UNIVERSITY OF THE WESTERN CAPE

FACULTY OF LAW

WHEN DOES THE CONDUCT OF AN EMPLOYER INFRINGE ON AN EMPLOYEE'S CONSTITUTIONAL RIGHT TO PRIVACY WHEN INTERCEPTING OR MONITORING ELECTRONIC COMMNUNICATIONS?

NQ MABEKA

SUPERVISOR: CRAIG BOSCH

Key words

Electronic communication

Monitoring communication

Employee's right to privacy

Workplace privacy

Employer

Privacy

Communication

RICA

Direct communication

Indirect communication

ABSTRACT

The Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) that regulates the monitoring of electronic communications has not yet been tested by our courts.

This paper explores the likelihood of an infringement of an employee's right to privacy by an employer in the process of intercepting the latter's electronic communications.

It is argued that there is no explicit provision of the protection of the right to privacy that is provided in the LRA.

It is further argued that the provisions of section 4, 5 and 6 of RICA as they stand do not necessarily provide for the protection of an employee's right to privacy, but the incorporation of these sections could be construed as meaning that the legislature or the framers of the legislation intended to limit the employers right to trade freely, at the same breath, limit the employees' right to privacy.

It is argued that RICA does not provide protection for the right to privacy wherein consent has been obtained under duress or based on misrepresentation of facts. It is contended that the interception of employees' electronic communications in such circumstances would be regarded as an infringement of such employees' right to privacy. The burden of proving duress or misrepresentation of facts rests on the employee who alleges that such consent was obtained under duress or based on misrepresentation of facts.

It is also argued that RICA does not define the meaning of the words "*in the course of carrying on of business or reasonable steps*" provided in section 6 of RICA. It is argued that the meaning of "*in the course of carrying on of business*" would be determined by the type of the industry upon which the business operates, as well as the circumstances of the case.

Reasonable steps would be regarded as being taken if employers notify employees that their electronic communications would be intercepted. The manner of notification would be determined by the circumstances of the case.

It is argued that if employers conform to the provisions of section 4, 5 and 6 of RICA, and intercept the employees' electronic communications, the employer's conduct would not be regarded as an infringement of such employees' right to privacy.

The paper is concluded by providing a copy of the draft proposed regulations that illustrates the submissions and recommendations made to address all the problematic areas that have been identified in RICA.

31 May 2008

DECLARATION

I Nombulelo Queen Mabeka declare that *When does the conduct of an employer infringe on an employee's constitutional right to privacy when intercepting/monitoring electronic communications?* is my work, and that it has not been submitted before for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged as complete references.

Nombulelo Queen Mabeka 31 May 2008

Signed …….

ACKNOWLEDGEMENT

I wish to express my sincere gratitude to my supervisor, Craig Bosch and Prof F du Toit for sharing academic expertise with me and assisting in the production of the quality of this paper, which would play a significant role in the development of our law.

Table of contents

Chapter 1

Chapter 2

Chapter 3

15. Introduction
16. General Literature
17. International Conventions
18. United Kingdom

18.1The relevant provisions of the Data Protection Act of 1998

18.2 The approach of the European Courts

19. United State of America
20. Canadian Law
21. Australian Law
22. Conclusion

Chapter 4

23. Introduction
24. Common law principles relating to employment relationship
25. Labour Relations Act
26. Promotion of Access to Information Act 2 of 2000
27. How do courts apply the common law principles relating to employment relationship in light of monitoring electronic communications?
28. General principles of interpreting statutes

Chapter 5

ABBREVIATIONS

Regulations of Communications and Provisions of Communication-Related Information Act 70 of 2002	RICA
Interception and Monitoring Prohibition Act 127 of 1992	IMP Act
Labour Relations Act 66 of 1995	LR A
The Constitution of the Republic of South Africa	1996 Constitution
Electronic Communications Act 36 of 2005	EC Act
Electronic Communications and Transactions Act 25 of 2002	ECT Act
South African Law Reform Commission	SALRC
Law of South Africa	LAWSA
The Protection of Personal Information Bill	The Bill
Personal Information Protection and Electronic Documents Act	PIPEDA
Electronic Communications Privacy Act of 1986	ECPA

