuse of telephones, email and the internet. As well as to protect their communication systems from viruses, spam, hackers, and other threats. It follows then, that the interception of communication for purposes of detecting hardware and software problems or errors, viruses and hacking would qualify as measure taken 'to secure… the effective operations of the system' and would be regarded as a legitimate basis for intercepting and monitoring indirect communication in the course of transmission.[301]

The requirement of prior written consent has been a discussion point for many academic scholars. It has been argued that it is absolutely crucial that an employer obtain the prior written consent of its employee before such employer may intercept the electronic communication of the employee.[302] This argument is primarily based on the literal interpretation of section 5 (1) which provides for 'consent in writing to such interception', which may apply on a case-by-case basis.[303] Conversely, it is argued that a general consent contained in the conditions of employment of the employee is suffice and falls within the ambit of the consent envisaged in Section 5.[304]

---

[296] Beech op cit note 251 at 658.
[297] Ibid.
[298] Ibid.
[299] Schoeman and Jones op cit note 205 at 9.
[300] Beech op cit note 251 at 656. Beech submits that the reference to detection of unauthorised in this section makes its application extremely wide.
[301] Bawa op cit note 250.
[302] VA Lawack-Davids & A van der Walt 'Interception of Electronic Communication in the Workplace' (2005) 26 (1) *Obiter* 133 at 139.
[303] Pistorius op cit note 2 at 8.
[304] Ibid.

Moreover, it is argued that the only time that such prior written consent is required is in terms of section 5 where the employee, as a party to the communication, has to give such consent.[305] As a result, many scholars have read the need for written consent into section 6.[306] However, it is evident that section 6 postulates that employer must obtain *the express or implied consent of the person* who uses the telecommunication system in order to monitor or intercept email communication sent on its network. Therefore, unlike section 5 which provides for prior written consent to be obtained, section 6 does not explicitly set out the same requirement. Consequently, the academic scholars have supported the view that if the employee has consented in advance, it can be taken that the system controller has made all reasonable efforts to inform in advance that indirect communication transmitted by means of a telecommunication system may be intercepted (in terms of section 6 (2) (c)). Similarly, if written consent has been obtained, it will be viewed as interception with the express consent of the employee who uses the system (section 6 (2) (d)).

Due to the controversy and uncertainty surrounding the requirement of consent in section 5 and 6 it has been submitted that it is advisable for employers to obtain the prior written consent of all its employees who use the telecommunication system in accordance with an electronic communications policy. This consent may be also be obtained through employment contracts and policies.[307] Alternatively, employers may also make use of electronic agreements, referred to as 'click-wrap agreements' in terms of which they ensure that they have made all reasonable efforts to inform the employee in advance that indirect communications may be intercepted . In terms of such agreements, an employee is deemed to have consented to the interception and monitoring of his or her electronic communication and internet access when he or she clicks on the acceptances button when logging onto the computer network of the business.[308] This aspect will be elaborated on later in this Chapter, in terms of the enactment of the Electronic Communication and Transactions Act 25 of 2002.

Despite the above points of raised by the provisions of RICA, as discussed above – the case law decided after the enactment of RICA have not directly addressed the application of RICA. Nonetheless, it is central to this discussion, to consider the consequences of such interception and monitoring by the employer on the individual employment relationship as governed by the Labour Relations Act.[309]

[305] Beech op cit note 251.
[306] Lawack-Davids & van der Walt op cit note 302 at 135.
[307] Bawa op cit note 250 at 316.
[308] Ibid at 316; Lawack-Davids & van der Walt op cit note 302 at 135.
[309] Act 66 of 1995.

4.4 LABOUR RELATIONS ACT 66 OF 1995

The Labour Relations Act[310] (LRA) is the primary source of legislation regulating the relationship between an employee and employer.

Section 1 of the Act provides that the purpose is to advance economic development, social justice, labour peace and the democratisation of the workplace by fulfilling the primary objectives of the Act, which are*, inter alia*, to give effect to and regulate the fundamental rights conferred by section 27 of the Constitution. Furthermore, section 3 provides that:

> 'Any person applying this Act must interpret its provisions –
>
> a) to give effect to its primary objects;
> b) in compliance with the Constitution; and
> c) in compliance with the public international law obligations of the Republic.'

Schedule 8 Item 1 (3) provides that:

> 'The key principle in this code is that employers and employees should treat one another with mutual respect. A premium is placed on both employment justice and the efficient operation of business. While employees should be protected from arbitrary action, employers are entitled to satisfactory conduct and work performance from their employees.'

This item is of particular significance to this paper – as it is pertinent to the balancing of the employer's interest to protect its business operations versus the employee's right to privacy in the workplace. This item appears to reinforce the common law principles, discussed in the earlier chapters, that employers have an obligation to protect the employees' right to privacy in the workplace. However, employees should not abuse the employer's electronic facilities.[311]

Item 7 of Schedule 8 of the LRA provides that when considering whether a dismissal is fair, one needs to consider whether or not the employee contravened a rule and if a rule was contravened, whether or not:

1) The rule was reasonable;
2) The rule had been brought to the attention of the employee
3) The rule was broken.

---

[310] Ibid.

[311] NQ Mabeka 'When Does the Conduct of an Employer Infringe on an Employee's Constitutional Right to Privacy When Intercepting or Monitoring Electronic Communications? (unpublished LLM, University of the Western Cape, 2008) at 89.

Consequently, if it is alleged that an employee has abused the employer's electronic communication facilities, it must be determined whether or not that employee was aware that he or she was not supposed to abuse such facilities before any disciplinary proceedings are instituted against him/her, having due regard the circumstances of the case.[312]

As highlighted in the preceding case law discussion, our Courts and the CCMA have had to therefore address the pertinent questions of:

- Whether the use of the employer's internet and/or telecommunication system, for personal motives, justifies dismissal?
- What content of material may or may not be distributed on an employer's telecommunication system?
- Can the employer access the employee's email to prove misconduct and justify a dismissal?

Further to the case law discussed earlier**,** an examination of other pertinent judgements are set out below:

In *Toker Bros Pty (Ltd) & Keyser*[313], the employer had intercepted the employee's electronic communication. The employee was charged with dishonesty in that he abused the employer's email and internet facilities. The employee argued that the employer's interception of his electronic communication was a violation of his right to privacy. The employer denied that it had violated the employee's privacy and argued that the employee spent excessive time on the internet for his personal use which was at the expense of the employer. Furthermore, the employer argued that the employee had been aware that his conduct was objectionable.

The Commissioner concluded that the interception was justified in the circumstances regardless of the fact that the employer had no rules or a policy regulating the interception of the latter's electronic communications. The Commissioner submitted that the employee was expected to exercise his discretion in the manner in which he used the facilities and the amount of time spent thereon. After considering the evidence, the Commissioner therefore held that the employee could have reasonably expected to be aware that he was not allowed to abuse the workplace facilities.

Regarding the employee's right to privacy in terms of section 14 of the Constitution, the Commissioner noted that although section 14 prevented the employer from intercepting the employee's electronic communications without his knowledge or consent, the interception was conducted to investigate allegations of abuse of the employer's facilities and such interception

[312] Ibid at 90.
[313] *Toker Bros* supra note 228.

was *'not malicious but incidental to the investigation'.*[314] Accordingly, the employee's right to privacy had not been infringed and the evidence obtained was admissible. Furthermore, the Commissioner considered the vicarious liability of the employer in this instance and held that this fact, justified the limitation of the employee's right to privacy.

Consequently, this judgement affirmed the principles that:

- Regardless of whether the employer has standing rules or a policy regulating the interception of the latter's electronic communications, employees are expected to exercise their discretion in the manner in which they used the facilities and the amount of time spent thereon.
- There is no infringement of the right to privacy where one party consents to the interception.
- That the employee's right to privacy is not absolute and is subject to limitations as set out in section 36 of the Constitution.
- Evidence which is obtained by intercepting employee's electronic communication could be admissible in Court, if the interception was conducted to investigate allegations of misconduct. However, this would be determined by the facts of each case.
- Employers may be held either criminally or vicariously liable for the conduct of their employees in the workplace, thus, in certain instances it may be necessary to intercept the employee's electronic communication.