CHAPTER ONE

19. Introduction

The object of this thesis is to address problems that have been identified in balancing the employer's right to conduct its business effectively by monitoring its employees' electronic communications, on the one hand and the employees' right to privacy on the other hand. These problems are identified in section 4, 5 and 6 of RICA. Section 4 of RICA provides for the interception of electronic communications by a party to communication. Section 5 provides for interception of communications with prior consent in writing from a person who is a party to such communication. Section 6 of RICA provides for the interception of indirect communication in connection with carrying on of business.

The question is, do the said provisions include implied consent where there is no express provision incorporated in the employment contract or where there are no policies in place? Furthermore, do the provisions in question include instances where employees only conclude oral contracts of employment? These questions are asked notwithstanding the fact that RICA provides that prior consent in writing ought to be obtained, because in practice there are circumstances where employees do not sign contracts that expressly incorporate provisions that permit employers to monitor their electronic communications.

Above this, some employers do not have policies in place that permit monitoring of employees' electronic communications. Another question that is pertinent in the construction of the provisions of section 6(1)(a) of RICA is, what is regarded as ordinary course of business? As it will be seen later, there are loopholes in RICA, which could result in the possibility of an infringement of the right to privacy.

This thesis examines the problems that are illustrated *supra* and provides possible guidelines and submissions that our courts should consider in interpreting and applying the provisions of RICA when considering whether or not employees' right to privacy has been infringed. This is achieved by employing legal principles relevant in the interpretation of statutes.

In addition, the questions that are asked in this thesis are answered by considering the following: the approach followed by the courts in cases decided pursuant to the provisions of the IMP Act, the Constitution and Constitutional Court judgments, wherein the protection of the right to privacy is invoked or challenged. Other statutes, namely the LRA are also employed. Furthermore, this thesis investigates the likelihood of the promulgation of regulations pursuant to the provisions of RICA that would balance the conflicting rights and a draft copy of the proposed regulations is provided, which should be considered by the legislature as well as the judiciary.

20. **Research methodology**

This thesis is divided into five chapters. The first chapter briefly sets out the idea for the thesis and its motivation by considering the problems that are identified in the construction of sections 4, 5 and 6 of RICA. The information in this thesis is extracted from various textbooks, statutes, internet, case law and treaties. The gist of the following is considered: common law, the Constitution, LRA, RICA, ECA, ECT Act and international law. Chapter two discusses in great detail the following: the common law; the 1996 Constitution, IMP Act, RICA, EC Act, ECT Act and the LRA. In addition, the principles of interpretation of statutes, having due regard to any other instruments that relate to the right to privacy and the monitoring or interception of electronic communications, are also considered. The interpretation of the said provisions is accomplished by employing the statutes referred to in this paragraph, case law, various textbooks, articles, law journals and jurisprudence.

Chapter three discusses in detail, international and foreign law with specific reference to the United Kingdom, Canada, the United States of America, Australia and International Conventions or Treaties. The international law instruments that regulate the interception or monitoring of electronic communications in the said countries are also considered together with the relevant case law. Various international and foreign academic articles and books are also employed.

Chapter four discusses in detail the role of the right to privacy in the context of electronic communications. This is executed by considering common law, the LRA, RICA, and other employment statutes that might be relevant to this thesis.

The provisions of the 1996 Constitution are also considered together with legal principles of the construction of statutes. In addition, case law, textbooks articles, internet and law journals are consulted. Chapter five illustrates the findings and recommendations that relate to the protection of the right to privacy and the interception or monitoring of electronic communications in the workplace. This chapter is concluded by providing a draft copy of proposed regulations pursuant to RICA.

CHAPTER TWO

3. Introduction

"What and where is the balance between the rights to have one's privacy respected the free flow of information, the right to receive and impart information and the right to engage in economic activity"?[1] The right to privacy has been found to be one of the most fundamental rights by the Constitutional Court, and now the protection of this right is entrenched in section 14 of the Constitution. In *Bernstein v Bester*[2] the court put emphasis on the protection of the right to privacy insofar as the interception of one's communication is concerned. Warren Beech[3] expresses the view that employers should draft policies that aim at protecting their interest in relation to the unauthorised use of their facilities, thus computers and telephones.

This chapter considers various sources that are pertinent to the protection of the right to privacy, in the context of interception or monitoring employees' electronic communications. The chapter begins by discussing common law, this is followed by the discussion of the 1996 Constitution; how our courts protect the right to privacy? RICA, EC Act, ECT Act, the LRA, principles relevant to interpreting statutes and the Protection of Personal Information Bill.

21. The law before the Constitution

Ronald Standler[4] illustrates that the courts have classified the protection of the right to privacy as the "right to be left alone". This principle has been reinforced by the South African court in *O'Keeffe v Argus Printing and Publishing Co. Ltd and Others*.[5]

---

[1] S Nadasen (2002) *Data Protection is coming … time to start preparing: Insurance & Tax* V 14(4).

[2] 1996 4 BCLR 449 (CC)

[3] Warren Beech (2005) *The right of an employer to monitor employee's electronic mail, telephone calls, internet usage and other recordings.- page?*

[4] Ronald Standler (1997) Privacy in the USA [Online] Available

http://www.rbs2.com/privacy.htm

[5] 1954 3 SA 244 (C).

Professor MacQuoid-Mason[6] asserts that the recognition of the protection of the right to privacy goes as far back as the Roman Dutch Law. Furthermore, the protection of the right to privacy has been enforced in the *actio iniuriarum* or Aquilian action and the protection of the right to privacy has been regarded as the concept of *dignitas.* The SALRC[7] in the Discussion Paper 109 Project 124 puts emphasis on the principle set out in *O'Keeffe v Argus Printing and Publishing Co Ltd* that the protection of the right to privacy falls within the ambit of the concept of *dignitas*. [8]

The National Workrights Institute[9] indicates that employees who sought to claim the protection of the right to privacy in relation to the monitoring of their electronic communications brought this action under the intrusion or seclusion principle. The South African courts might consider the views expressed by the US courts in the construction of the provisions of RICA, because the 1996 Constitution requires the courts to consider international and foreign law pursuant to the provisions of section 39 of the Constitution. This however in my view does not necessarily mean that the courts would not find for employees who seek to protect their right to privacy against the employer who has applied the provisions of section 4, 5 and 6 of RICA. The South African Courts have an inherent jurisdiction to exercise their discretion based on the merits of each case.

In *S v A*[10] the court had to consider whether there had been an infringement of the right to privacy or not. In this case, private investigators tapped the complainants' telephone in order to obtain evidence of infidelity. Botha AJ reiterated the principle that the right to privacy is a right that individuals ought to enjoy. Further, the infringement of the right to privacy in the circumstances constituted an impairment of the right to dignity.

---

[6] D J McQuoid-Mason 1978 p xxxix.

[7] South African La Reform Commission Discussion Paper 109 Project 124 2005 Chapter 2 ; See also Neethling *et al* (2005) 219.

8.Neethling *et al* (2005) 219.

[9] The National Workrights Institute, *Electronic Monitoring in the Workplace: Common Law & Federal Statutory Protection* [Online] Available

http://www.workrights.org/issue-electronic/em-common-law.html.

[10] 1971 2 SA 293 T.