In the case of *Warren Thomas Griffith's v VWSA*[315], the employee was employed as a senior engineer in the manufacturing division. The employer discovered that the employee had used the company telephone excessively to call his girlfriend. Around the same time, the employer also discovered that the internet facilities had also been abused in that 'undesirable' sites had been accessed from the employee's computer. For both abuses, the employer warned the employee and revoked his internet access. Sometime thereafter, the employee was discovered to have been surfing the internet on a colleague's computer. He was then charged with and dismissed for wilful disobedience. The employee argued, *inter alia*, that the employer had no policy relating to the use of the telephone or internet. In response, the employer submitted that the employee had been previously warned not to abuse the facilities, yet he continued to do so. [316]

The Commissioner found that despite the fact that the employer did not have any standing rules regarding email and internet use by an employee, a person with the employee's intelligence and

[314] Ibid.
[315] *Warren Thomas Griffith's v VWSA* Unreported case, CCMA, 22 June 2000 (case number EC16714).
[316] Modiba op cit note 115 at 367.

experience should have appreciated the fact that intentional disregard of the employer's warnings constituted misconduct in the ordinary sense.[317]

Finally, in the case of *Van Wyk v Independent Newspapers Gauteng (Pty) Ltd & Others*[318], the employee had addressed an email to her superior expressing her frustrations at work, following an argument with the editor and two other employees the previous night. In this email, she made derogatory remarks about the editor and related employees. Despite the fact that the email was not forwarded to any other parties, the email was delivered to the editor's desk in an unmarked envelope. The employee was subsequently dismissed for gross misconduct, in that she sent an email of malicious nature and containing derogatory remarks about the editor and other colleagues.[319]

At the arbitration, the employee argued that this email was of a private nature and should not be admissible in the disciplinary proceedings.[320]The Commissioner found that the employee should have been reasonably aware that the email could be read by persons other than its intended recipient. The arbitrator based this assertion on the fact that: the company's email policy stipulated that all information stored on the company system belongs to the company; the email had been sent to a communal company computer; the email was not marked private/confidential and dealt with work related issues.

The Labour Court confirmed the Commissioner's decision, thereby reinforcing the principle that personal emails sent from an employer's email facility are not private, especially when the intended recipient also uses the company's email system.

4.5 ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

The Electronic Communications and Transactions Act[321] (ECT Act) came into force on 30 August 2002. The Act is based on a resolution by the General Assembly of the United Nations Commission on International Trade Law (UNCITRAL) regarding electronic commerce, *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*, with additional article 5 bis as adopted in 1998 (UNCITRAL Model Law on Electronic Commerce or Model Law).[322]

---

[317] Ibid.
[318] *Van Wyk v Independent Newspapers Gauteng (Pty) Ltd & Others* 2005 (26) ILJ 2433 (LC).
[319] Ibid at para [2].
[320] Ibid at paras [13]-[15].
[321] Act 25 of 2002.
[322] SA Law Reform Commission Issue Paper 27 (Project 126 2010) *Review of the Law of Evidence Electronic Evidence in Criminal and Civil Proceedings: Admissibility and related issues* at 28.

It is believed that the ECT Act was enacted to remove barriers that previously hampered the validity of electronic consent[323]. According to the Act, the objectives are to:

- to remove barriers to electronic communications and transactions in the Republic;
- 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.[324]

Section 1 of the Act defines the following relevant terms as follows:

'data' as electronic representations of information in any form.

'data controller' as any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject.

'data subject' as any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act.

'electronic communications' as a communication by means of data messages.

Section 3 deals with the application and interpretation of the Act, and importantly, makes it clear that the adoption of the Act must not be interpreted to exclude any statutory law or the common law principles applicable to recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act and that will still apply.

Significantly, the ECT Act facilitates the legal recognition of data messages by providing that the requirements of writing, signature and contract formation may be met by such data messages.[325] These provisions therefore have implications in respect of the compliance with RICA – which, as discussed above, provides for *'prior written consent'* and *'expressed or implied consent'* to be obtained.

In terms of section 12 of the ECT Act provides that if there is a legal requirement that a document or information must be in writing, the requirement will be met if the information is a) in the form of a data message and b) it is accessible in a manner usable for subsequent reference. This section therefore means that the legal requirement that a document or information must be in writing

[323] Pistorius op cit note 2 at 7.
[324] Section 2(1) of the ECT.
[325] Pistorius op cit note 2 at 15.

will now be satisfied if the document or information is in electronic format. However, the document or information must be accessible in such a manner that the person retrieving it would be able to use it afterwards.[326]

Furthermore, section 13 of the ECT Act provides that:

1) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature[327] is used.
2) Subject to subsection (1), an electronic signature is not without legal force and effect merely because it is in electronic form.

Section 13 (5) stipulates that any other expression of intent or statement is not without legal force and effect merely on the grounds that- a) it is in the form of a data message; or b) it is not evidenced by an electronic signature by means from which such persons intent or other statement can be inferred.

The overall effect of these provisions, in the employment context, is that it assists in complying with the requirements of RICA, particularly pertaining to the monitoring and interception of employee electronic communication by the employer. This is since, in terms of the provisions, legal recognition and validation is given to the use of electronic agreements and electronic signature. Parties (such as the employee and employer) to such agreements may also agree to other methods, other than the electronic signatures, to express intent or consent. Employers may therefore conclude electronic agreements through the use of 'click wrap agreements' and make use of the electronic environment to convey policies to the employees on the use of the computer equipment and networks.[328]

Another noteworthy aspect of the ECT Act, is the provision of the protection of personal information. In this regard, section 50 highlights the provisions pertaining to the protection of personal information and section 51 (1) lists nine principles that a data controller must comply with when dealing with the interception of electronic communication.[329] These requirements, include *inter alia*, that:

[326] S Gereda 'The Electronic Communications and Transactions Act' 263 at 270 available at http*://thornton.co.za/resources/telelaw12.pdf,* accessed on 21 November 2014.
[327] An advanced signature is an electronic signature that can be authenticated only by an agency that has been accredited by the Department of Communications in terms of Section 37 of the ECT Act.
[328] Pistorius op cit note 2 at 15.
[329] Section 51(1) of ECT Act.

(1) A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.

(2) A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.

(3) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.

(4) The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.

Finally, Chapter VIII deals with the issue of Cybercrime. Essentially, in terms of section 86 of the Act entitled '*Unauthorised access to, interception of or interference with data'*, subject to the provisions of RICA, any person who intentionally accesses or intercepts any data without authority or permission to do so is guilty of an offence. Section 89 provides that the maximum penalty for a contravention of section 86 is a fine or imprisonment of 12 months. Consequently, the effect of the above provisions is that when intercepting the electronic communication of an employee, unless the employer complies with the provisions of RICA or has authority or permission from the employee to do so, such interception will amount to a contravention of section 86 of the ECT Act and therefore constitute a criminal offence.

4.6 PROTECTION OF PERSONAL INFORMATION ACT, 4 OF 2013

After much debate and anticipation in the legal community, the Protection of Personal Information Act[330] (POPI) was enacted in November 2013. Its commencement date shall be determined in accordance with section 115 of POPI by the President and its provisions will come into effect one year thereafter.

The Act was drafted largely on the recommendations of the SALC (in discussion paper 109 of project 124) wherein the SALC expressly recognised the importance of privacy in terms of the Constitution and pre-existing common law. It noted that while privacy is a fundamental right, it can be limited and balanced against economic and trade considerations looking at data privacy.[331]

[330] Act 4 of 2013.
[331] R Luck 'POPI - is South Africa keeping up with international trends?' (May 2014) *De Rebus* 84.