Botha AJ however could not agree with the argument that the placing of the listening device in the complainants' telephone constituted only a slight impairment of the right to privacy. Instead Botha AJ found that the infringement of the complainants' right to privacy *in casu* was considered to be serious impairment of such a right. This principle was later affirmed by the court in *S v I*[11]. The appellants were held criminally liable for peeping through the complainants' bedroom window in an attempt to obtain evidence of infidelity. Beadle ACJ considered and applied the principles set out in *S v A* 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.

Beadle ACJ further applied the Canadian Court principle of reasonable circumstances test that has been set out by the court in *Davis v McArthur*[12]. This test according to the court is applied by considering the lawful interest of others. In addition, Beadle ACJ set out the elements that should be considered in protection of the right to privacy. These elements are: "*the nature, incidence and occasion of the act or conduct and to the relationship, whether domestic or other, between the parties* …". [13] These elements are pertinent in considering whether or not employees' right to privacy has been infringed by the interception or monitoring of the latter's electronic communications.

In *Kidson v SA Associated Newspapers Ltd*[14] *Kuper* J considered 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. It was alleged that '97 Lonely Nurses want Boy Friends'.[15] The applicants were nurses, one of them was married, one of the applicants was engaged to be married and the third applicant was unmarried.

---

[11] 1979 1 SA 781 RA.

[12] 1970 17 D.L.R 760.

[13] *Ibid.*

[14] 1957 3 SA 461 W.

[15] *Ibid.*

Kuper J concluded 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 or *contumelia* to the young married plaintiff, thus there had indeed been an infringement of the right to privacy". [16] The principle illustrated in this case, although the case considers the general application of the protection of the right to privacy, may be employed if employers publish information that has been intercepted by the latter to determine whether or not such interception infringes on the employees' right to privacy.

The above common law review denotes the principles that our courts could apply in constructing the provisions of RICA, to determine whether an employee's right to privacy had indeed been infringed or not. The common law protection of the right to privacy is now entrenched in section 14 of the 1996 Constitution. Before this, this right was protected in section 13 of the Interim Constitution. The provisions of these two Constitutions are discussed *infra.*

5. **The Constitution**

Section 1 of the 1996 Constitution makes provision for the founding values of the Constitution.

This section states:

> The Republic of South Africa is one, sovereign, democratic state founded on the following values:
>
> (a)Human dignity, the achievement of equality and the advancement of human rights and freedoms.
>
> (b)Non-racialism and non-sexism.
>
> (c)Supremacy of the constitution and the rule of law.
>
> (d)Universal adult suffrage, a national common voter's roll, regular elections and a multi-party system of democratic government, to ensure accountability, responsiveness and openness.

[16] *Ibid.*

The provision of this section reinforces the principle that human dignity is regarded as one of the fundamental rights that is related to the right to privacy by Neethling *et al*, Debbie Collier and other academic writers.

Section 2 of the Constitution provides that:

> This Constitution is the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled.

This provision of the Constitution must be read with section 172 of the Constitution because same confers powers on the Constitutional Court to declare RICA invalid, if it is found that same is inconsistent with the provisions of the Bill of Rights.

Section 7 of the Constitution provides that:

> The Bill of Rights is a cornerstone of democracy in South Africa that enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality and freedom.
> The state must respect, protect, promote and fulfil the rights in the Bill of Rights. The rights in the Bill of Rights are subject to the limitations contained or referred to in section 36 or elsewhere in the Bill.

This section affirms the founding value of human dignity that has been clustered with the right to privacy. The courts may apply these provisions when balancing the competing rights. Thus, the right to trade freely and the right to privacy.

Section 8 of the Constitution provides that:

> (1) The Constitution applies to all and binds the legislature, the executive, the judiciary and all organs of state.
> (2) When applying a provision of the Bill of Rights to a natural or juristic person in terms of subsection (2), a court –
>
> (a) in order to give effect to a right in the Bill, must apply, or if necessary develop, the common law to the extent that legislation does not give effect to that right; and

> may develop rules of the common law to limit the right, provided that the limitation is in accordance with section 36.

The provisions of this section illustrate that the Bill of Rights apply in an employment law context because it illustrates that employers are also bound by the Bill of Rights. Therefore employers are required to protect the employees' rights in the process of intercepting the latter's electronic communications. This provision is significant because it shows that employers are also bound by the provisions of the 1996 Constitution. Therefore they cannot just intercept employees' electronic communications without considering the protection of the right to privacy that is entrenched in section 14 of the 1996 Constitution.

Section 14 provides that:

> Everyone has the right to privacy, which includes the right not to have:
> (a)their person or home searched;
> (b)their property searched;
> (c)their possessions seized; or
> (d)the privacy of their communications infringed.

The provisions of section illustrate that employers are required to protect employees' right to privacy. Therefore these employees have a reasonable expectation to privacy in the workplace. Currie & de Waal[17] describe the provisions of section 14 of the Constitution as having two parts: ''The first part guarantees a general right to privacy, the second protects against specific infringements of privacy, namely searches and seizures and infringement of the privacy of communications".[18] In addition, the interception of electronic communications is regarded as one of the grounds for claiming the protection of the right to privacy.

[17] Currie & de Waal (2005) Bill of Rights Handbook 317 & 318 (Please note that reference to Currie & de Waal in this paper refers to this Bill of Rights Handbook) .

[18] *Ibid.*

Currie & de Waal[19] further articulate that there is a subjective and objective expectation of the right to privacy. Furthermore, if one waives his/her right to privacy, he/she cannot expect to later seek the protection of the right to privacy. The waiver of the right in question according to these academic writers occurs when a person consents to the invasion of the right to privacy. In addition, such consent can either be expressly or impliedly obtained. Further the test that is applied is what is reasonable pursuant to the values that "link the standard of reasonableness".[20] This averment shows that if employees sign employment contract wherein they waive their right to privacy, they cannot later claim the protection of the right to privacy when their electronic communications are intercepted by employers.

Neethling[21] expresses the view that "the acquaintance with private facts should not only be contrary to the subjective determination and will of the prejudiced party, but at the same time, viewed objectively, also be unreasonable or contrary to the legal convictions of the community". [22]This principle according to Neethling has been reinforced by the Constitutional Court.

Debbie Collier[23] suggests that the protection of the right to privacy includes the protection of personal data in an employment law context. Collier further articulates that employers are required to protect employees' personal data from being disclosed to others. The provisions of section 14 of the Constitution, according to Collier, strictly prohibit the interception of employees' electronic communications. Moreover, the interception is only permitted if the circumstances of the case call for the limitation of such employees' right to privacy.

[19] *Ibid.*

[20] *Ibid.*

[21] J Neethling *Personality rights: A comparative overview* CISA Vol 38(2) July 2005.

[22] *Ibid.*

[23] Debbie Collier *Workplace Privacy in the Cyber Age* http://www.general.rau.ac.za/infosoci/www2002/Full-Papers/Colliers%20D/Colliers-Workplace Privacy.

Paul Esselaar[24] states that "privacy is a difficult area in law, too little knowledge of your employees' activities exposes you financially, and too much intrusion alienates your employee".[25] Ryk Meiring[26] expresses the view that "interception of work-based communications is fraught with pitfalls for the employer".[27] The principles illustrated above assert the significance of the need for the protection of the right to privacy.

Section 22 provides that:

> Every citizen has the right to choose their trade, occupation or profession freely. The practice of a trade, occupation or profession may be regulated by law.

The construction of this provision implies that an employer has a right to trade freely by ensuring that there is increased productivity. This is measured by the quality and quantity of the work produced by the employees. One of the pertinent methods of monitoring employee's productivity is through intercepting the latter's electronic communications. This right must be balanced with the right to privacy taking due regard the provisions of section 36 of the Constitution.