Consequently, POPI ultimately seeks to enforce the protection of section 14 of the Constitution, the right privacy, and has significant implications for employers; in that it introduces measures to ensure the personal information of employees is safeguarded when it is processed by employers. Employers will have to comply with the provisions of POPI whenever the personal information employees is collected, stored, or used.[332]

Section 1 of POPI defines:

'electronic communication' as any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Furthermore, 'personal information' means information relating to a person and includes all information about that person, including, *inter alia*: race, age, gender, sex, pregnancy status, marital status, nationality, ethnic or social origin, sexual orientation, physical or mental health, disability, religion, culture and language, educational, financial, criminal or employment history, location information (such as email and telephone/cellular contact numbers, biometric information).[333]

Chapter 3 of the Act deals with the '*Conditions for Lawful Processing of Personal Information'*. These provisions are similar to the provisions of section 51 of the ECT Act (as discussed above) and effectively impose several limitations on how an employer may process the personal information of an employee.

In this regard, POPI provides that:

- personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject (employee). [334]
- personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.[335]
- Personal information may only be processed if[336]:
    - The data subject consents to the processing

[332] J Van Wyk and A Van Heerden 'The Protection of Personal Information Bill from an employment perspective' available at http://werksmans.com/legal-briefs-view/protection-personal-information-bill, accessed on 02 October 2014.
[333] Section 1 of POPI.
[334] Section 9 of POPI.
[335] Section 10 of POPI.
[336] Section 11(1) of POPI.

- Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party
- Processing complies with an obligation imposed by law on the responsible party
- Processing protects the legitimate interest of the data subject
- Processing is necessary for pursuing the legitimate interest of the responsible party or of a third party to whom the information is supplied.

- Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. Steps must be taken to ensure that the data subject (employee) is aware of the purpose of the collection of the information. [337]
- Personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, except under certain conditions.[338]
- Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of section 13. [339] Hence, if an employer wishes to process information more than once, the subsequent processing must also comply with the conditions set out in POPI and be compatible with the original purposes for which it was collected.[340]
- If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of an array of facts[341]. Such details include what information is collected, the purpose of such collection and who will have access to the information.[342]

Consequently, that POPI regulates the extent to which an employer may obtain and use a variety of private employee information. This has significant impact on the employer's ability to monitor and intercept employee's electronic communication. The provisions of the Act, make it clear, that the processing of employee information is permitted, in instances only where employees consent to such processing or is aware of such processing. The import therefore, similarly to the provisions of RICA, is that an employer may only intercept or monitor employee's electronic communication, if the employee consents to such interception or is aware of the interception where they have not consented.

[337] Section 13 of POPI.
[338] Section 14 of POPI.
[339] Section 15 of POPI.
[340] Van Wyk and Van Heerden op cit note 332.
[341] Section 18 of POPI.
[342] Ibid.

CHAPTER FIVE - UNITED STATES OF AMERICA

5.1 INTRODUCTION

In the United States of America, research revealed that in the nineteenth century employee electronic monitoring took the unsophisticated form of a supervisor walking the assembly line and visually inspecting employee work.[343] At study by the American Management Association reported that 77.7% of employers responding used some form of electronic monitoring and/or surveillance to track employee activity.[344] The prevalence of this monitoring has however raised the fear that today's more sophisticated electronic tracking of employees' internet and email use diminishes employee privacy in the workplace. Many fear that the new danger of the technological workplace is the 'electronic sweatshop' where employees are subject to constant electronic monitoring.[345]

On the other hand, employers in the United States argue that they monitor employees for three primary reasons: protecting information and other intellectual property assets; increasing productivity; and avoiding liability, including exposure associated with copyright infringement by employees.[346]

This Chapter will focus on the scope and extent of the right to privacy in the United States with particular reference to the three primary sources of privacy protection: the US Constitution, Common Law, and Federal Statutes. It will consider the applicability of these sources of privacy in the employment context and analyses the dicta by the American Courts.

5.2 BACKGROUND

The essence of the right to privacy in America emanated fundamentally from the article authored by Warren and Brandeis, entitled 'The Right to Privacy'[347] which was published in the 1980s. The article emanated from Warren and Brandeis' fear of the threat to personal privacy posed by the advances of technology, which at that time related primarily to print media.[348]

---

[343] L Rustad and S Paulsson 'Monitoring employee e-mail and Internet usage: avoiding the omniscient electronic sweatshop: insights from Europe' (2005) 7 U.PA. *J Labor and Employment L* 829 at 861.
[344] AMA. 'Survey Workplace Monitoring & Surveillance: Policies and Practices, Summary of Key Findings' (2001) at 1, available at http://www.amanet.org, accessed on 28 October 2014.
[345] Rustad and Paulsson op cit note 343 at 861.
[346] R Sprague and L Determann 'Intrusive monitoring: employee privacy expectations are reasonable in Europe, destroyed in the United States' (2011) 26 *Berkeley Technology LJ* 979 at 982.
[347] S Warren and J Brandeis 'The right to privacy' (1980) *Harvard Law Review* 193.
[348] I David 'Privacy concerns regarding the monitoring of instant messaging in the workplace: is it big brother or just business?' (2004) 5 *Nevada LJ* 319 at 322; Warren and Brandeis op cit note 347 at 211.

In the article, Warren and Brandeis described the right to privacy as the right to be left alone. They further described the realisation that society was in a perpetual state of advancement; consequently, the American legal system also had to evolve perpetually to protect the individual's privacy rights.[349] It is for this reason that the article was influential in convincing the states to recognize privacy-based torts.

Subsequent to the article, Justice Brandeis went on to expand the phrase 'the right to be let alone' in his famous dissent in *Olmstead v. U.S*[350]:

> 'The makers of our Constitution understood the need to secure conditions favourable to the pursuit of happiness, and the protections guaranteed by this are much broader in scope, and include the right to life and an inviolate personality -- the right to be left alone -- the most comprehensive of rights and the right most valued by civilized men. The principle underlying the Fourth and Fifth Amendments is protection against invasions of the sanctities of a man's home and privacies of life. This is a recognition of the significance of man's spiritual nature, his feelings, and his intellect.'

Today, the concerns postulated by Warren and Brandeis in the 1980s have been replaced by concerns regarding the ability of an employer to 'electronically eavesdrop' or censor the communication of the employer.[351]

5.3 FEDERAL CONSTITUTIONAL PROTECTION OF PRIVACY

The United States Constitution does not explicitly protect the right to privacy.[352] However, the general right to privacy is rooted in the Fourth Amendment of the US Constitution which provides that 'the right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.'

This right has been unequivocally endorsed in the landmark case of *Griswold v Connecticut*[353]**,** by the Unites States Supreme Court. In the judgement, the Court determined that:

[349] Baum op cit note 12 at 1011.
[350] *Olmstead v. U.S* 277 U.S. 438, 478 (1928).
[351] David op cit note 348 at 322.
[352] A Rodriguez 'All bark, no byte: employee email privacy rights in the private sector workplace' (1998) 47 *Emory LJ* 1439 at 1442.
[353] *Griswold v Connecticut* 381 U.S 479 (1965).

> 'specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy'[354]

In the employment context, the right to privacy is usually derived from the Fourth Amendment. The limits to this right have been substantively shaped by the United States case law which has essentially established that the Fourth Amendment implied right to privacy in limited circumstances lays the foundation for potential privacy rights for public sector employers. [355] This was illustrated in the case of *Katz v United States*[356]**,** where Justice Harlan established the 'reasonableness test', a standard which still serves as the method of analyses for claims invoking the constitutional right to privacy.[357] According to Justice Harlan, the test should be a two staged enquiry[358]:

- the first enquiry is whether the individual by his or her conduct exhibits an actual (subjective) expectation of privacy?
- the second enquiry is whether the individual's subjective expectation of privacy is on that society is prepared to recognized as reasonable?

The first case to consider the application of the Fourth Amendment privacy protection in the workplace context was case of *O'Connor v Ortega.*[359] In this case, Dr Ortega who was the chief of Professional Education at the State Hospital, claimed that employees of the hospital conducted an illegal search of his office which arose from an internal investigation. The Court was therefore required to balance Dr Ortega's reasonable expectation of privacy against the Hospital's need for supervision, control and efficient operation of the workplace.[360] The Court found that:

> 'The operational realities of the workplace…may make some employee's expectations of privacy unreasonable when an intrusion by a supervisor rather than a law enforcement official. Public employees' expectation of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.'[361]

[354] Ibid at 483.
[355] Sprague and L Determann op cit note 346 at 987.
[356] *Katz v United States* 389 U.S 347 (1967).
[357] Rodriguez op cit note 352 at 1443.
[358] *Katz* supra note 356 at 361.
[359] *O'Connor v Ortega* 480 U.S 709 (1987).
[360] Ibid at 720.
[361] Ibid at 717.