This balance is discussed more fully later in chapter four.

Section 23 provides that:

> Everyone has the right to fair labour practices.

---

[24] Paul Esselaar 2005, *Interception of communications* http://www.ghostdigest.co.za/A-784html.

[25] *Ibid.*

[26] Ryk Meiring 2005, Advisory *13: Interception of Private Communications in the Workplace* http://www.ispa.org.za.

[27] *Ibid.*

The application of this section in the employment law context is achieved by ensuring that employers do not select certain employees whose electronic communications should be monitored. In other words, the monitoring of employee's electronic communications must be done to all employees in the work place, thus consistently. The consistent interception would in my mind be regarded as fair labour practice. Section 36 of the 1996 Constitution provides that the Bill of Rights may be limited by the law of general application if the limitation is reasonable and justifiable in an open and democratic society.

Debbie Collier [28] indicates that the right to privacy is classified as one of the values of human dignity and it is subject to be limited. Furthermore, the protection of the right in question would be sought, if employees have a reasonable expectation of the right to privacy at the workplace. Collier[29] argues that employees spend more hours at work than at home, thus employees have reasonable expectation of the protection of the right to privacy at work. This illustrates that employers cannot just intercept employees' electronic communication without conforming to the provisions of RICA.The application of the provisions of section 36 in relation to this paper is crucial because section 4, 5 and 6 of RICA must be construed to determine whether same satisfies the limitation clause that is provided in section 36 of the Constitution. This assessment is done later in chapter four.

Section 39 of the 1996 Constitution confers powers on the courts to promote the spirit, purport and object of the Bill of Rights. Moreover, the courts are required to consider international law and may consider foreign law. The application of this section in this dissertation is equally important in the construction of the provisions of sections 4, 5 and 6 of RICA, in light of balancing the employee's right to privacy and the employer's right to monitor the latter's electronic communications pursuant to RICA. The application of this section is illustrated later in chapter four.

[28] *Ibid.*

[29] *Ibid.*

6. How do our courts protect the right to privacy?

In *Goosen v Caroline's Frozen Yoghurt Parlour Pty Ltd / Tru Food & Dairy Products Pty Ltd*[30] the applicant recorded telephone conversations between the employer's witness at the disciplinary inquiry and the chairperson of the inquiry, without their knowledge. The applicant was subsequently dismissed after the inquiry. Surprisingly, the employer argued that its right to privacy had been infringed by the recording of the conversation, without the employer's consent or knowledge. Further, the recording according to the employer was conducted unlawfully. The court concluded that the interception of the communication was indeed an infringement of the employers' right to privacy pursuant to the provisions of section 13 of the Interim Constitution. This case denotes the affirmation of the recognition and the protection of the right to privacy, but at the same time, it illustrates that this right is subject to the limitation clause test and this limitation would depend on the merits of the case.

In *Bernstein v Bester NO*[31], Ackerman J considered whether there had been an infringement of the right to privacy or not. Ackerman J applied and considered international law and held that the test that determines the infringement of the right to privacy is the principle of the *boni mores*. Ackerman J further found that the interception of the communication in the circumstances was one of the examples of the wrongful intrusion. In addition, Ackerman J observed that "an integrated approach to the interpretation of the right to privacy should be adopted: broad concept of privacy; extending beyond the individual's personal realm; privacy is acknowledged in the truly personal realm, but as soon as a person moves into communal relations and activities, such as business and social interaction, the scope of personal space shrinks accordingly".[32] This judgment shows that an employee's right to privacy may be diminished the minute he/she steps out of her own house or property.

[30] 1995 4 LCD 152 (IC).

[31] 1996 2 SA 751 (CC).

[32] *Ibid.*

In *Mistry v Interim National Medical and Dental Council of South Africa*[33] Sachs J considered the likelihood of an infringement of the right to privacy in relation to the searches conducted pursuant to the provisions of section 28(1) of the Medicines and Related Substances Control Act 101 of 1965. Sachs J found that such searches intruded on the right to privacy and thus, "amounted to an intrusion into a person's inner sanctum".[34] This section permitted the Council to order inspections on the premises of private practitioners without obtaining search warrants. These judgments illustrate that the courts do not readily find for employees, if the protection of the right to privacy sought relates to the infringement of the right to privacy in the workplace. The nature of the right to privacy in an employment law context to my mind is only to the extent that the employee in question has a reasonable expectation to privacy. This is determined by the circumstances upon which the right to privacy has been limited.

The Constitutional Court has also considered the protection of the right to privacy in *Janse van Rensburg v Minister van Handel en Nywerheid*[35] and in *President of the Republic of South Africa v South African Rugby Football Union*[36]. In both cases the Constitutional Court illustrated the significance of the limitation of the right to privacy, when the circumstances call for such limitation. The infringement of the right to privacy in relation to the employment law context was illustrated by the court in *S v Dube*[37]. McCall J had to consider whether the provisions of section 2(1)(b) of the IMP Act 127 of 1992 were contravened or not. In this case briefly, Toyota employed private investigators to investigate theft of parts of motor vehicles. The employees in question were not aware that their meeting was being recorded. They argued that their right to privacy was infringed by such recording. Therefore, evidence obtained by such recording should not be admitted as such.

[33] 1998 4 SA 1127 (CC).

[34] *Ibid.*

[35] 2001 1 SA 29 (CC).

[36] President of the Republic of South Africa v South African Rugby Football Union 2000 1 SA 1104 (SCA).

[37] 2000 2 SA 583 (N).

McCall J considered whether the employees in question had a legitimate expectation to privacy or not. In applying this principle, McCall J took into consideration the scope of the prohibition during the process of intercepting confidential information. McCall J concluded that "confidential information was defined by the same act, as meaning information upon which law conferred attribute of confidentiality, conversation during, which information regarding proposed participation in theft relayed was not regarded as having attributed to confidentiality".[38]
In addition, by participating in an unlawful activity, the employees in question waived their right to claim legitimate expectation to privacy. Consequently, the employees in question could not be protected in law by the application of the principle of legitimate expectation. McCall J reinforced the principle set out by Cameron J that the limitation of the right to privacy can be limited when the circumstances calls upon such limitation. This principle articulates that if the court had to enforce the protection of the right to privacy in the circumstances of this case, it would be to apply "an inappropriate extravagant notion of privacy."[39] This case illustrates the justification of limiting the right in question if employees are involved in unlawful activities that could have serious repercussion on the interest of the employer.

I embrace McCall J's judgment because an employee who is involved in corruption or any other criminal activity, during official working hours, and uses electronic facilities that are provided by an employer, cannot claim to have a legitimate expectation of the right to privacy. The monitoring of such employee's electronic communications with or without consent or knowledge would be justified pursuant to section 36 of the Constitution.

In *Tape Wine Trading CC v Cape Classic Wines (Western Cape) CC*[40], Prisman AJ had to determine whether or not the recording of telephone conversation of the employee in question, without his consent and knowledge was a contravention of the provisions of the IMP Act. In this case, an application was made to the court to strike out evidence obtained against the employee by the recording of the latter's telephone conversation. It was argued that such recording impinged on the employee's constitutional right to privacy.

[38] *Ibid.*

[39] *Ibid.*

[40] 1992 4 SA 194 (C).

Prisman AJ concluded that "participant electronic surveillance did not breach the provisions of the IMP Act. The use of traps in regard to the participant electronic surveillance did not infringe on any constitutional right."[41] Prisman AJ thus, refused to grant the application sought by the respondent. This case again, illustrates the limitation of the right to privacy when circumstances call for such limitation.