The Court went on to hold that the propriety of a workplace search, at its inception and in its scope, should be judged by the standard of reasonableness under all the circumstances.[362] The Court concluded that under this standard the Fourth Amendment is violated only if public employees have an expectation of privacy that society is prepared to consider reasonable.[363] The Court ultimately resolved that this standard requires balancing the employer's need for control and supervision of the workplace against the privacy interests of employees.[364]

However, it is clearly evident that the Fourth Amendment applies only to governmental actors.[365] It does not provide rights against private individuals and in turn therefore against private employers. As a result, the Fourth Amendment right to privacy does not protect private employees from workplaces searches conducted by their employers. Thus, even if society is prepared to recognize the reasonableness of private employees' privacy expectations, the Fourth Amendment to the United States Constitution affords no protection in the private sector workplace.[366]

Nevertheless, the Fourth Amendment jurisprudence has been fundamental to the way in which the Courts have confronted claims of invasion of privacy based on others sources of the right to privacy.[367]

5.4 STATE CONSTITUTIONAL PROTECTION OF PRIVACY

Unlike the Federal Constitution, many (ten) State Constitutions explicitly guarantee a right of privacy which encompass zones of privacy broader than the privacy protections granted by the Fourth Amendment. [368] However, similarly to the Federal Constitution, the protection still generally extends only to public employees[369] and California is the only state to have extended its constitutional protection of the right to privacy to both the public and private entities.[370]

In applying this right in the employment context, the earlier judgements of the Court required private employers to show a 'compelling interest' in order to justify employee monitoring. However, in the breakthrough case of *Hill v National Collegiate Athletic Association,* [371] the

[362] Katz supra note 356 at 725-726.
[363] Ibid at 715.
[364] Ibid at 719-720.
[365] Sprague and Determann op cit note 346 at 986.
[366] Kopp op cit note 13 at 866.
[367] Rodriguez op cit note 352 at 1445; For instance, the reasonableness test laid down in *Katz* is essentially the same approach used by state courts to analyse the common-law tort of invasion of privacy.
[368] Rodriguez op cit note 352 at 1446.
[369] Kopp op cit note 13 at 867; nine out of the ten states, still maintain that their constitutional right to privacy applies only against state agencies.
[370] Rodriguez op cit note 352 at 1447.
[371] *Hill v National Collegiate Athletic Association* 865 P.2d 633 (Cal. 1994).

California Supreme Court rejected the 'compelling interest' requirement in favour of a 'balancing test' in which the privacy interest at stake must be 'specifically identified and carefully compared with competing or countervailing privacy and non- privacy interests'.[372] The Court found that the 'compelling interest' standard would still be applicable against private employers if the privacy interest at issues was fundamental to personal autonomy such as the freedom from involuntary sterilization or the freedom to pursue consensual familial relationships.[373]

Furthermore, in the case of *Flanagan v Epson America* [374] the Court declined to extend constitutional protection to email communication of private employees. In this case, the employee brought a class action challenging Epson's routine monitoring of employee email. The Court rejected the employee's constitutional claim on the basis that that the Court found that an extension of constitutional privacy rights to protect employee email communications from employer monitoring should be undertaken by the legislature and not the judiciary.[375]

5.5 FEDERAL LEGISLATION PERTAINING TO MONITORING AND REGULATION OF EMPLOYEE ELECTRONIC COMMUNICATION

5.5.1 ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

Due to the lack of protection provided by the United States Constitution, Congress responded by enacting the Electronic Communications Privacy Act of 1986 (ECPA).[376]The ECPA protects against unwarranted interception or retrieval of electronic communications.[377] Essentially, it prohibits 'the intentional or wilful interception, accession, disclosure, or use of one's electronic communication.'[378]

Title I (Federal Wiretap Statute) governs interception of communications in transmission, such as wiretaps and bugs.[379] 'Intercept' is defined as the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.[380] This Act makes it a criminal offence to intentionally intercept a wire, oral or electronic communication. In this regard, there are there are three types of activities that are prohibited: i) intercepting or endeavouring to intercept communications, , (ii) disclosing or

[372] Ibid at 655.
[373] *Hill* supra note 371 at 653.
[374] *Flanagan v Epson America* BC007036 (Cal.Super.CT1991).
[375] Ibid at 1019.
[376] C Ciocchetti 'Monitoring employee e-mail: efficient workplaces vs employee privacy' (2001) *Duke L. & Tech. Rev* 1.
[377] David op cit note 348 at 327.
[378] S Diluzio 'Workplace email: it's not as private as you may think' (2000) 25 *Del. J Cor. L* 741 at 745.
[379] 18 U.S.C§ 2511.
[380] 18 U.S.C. **§** 2510 (4).

endeavouring to disclose intercepted information, and (iii) using the content of intercepted information.[381]

In an employment context therefore, an employer who monitors email or intercepts internet communications will be deemed to have intercepted electronic communications within the meaning of the ECPA.[382] This interception has to be intentional, which means that the person committing the interception has to know or have reason to know that the information has been illegally intercepted.[383] Furthermore, third parties are allowed to monitor the transactional information of the email such as who the sender and recipient are, the date and time, and the length and subject heading of the message.[384] However, the Title protects the content of the messages when they are under transmission.[385] This means that Title I is inapplicable to an employer's search of an employee's stored email messages.[386]

Title II (Stored Communications Act) protects data post-transmission, typically once a message has been received and stored.[387] This Title protects stored communications from unauthorized or exceeded authorized access, but it does not apply to:

- the person or entities providing the wire or electronic communications service.[388]
- the user of that service or in a situation where the service was intended for that user.[389]

Importantly to the present discussion, the ECPA has three exceptions pertinent to employer monitoring:

- ***The Provider Exception***

According to section 2511 (2) (*a*) (i*), it shall not be unlawful for an operator of a switchboard, of an officer, employee or agent of a provider of wire or electronic communication service to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights.*

[381] 18 U.S.C. **§** 2511.
[382] Rustad and Paulsson op cit note 343 at 847.
[383] 18U.S.C.§2511(1).
[384] 18 U.S.C. **§** 2511.
[385] 18 U.S.C. § 2510(1).
[386] Rustad and Paulsson op cit note 343 at 847.
[387] 18 U.S.C§ 2701.
[388] 18 U.S.C. § 2701(a), (c).
[389] 18 U.S.C. § 2701(c) (1).

This section therefore allows network providers to intercept, disclose or use employee email if the privacy intrusion in question is made during the ordinary course of business and is either: 1) necessary to the rendition of service or 2) necessary to protect the rights or property of the company.[390]

This exception has been broadly interpreted by some commentators who suggest that most private employers will be exempt from ECPA liability so long as the employer is the provider of the email system.[391]This will effectively mean then that employers have an unrestricted right to monitor the email communication of its employees on a company-owned email system. However, other commentators warn that the exception is not that wide and does not apply to employers who merely provide email service to its employees through a common carrier.[392]

In the case of *Flanagan v Epson*[393], the Court considered the provider exception in the context of email monitoring in the workplace. The Court stated that 'there is simply no ECPA violation of the person or entity providing a wire or electronic communications service intentionally examines everything on the system.[394]

This argument has found support in any cases, particularly, the recent case of *Bohach v City of Reno.*[395] In this case, the officers of the Reno Police Department alleged that the Department's search of their messages over the Department's computerized paging system violated the Fourth Amendment and the wiretapping statues. The Court likened the computerized paging system to email and analysed the wiretapping claims in terms of the ECPA.[396] The Court established that the Police Department was the provider of the paging system and therefore the Court concluded that the provider exception in terms of the ECPA allows the service providers to do as they wish when it comes to accessing communications in the electronic storage system.[397]

According to Kopp, these judgements indicate that the Courts are likely to arrive at similarly broad interpretations of the provider exception to the ECPA. Kopp postulates that further that, whether intended or not, the provider exception has effectively eliminated email privacy protection for employees who utilize company-owned email systems.[398]

---

[390] Rodriguez op cit note 352.
[391] Kopp op cit note 13 at 871.
[392] Ibid.
[393] *Flanagan* supra note 374.
[394] Ibid at 100.
[395] *Bohach v City of Reno* 932 F. Supp (D.Nev.1996).
[396] Ibid at 1234.
[397] Ibid at 1236.
[398] Kopp op cit note 13 at 873.

However, notwithstanding the judgements above, more recently in a landmark decision of *City of Ontario v Quon*[399], the US Supreme Court decided against employee privacy on employer-provided devices.[400] In this case, the City of Ontario police department provided pagers to Jeff Quon and other officers. The Department's contract with its pager service provider contained a monthly limit on the number of characters each pager could send and receive. Usage exceeding that number would result in additional fees. At that time, the City had a Computer Usage, Internet and Email Policy which stated that the City reserved the right to monitor and log all network activity including email and internet use, with or without notice and that users should have no expectation of privacy or confidentiality when using these resources. Mr Quon had signed a statement of acknowledge in respect of the policy.[401]

After some time, when some police officers had exceeded their monthly character limit the city looked into a reimbursement option. However, this became an administrative burden and the City sought to determine whether the over usage was as a result of personal use. Consequently, the pager company forwarded the City transcripts of the some of the text messages. The City determined that the messages were not work related and some were sexually explicit. Mr Quon was subsequently disciplined for violating the City policy.[402] However, after discovering that the City had read their messages, some of the officers sued for a violation of their privacy.

The District Court found that the Department had an appropriate business reason to conduct a search on the transcripts, but that the officers had a reasonable expectation of privacy in their text messages. The Nineth Circuit Court agreed with the Court a quo that the officers had a reasonable expectation of privacy. Notwithstanding, the Supreme Court dissented with this view. The Supreme Court held that the City's search of the officers' text messages which were sent and received on City owned pages was reasonable under the Fourth Amendment[403] and normal in the private context.

- ***The Ordinary Course of Business Exception***

This exception focusses on the type of equipment used to access a transmission. In order to find liability under the ECPA, the violator must intercept the communication with an 'electronic, mechanical or other device'.[404] This therefore excludes from its definition any 'telephone or

[399] *City of Ontario v Quon* 130 S.Ct. 2619, 560 U.S.
[400] D Burtch and P Logan 'Reducing your Liability from Employee Electronic Communications' available at http://www.acc.com/chapters/wmacca/upload/wmacca-seminar-outline-11-4-10.pdf, accessed on 28 October 2014.
[401] Ibid.
[402] Ibid.
[403] 130 S. Ct 2619 (U.S 2010).
[404] Court and Warmington op cit note 108 at 30.

telegraph instrument, equipment or facility, or any component thereof' which is used by a provider of wire or electronic communication service in the ordinary course of its business.[405]

This exception is yet to be applied to email communication in the workplace.[406] Though, guidance is sought from an examination of its application in the context of telephone communication. Based on the case law relating to telephone communication, it is evident that the Courts have applied this exception in terms of two different approaches: a context approach or a content approach.[407]

The content approach focuses on the nature of the communication and generally allows employers to monitor business-related communications but disallows monitoring of personal communications.[408] Conversely, the context approach focuses on the employer's reason for monitoring to determine whether a legitimate business reason justified the monitoring.

The Court in the case of *Sanders v Robert Bosch Corp*.[409] followed a context approach. In this case, the employer had installed a telephone recording device known as a voice logger, which continuously recorded all telephone conversations on certain telephone lines. The employee, when learning about the recording, brought an action against the employer in terms of ECPA for the surreptitious recording of her telephone calls. The employer responded by stated that the reason for the monitoring was due to bomb threats received and therefore claimed exemption from liability under the ordinary course of business exception.[410]

After considering the evidence, the Court found that the employer failed to satisfy the required that the employer's use of the device must be made in the ordinary course of business. The Court held that the basis of recording the telephone calls due to bomb threats did not fall within the ordinary course of the employer's business. The Court also disapproved the covert nature of the monitoring – in that – the employer never informed its non-supervisory employees of the monitoring. The Court noted that the employer must invoke a legitimate business reason for covert monitoring.[411]

Conversely, in the case of *Watkins v L.M. Berry & Co,*[412] the Court followed a content approach when considering the ordinary business exception. In this case, the employee sued her employer for monitoring a personal calls he received during her lunch break. The employer alleged that a

[405] 18 U.S.C§ 2510 (4).
[406] Kopp op cit note 13 at 874.
[407] Ibid at 876.
[408] Ibid at 874.
[409] *Sanders v Robert Bosch Corp* 38 F.3d 736 (4th Cir.1994).
[410] Ibid at 740.
[411] Ibid at 741-742.
[412] *Watkins v L.M. Berry & Co* 704 F.2d 577 (11th Cir.1983).

telephone solicitation business has an established policy of monitoring calls made by its employees.[413] Furthermore, all the employees were aware of the policy as it had been part of the training program. However, employees were permitted to make personal calls but were informed that their calls would not be subject to monitoring.[414] The Court found that the employer's monitoring of solicitation calls was within the ordinary course of business however the call in question was not considered to be a business or solicitation call.[415] Thus, the Court held that the ordinary course of business exception would not exempt the employer for intercepting the personal call, except for the purpose of determining whether it is a personal call.[416] Consequently, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents.[417]

In applying these principles to electronic communication in the workplace, it is evident that in following a context approach the Courts may deem interception of employee's personal emails to fall outside the ordinary course of business exception. Whereas, in terms of the content approach, the Court may permit the interception of email communication if the employer can establish a legal interest in the subject matter of the communication.[418]

- ***The Consent Exception***

Section 2511 (2) (*d*) provides that, it shall not be unlawful to intercept communication where a person who is a party to the communication has given prior consent to such interception.

This scope of the section was considered in the case of *Deal v Spears.*[419] In this case, the employer claimed exemption under the consent exception as it alleged that it informed the employee on one occasion that it may monitor her phone calls as result of excessive use of the telephone. The Court rejected this argument and reasoned that the employer never informed the employee that it would in fact be monitoring her calls. Thus the employer was unable to escape liability under the consent exception.[420]

Conversely, in the case of *Sporer v UAL*[421], the employee was fired when the company's security department during a routine audit discovered emails of a pornography content. The employee sued the employer in terms of the ECPA for a violation of privacy. The Court dismissed the

[413] Ibid at 579.
[414] Ibid.
[415] Ibid at 582.
[416] Ibid at 583.
[417] Ibid.
[418] Kopp op cit note 13 at 881.
[419] *Deal v Spears* 980 F.2d 1153 (8th Cir.1992).
[420] Kopp op cit note 13 at 882.
[421] *Sporer v UAL* 2009 U.S Dist. LEXI 76852 (N.D Cal).

employee's claim and found that there was no privacy in emails. The Court held that the use of computers in the employment context carries with it social norms that effectively diminish the employee's reasonable expectation of privacy; and that more than three quarters the country's major firms monitored, recorded and reviewed employee communication on the job, including their emails, telephone calls, internet connections and computer files.[422]Importantly, the Court also recognised employee consent via 'click through' agreements in that the Court found that in this instance the employee had impliedly consented to the search since he clicked 'OK' acknowledging that his communication could be monitored.[423]

It is therefore argued that in terms of this section, an employer may successfully evade the prohibitions of the ECPA by implementing a policy which accepted by the employee and which therefore constitutes consent. Thus an employer would be immune from liability in terms of the ECPA.[424]

5.6 COMMON LAW PROTECTIONS

As noted, private sector employees do not enjoy any Fourth Amendment rights vis-a- vis searches or surveillance by their employers under the U.S Constitution.[425] However, private employees may derive privacy rights from a common law right to privacy which has been developed among the states during the twentieth century.[426] These rights comprise of the following:

1 Intrusion upon seclusion
2 Public disclosure of embarrassing private facts
3 Publicity which places a person in a false light in the public eye; and
4 Commercial appropriation of a person's name or likeness.

The most relevant tort to the present discussion – relating to monitoring of electronic communication in the workplace- is the intrusion upon seclusion. In terms of this tort:

> 'one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of privacy, of the intrusion would be highly offensive to a reasonable person'[427]

[422] Ibid at 8.
[423] Ibid at 9.
[424] Kopp op cit note 13 at 883.
[425] Sprague and Determann op cit note 346 at 990.
[426] Ibid.
[427] Restatement (Second) of Tort § 652B (1977). Thus, since this tort applies to invasions of privacy, 'physical or otherwise' it could be extended to protect against email monitoring.

Similar to the Fourth Amendment standard, this tort also imposes a standard of objective reasonableness. The four elements are: i) Whether the intrusion intentional ii) Whether the act in question is highly offensive to the reasonable person iii) Whether the employee's activity was subjectively and objectively private iv) Whether the employer has a legitimate purpose justifying the invasion.[428]

In the case of *Smyth v Pilsbury Co,*[429] the employee instituted a claim against his employer for wrongful discharge. The employee was discharged after the company had reviewed his emails and found offensive references to the sales management. The employee argued that his termination was against public policy as a violation of his common law right to privacy.

The Court considered the claim under the intrusion upon seclusion tort. The Court found that the employee could have a reasonable expectation of privacy in email communications voluntarily made to his supervisor over the company email system.[430] The Court found further that even if the employee was determined to have a reasonable expectation of privacy in the contents of his email, the Court would not consider the employers interception of the communication to be substantially and highly offensive invasion of his privacy.[431]The Court concluded that the privacy interest of the employee was outweighed by the employer's interest in preventing in appropriate comments over its email system.[432]

5.7 CONCLUSION

Unlike South Africa, the United States Constitution does not explicitly protect the right to privacy as a fundamental right central to the tenet of human dignity. It merely, in terms of the Fourth Amendment, prohibits unreasonable searches and seizures by state officials thereby treating the right to privacy as akin to personal property. This protection is further restrictive in that it only extends to public sector employees and therefore plays no role in the private workplace. The import is that the extent of employees' privacy rights in the workplace depends primarily on whether employees work in the public sector or private sector.

Though, despite the absence of the explicit right to privacy in the Federal Constitution, many of the States enacted the right to privacy in their Constitutions thereby recognising the protection of this right. Nonetheless, these State Constitutions mirror their federal counterpart, also offering

[428] Kopp op cit note 13 at 885.
[429] *Smyth v Pilsbury Co* 914 F.Supp. 97 (E.D Pa 1996).
[430] Ibid at 101.
[431] Ibid.
[432] Ibid.

marginal protection for employees' privacy in private sector workplaces as the protection primarily extends only to public sector employees.[433]

Similarly, despite the ECPA being enacted to prohibit unauthorized access to electronic communication, it has not significantly limited the employer's ability to intercept employee electronic communication in the workplace. The ECPA's three exceptions have proven to be strong allies to all employers desiring to monitor employee electronic communication in the workplace in that: once an employer meets of the exceptions, the ECPA places no restrictions on the manner and extent of monitoring, nor does it require that an employer notify employees of monitoring.[434]

Moreover, the common law tort of intrusion upon seclusion also does not directly uphold the employee privacy rights in the private sector workplace. This is since in order to succeed with this claim, the employee must show that the intrusion is highly offensive to a reasonable person. This is clearly a demonstrable obstacle to the employee; in that, given the nature of the business interest of most employers, it will be difficult for an employee to establish a reasonable expectation of privacy. A further difficulty is that many employers inform employees that they may be monitored and in most cases gain the consent of the employees to do. This then completely negates any expectation of privacy that an employee may have.

Consequently, after considering its application and scope, it is seemingly apparent that the expectation of privacy in the United States workplace, is to a large degree curtailed and employees appear to enjoy a very narrow zone of privacy. This assertion is based on the exposition by the American Courts who have to a certain degree illustrated, that employees have no real reasonable expectation to privacy at the workplace – particularly – in respect of email communication which is sent over an employer's email system and in cases where the employer has given the employee notice that he or she may be monitored. It is however noted that the judgement of Quon has laid down underlying principles in terms of an employer's ability to monitor employee communications on employer-provided electronic devices:[435]

- All employers should maintain comprehensive electronic equipment and system usage policies to help define an employer's right and employee's expectation of privacy within the workplace.
- Those policies should be unambiguous and clearly communicated to employees.

[433] G Lasprogata, N King and S Pillay 'Regulation of electronic employee monitoring: identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada' (2004) *Stan Tech LRev* 4.
[434] Ibid.
[435] Burtch & Logan op cit note 400 at 11.

- Employer's ability to review the electronic communication should be structured to limit intrusions into employee privacy, which is reasonably limited to the employer's legitimate, work related purposes.
- Employers should obtain a written acknowledge and consent from employees that they have received and agree to the provisions of such a policy.

Nevertheless, ultimately on the overall position in the United States, I agree with Professor Finkin on his conclusion that:

> 'The United States has no comprehensive, coherent conception of how employer and employee interests in the collection, collation, use, and dissemination of personal data are best balanced. Rather, it is a skein of discrete pockets of legislation woven against the background of a common law that fails to fill in the gaps.'[436]

[436] A Levinson 'Industrial justice: privacy protection for the employed' (2009) 18 *Cornell J L Public Policy* 609 at 619.

CHAPTER SIX - CONCLUSIONS

Although recognised both internationally and domestically as one of the most important human rights, defining the extent of the right to privacy has remained challenging. This is particularly true in the workplace context where the progression in technology has dramatically changed the way organisations perform their day-to-day operations. There is no escaping the fact that the use of the internet and email facilities (as well as other electronic means) are now critical business tools and it is almost impossible to imagine a workplace without it. However, these same tools also expose businesses to catastrophic threats and it is for this reason that employers fervently argue in favour of employee monitoring in order to protect their liability and assets.

In South Africa, the right to privacy enjoys explicit constitutional and common law protection. However, this right must be balanced with other rights and is subject to the provisions of the limitation clause as set out in section 36 of the Constitution. This was reaffirmed by the landmark Constitutional Court judgement of the *Bernstein* case, where it was recognised that no right is absolute and each right, including the right to privacy, is always limited by every other right accruing to another individual. Accordingly, in respect of the extent of the right to privacy, the Court found that a person's right to privacy extends only to those aspects of his or her life in regard to which there is a legitimate expectation, which is a subjective expectation of privacy that society recognises as objectively reasonable. It was accepted therefore that as a person moves into the public domain away from the personal realm, the more his or her right to privacy may become limited.

In addition to the common law and constitutional protection, South Africa has also enacted legislation such as RICA, the ECT Act and POPI in order to regulate the interception of electronic communication. However, as discussed in the preceding chapters – these legislative provisions, particularly pertaining to RICA, have been the subject of much debate and uncertainty. Moreover, case law has not directly addressed the application thereof. Consequently, it is evident that the existing legislative framework still does not specifically address the privacy concerns in a workplace context. Employers and employees remain unclear and are left with no clear legislative guidelines to indicate the exact extent of employee privacy and its interrelation with the employer's right to monitor.

Nevertheless, direction can be taken from the minority of cases where the Courts have had to consider this clash of interests between the employer and employee. In these instances, the Courts have demonstrated that employees enjoy very little privacy in respect of their electronic communications in the workplace. Essentially, the Courts have confirmed that employers are entitled to monitor and intercept the electronic communication of their employees, with or

without their consent. In reaching this position, the Courts have placed significant weight on the business reasons for employee monitoring, including the notion that the employer, as the owner of the electronic communication systems in the workplace, is justified in regulating employee communication in order to protect its business interests. The Courts have held further that although the employee has a legitimate expectation of privacy, this expectation is determined and dependant on the operational requirements of the workplace and in certain circumstances, an employer may be justified in intercepting or monitoring the employee's electronic communication without his or her knowledge and even in the absence of an electronic policy.

On the other hand, our Courts have not afforded employers unrestricted entitlement to intercept or monitor electronic communication. The Courts have held that the employer is still required to respect the rights of the employers and exercise care and discretion when intercepting the contents of employee email communication. Particular consideration is given to the manner in which the communication is intercepted and whether the employer could employ other less restrictive methods of obtaining the information.

Consequently, it is apparent that although generally employee monitoring has found support in the jurisprudence (albeit through a limited number of cases); employers are still warned to tread carefully when intercepting electronic communication in the workplace.

The writer of this dissertation, is in agreement with the position favouring employee monitoring due to the simple reason that it is irrational to expect employers not to take steps to protect the business against the potential harm which could be caused. However, having said that – the writer does not support the principle of monitoring or intercepting employee communication *'in secret'*. It is trite that the employee relationship is one based on trust, loyalty and respect, and adopting such practices without the consent or knowledge of the employee could lead to a breakdown of the relationship.

As a result, it is the writer's view that they best way to achieve the balance between the interests of the employer and employee, would be for the employer to formulate, adopt and communicate an electronic communication policy, which clearly sets out:

- the rights and obligations of the employer as well as the duties of the employee.
- the rules regarding the email and internet use, especially with regard to the private use of the workplace facilities.
- the expectation of privacy.

It is advisable for the employer to ensure that such policy is acknowledged and consented to by the employee, preferably upon commencement of their employment. This prior consent will

effectively protect the employer from liability and remove any expectation of privacy. It will also in turn protect the employee in that he or she will be fully aware that such electronic communication may be monitored and can guard against sending any detrimental information.

Case List

B

Bamford & Others / Energiser (SA) Ltd 2001 (12) BALR 1251 (P)

Bernstein v Bester 1996 (2) SA 751 (CC)

Bohach v City of Reno 932 F. Supp (D.Nev.1996)

Boland Bank Bpk v Belville Municipality 1981 (2) SA 437 (C)

C

Case & Another v Minister of Safety and Security & Others 1996 (3) SA 617 (CC)

City of Ontario v Quon 130 S.Ct. 2619, 560 U.S

Cronje v Toyota Manufacturing 2001 (3) BALR 213 (CCMA).

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

D

Dauth & Brown & Weirs Cash & Carry 2002 (8) BALR 837 (CCMA)

Deal v Spears 980 F.2d 1153 (8th Cir.1992)

E

Epstein v Epstein 1906 TH 87

F

Feldman (Pty) Ltd v Mall 1945 AD 733

Flanagan v Epson America No BC007036 (Cal.Super.CT1991)

Fredericks v Jo Barkett Fashions 2011 JOL 27923 (CCMA)

G

Goosen v Caroline's Frozen Yogurt Parlour 1995 (16) ILJ 396 (IC)

Griswold v Connecticut 381 U.S 479 (1965)

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

H

Hill v National Collegiate Athletic Association 865 P.2d 633 (Cal. 1994)

I

Investigating Directorate: Serious Economic Offences & Others v Ltd & Others: In Re Hyundai Motor Distributors (Pty) Ltd & Others v Smith NO & Others 2011 (1) SA 545 (CC)

K

Katz v US 389 US (1967)

Kidson v SA Associated Newspapers Ltd 1957 (3) SA 461 (W)

M

Minister of Safety and Security v Jordaan 2000 (4) SA 21 (SCA)

Mistry v Interim Medical & Dental Council of South Africa & Others 1998 (4) SA 1127 (CC) 1127 (CC)

Mokoena & Another v Garden Art (Pty) Ltd & Another (2008) 29 ILJ 1190 (LC)

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

N

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

National Media Ltd & Another v Jooste 1996 (3) SA 262 (A)

National Media v Bogoshi (1998) 4 SA 1995 (SCA)

NK v Minister of Safety & Security 2005 (6) SA 40 (CC)

Ntsabo v Real Security CC (2003) 24 ILJ 2341 (LC)

O

O Keeffe v Argus Printing & Publishing Co.Ltd & Others 1954 (3) SA 244 (C)

O'Connor v Ortega 480 U.S 709 (1987)

Olmstead v. U.S 277 U.S. 438, 478 (1928)

P

Philander/CSC Computer Sciences 2002 (3) BALR 304 (CCMA)

Protea Technology Ltd & Another v Wainer & Others 1997 (9) BCLR 1225 (W)

R

Reid-Daly v Hickman & Others 1981 (2) SA 315 (ZA)

S

S v A 1971 (2) SA 293 (T)

S v Dube 2002 (2) SA 583 (NPD)

S v I & Another 1976 (1) SA 781 (A)

S v Jordaan 2002 (6) SA 642 (CC)

S v Kidson 1999 (1) SACR 338 (W)

S v Makwanyane 1995 (3) SA 391 (CC)

S v Manamela & Another (Director-General of Justice Intervening) 2000 (3) SA 1 (CC)

Sage Holdings Ltd & Another v Financial Mail (Pty) Ltd 1991 (2) SA 11 (W)

Sanders v Robert Bosch Corp 38 F.3d 736 (4th Cir.1994)

Sedick & Another v Krisray *(Pty) Ltd* 2011 (8) BALR 879 (CCMA);

Singh & Island View Storage Ltd (2004) 13 CCMA

Smuts v Backup Storage Facilities & Others [2003] 2 BALR 219 (CCMA)

Smyth v Pilsbury Co 914 F.Supp. 97 (E.D Pa 1996)

Sporer v UAL 2009 U.S Dist. LEXI 76852 (N.D Cal)

Sugreen v Standard Bank of SA 2002 (7) BALR 769 (CCMA)

T

Tape Wine Trading CC v Cape Classic Wines (Western Cape) 1999 (4) SA 194 (CC)

Toker Bros (Pty) Ltd &Keyser (2005) 26 ILJ 1366 (CCMA)

V

Van Wyk v Independent Newspapers Gauteng (Pty) Ltd & Others 2005 (26) ILJ 2433 (LC)

Viljoen v Smith 1997 (18) ILJ 61 (A)

W

Watkins v L.M. Berry & Co 704 F.2d 577 (11th Cir.1983)

Warren Thomas Griffiths v VWSA CCMA, 22 June 2000 (case number EC16714, unreported)

Legislation

The Constitution of the Republic of South Africa Act 108 of 1996

The Electronic Communications Act 25 of 2002

The Employment Equity Act 55 of 1998

The Interception and Monitoring Prohibition Act 127 of 1992

The Interim Constitution of the Republic of South Africa, Act 200 of 1993

The Labour Relations Act 66 of 1995

The Protection from Harassment Act 17 of 2011

The Protection of Personal Information Act 4 of 2013

The Regulation of Interception of Communications and Provision of Communication Related Information Act 70 Of 2002

Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 (III) of December 10 1948

Journals

1 Baum, K 'E-mail in the workplace and the right to privacy' (1997) 42 *Vill. L. Rev*. 1011.

2 Beech, W 'The right of an employer to monitor employees electronic mail, telephone calls, internet usage, and other recordings' (2005) 26 *ILJ* 650.

3 Botha, M and Millar, D 'The past, present and future of vicarious liability in South Africa' (2012) *De Jure* 225.

4 Calitz, K 'Vicarious liability of employers: reconsidering the risks as the basis of liability' (2005) 2 *TSAR* 215.

5 Ciocchetti, C 'Monitoring employee e-mail: efficient workplaces vs employee privacy' (2001) 0026 *Duke L. & Tech. Rev* 1.

6 Collier, D 'Workplace privacy in the cyber age' (2002) 23 *ILJ* 1743.

7 Conlon, K 'Privacy in the workplace' (1996) 72 *Chicago-Kent Law Review* 29.
8 Court, L and Warmington, C 'The workplace privacy myth: why electronic monitoring is here to stay' (2004) 29 *Okla. City U. L Rev* 15.
9 Dancaster, L 'Internet abuse: a survey of South African companies' (2001) 22 *ILJ* 862.
10 David, I 'Privacy Concerns Regarding the Monitoring of Instant Messaging in the Workplace: Is it Big Brother or Just Business?' (2004) 5 *Nevada Law Journal* 319
11 Dekker, A 'Vices or devices: employee monitoring in the workplace' (2004) 16 (4) *SA Merc LJ* 624.
12 Devenish, G 'The Limitation Clause Revisited – The limitation of Rights in the 1996 Constitution' 1998 *Obiter* 263.
13 Diluzio, S 'Workplace Email: It's Not a Private as You May Think' (2000) 25 *Del. J Corp. L.* 741.
14 Etsebeth, V 'The Growing Expansion of Vicarious Liability in the Information Age (part 1)' (2006) 2 *TSAR* 564.
15 Etsebeth V, 'The Growing Expansion of Vicarious Liability in the Information Age (part 2)' (2006) (4) *TSAR* 755.
16 Freeman, R and Martin, K 'Some Problems with Employee Monitoring' 2003 (43) *Journal of Business Ethics* 353.
17 Hornug, M 'Think before you Type: A Look at Email Privacy in the Work Place' 2005 (11) 1 *Fordham Journal of Corporate & Financial Law* 115.
18 Kopp, K 'Electronic Communications in the Workplace: Email Monitoring and the Right of Privacy' (1998) 8 *Seton Hall Constitutional Law Journal* 862.
19 Landman, A and Ndou, MM 'The Protection from Harassment Act and its implications for the Workplace' (2013) 22 (9) *April Contemporary Labour Law* 81.
20 Lasproga, G, King, N and Pillay, S 'Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada' (2004) *Stan.Tech.L.Rev* 4.
21 Lawack-Davids, V A and van der Walt, A, 'Interception of Electronic Communication in the Workplace' (2005) 26 (1) *Obiter* 133
22 Le Roux, R 'Aspects of South African law as it applies to corruption in the workplace' (2004) 17 *SACJ* 158.
23 Levinson, A 'Industrial justice: privacy protection for the employed' (2009) 18 *Cornell Journal of Law and Public Policy* 609.
24 Luck, R 'POPI - is South Africa keeping up with international trends?'(May 2014) *De Rebus* 84.
25 McGregor, M 'The right to privacy in the workplace: general case law and guidelines for using the internet and e-mail' (2004) 16 (3) *SA Merc LJ* 638.
26 Mischke, C 'Workplace Privacy, e-mail Interception and the Law' (2003) 12 (8) *CLL* 72.

27 Modiba, M 'Intercepting and monitoring employees' e-mail communication and internet access' (2003) 15 *SA Merc L* 365.

28 Neethling, J 'The concept of privacy in South African law: notes' (2005) 122 (1) *SALJ* 18.

29 Pistorius, T 'Monitoring, Interception and Big Boss in the workplace: is the Devil in the Detail?' (2009) *PER* 1.

30 Ressler, JS 'Privacy, plaintiffs and pseudonyms: the anonymous doe plaintiff in the information age' (2004) 53 (1) *The University of Kansas Law Review* 202.

31 Rodriguez, A 'All bark, no byte: employee email privacy rights in the private sector workplace' (1998) 47 *Emory L. J.* 143.

32 Roos, A 'Privacy in the Facebook era: A South African perspective' (2012) 129 *SALJ* 378.

33 Rustad, L and Paulsson, S 'Monitoring employee e-mail and internet usage: avoiding the omniscient electronic sweatshop: insights from Europe' (2005) 7:4 U.PA. *Journal of Labor and Employment Law* 829.

34 Sprague, R and Determann, L 'Intrusive monitoring: employee privacy expectations are reasonable in Europe, destroyed in the United States' (2011) 26 *Berkeley Technology Law Journal* 979.

35 Subramanien, D and Whitear-Nel, N 'A fresh perspective on South African Law relating to the risks posed to employers when employees abuse the internet' (2013) 37 (1) *SALR* 10.

36 Van Jaarsvel, M 'Forewarned is forearmed: some thoughts on the inappropriate use of computers in the workplace' (2004) 16 *SA Merc LJ* 651.

37 Warren, S and Brandeis, J 'The right to privacy' (1980) *Harvard Law Review* 193

38 Yerby, J 'Legal and ethical issues of employee monitoring' (2013) 1 *Online Journal of Applied Knowledge Management* 44.

Internet references

1 Vault.com. Survey Workplace Monitoring & Surveillance: Policies and Practices, Summary of Key Findings' (2001) available at http://www.amanet.org accessed on 28 October 2014.

2 Bawa, N, 'The Regulation of the Interception of Communications and Provision of Related Information Act' Telecommunications Law in South' (2006) available at http://thornton.co.za/resources/telelaw13.pdf accessed on 21 November 2014.

3 Burtch, D and Logan, P 'Reducing your Liability from Employee Electronic Communications' available at http://www.acc.com/chapters/wmacca/upload/wmacca-seminar-outline-11-4-10.pdf accessed on 28 October 2014.

4 Gereda, S 'The Electronic Communications and Transactions Act' available at http://thornton.co.za/resources/telelaw12.pdf accessed on 21 November 2014.

5 GFI. White Paper 'Internet Monitoring not 'Big Brother' but 'Wise Management'' available at http://www.gfi.com/whitepapers/Internet_Monitoring.pdf accessed on 21 November 2014.

6 Michalson, L 'The Use of E-mail and the Internet in the Workplace' (1999) available at http://www.comp.dit.ie/rfitzpatrick/The%20use%20of%20email%20and%20the%20Internet%20in%20the%20Workplace.pdf accessed on 21 November 2014.

7 Vault.com. 'Survey Internet Use in the Workplace' Fall 2000 available at http://www.vault.com/surveys/internetuse2000/results/2000 accessed on 21 November 2014.

8 SA Law Reform Commission Discussion Paper 109 'Privacy and Data Protection' (Project 124) (Pretoria: SALRC 2005) available at http://www.justice.gov.za/salrc/dpapers/dp109.pdf accessed on 16 August 2013.

9 SA Law Reform Commission Issue Paper 28 'Review of the law of evidence electronic evidence in criminal and civil proceedings: Admissibility and related issues' (Project 126) (Pretoria: SALRC 2010) available at http://www.justice.gov.za/salrc/ipapers/ip27_pr126_2010.pdf accessed on 21 November 2014.

10 Schoeman, H and Jones, M 'Legality of Monitoring E-Mail at the Workplace: A Legal Update' available at http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/078.pdf, accessed on 16 August 2013.

11 Van Wyk, J and Van Heerden, A 'The Protection of Personal Information Bill from an employment perspective' available at http://werksmans.com/legal-briefs-view/protection-personal-information-bill, accessed on 02 October 2014.

Books

1 Burchell, J *Personality Rights and Freedom of Expression: The Modern Actio Injuriarum'* (Cape Town: Juta & Co 1998).

2 De Waal, J and Currie, I *Bill of Rights Handbook* 5th ed (Cape Town: Juta and Co Ltd 2005).

3 Devenish, A *Commentary on the South Africa Bill of Rights* (Durban: Butterworths 1999).

4 McQuoid-Mason, D *The Law of Privacy in South Africa* (Johannesburg: Juta & Co1978).

5 Neethling, J et al *Law of Personality* 2nd ed (Durban: LexisNexis Butterworths 2005).

6 Neethling, J et al *Law of Delict* (Durban: LexisNexis Butterworths 2006)

Theses

1 Gondwe, M 'The Protection of Privacy in the Workplace: A Comparative Study' (unpublished PhD thesis, University of Stellenbosch, 2011).

2 Mabeka, N 'When does the conduct of an employer infringe on an employee's constitutional right to privacy when intercepting or monitoring electronic communications?. (unpublished LLM thesis, University of the Western Cape, 2008)

3 Watt, J 'Electronic Workplace Surveillance and Employee Privacy – A Comparative Analysis of Privacy Protection in Australia and the United States (unpublished LLM thesis, Queensland University of Technology, 2009).