In *Protea Technology Ltd v Wainer*,[42] Heher J had to determine whether or not the monitoring of the first respondent's telephone conversation at his office was in contravention of the IMP Act and infringed on his right to privacy. In *casu* an employer placed a device on the first respondent's telephone at his office, without his consent and knowledge. The employer further placed another device at the first respondent's office after same discovered that the first respondent was using his cell phone to circumvent the possibility of intercepting his conversation by his employer.

Heher J balanced the two competing rights by considering the provisions of section 36 of the Constitution. Heher J reinforced the principle set out in *Case v Minister of Safety and Security: Curtis v Minister of Safety and Security*[43], that the right to privacy is not absolute; it can be limited if the limitation is based on the law of general application and the circumstances of the case. Furthermore, Heher J described the scope of the right to privacy as "the scope of the right to privacy extends only to those aspects in regard to which a legitimate expectation of privacy can be harboured".[44] Heher J furthermore considered the relationship between the applicant and the first respondent and held that the first respondent had been employed in the position of trust; therefore he was accountable to the applicant.

[41] *Ibid.*

[42] 1997 9 BCLR 1225 (W).

[43] Case and Another v Minister of Safety and Security 1996: Curtis v Minister of Safety and Security 1996 3 SA 617 (CC).

[44] *Ibid.*

In addition, the telephone calls made by the first respondent were made during official working hours and in the premises of the applicant. That according Heher J justified the interception of the first respondent's telephone conversation, without his consent or knowledge. Heher J however illustrated that the nature of the relationship between the applicant and the first respondent, was such that the employee was entitled to receive private telephone calls at the applicant's business premises. The first respondent had a legitimate expectation of the right to privacy regardless of the fact that the employee was accountable to the applicant. The first respondent could therefore not be compelled to disclose to the applicant the substance of his calls.

In balancing the competing rights in this case, Heher J concluded that the applicant had a right to the protection of free economic activity under the Interim Constitution. Thus, the applicant had an interest "in the substance and the manner in which the first respondent conducted himself by words or gesture in carrying on his business."[45] This according to Heher J justified the limitation of the first respondent's right to privacy. Heher J further asserted the importance of affirming the discretion conferred on the courts when deciding on issues relating to the admissibility of the evidence presented to the court. This discretion according to Heher J should be exercised judicially not arbitrarily. The first respondent intentionally promoted his business interests at the expense of the applicant.

There was thus an element of undermining the applicant's business interest hence the limitation to the first respondent's right to privacy was necessary. As can be seen, this judgment is pivotal to this paper, because it illustrates that the intercepting or monitoring the employee's electronic communications without his/her knowledge or consent might be justified.

[45] *Ibid.*

I am of the view that Heher J correctly decided in this judgment, insofar as it relates to the conduct of the employee. With great respect to Heher J, however, the conduct of the employer, in my view, could be regarded as an infringement of the employee's right to privacy because, in my view, it amounted to some level of harassment. Although there is authority that employees need not be aware of the rules and policies regarding the interception of their electronic communications, the employer in this case, should to my mind, have advised the employee of the interception of his electronic communications, the moment the employer established that he was avoiding the interception by using his cell phone. That to me would have prevented the invasion of the employee in question's right to privacy without his consent or knowledge. Bawa[46] illustrates that there is likelihood that during the application of the provisions of RICA, employers might abuse the employees' right to privacy.

In *Moonsamy v The Mailhouse*,[47] Commissioner Van Dokkum had to consider whether or not there had been an infringement of the employee's right to privacy, by the interception of the latter's telephone conversation. In a disciplinary inquiry conducted by the employer, evidence that was obtained by the recording of the employee's telephone conversation at his office was presented. Commissioner Van Dokkum first considered whether or not he had jurisdiction to adjudicate the matter, as the issue of privacy falls under the ambit of constitutional matters, and this was answered in the affirmative.

Commissioner Van Dokkum found that the interception of the employee's telephone conversation was indeed a contravention of the provisions of the IMP Act as well as an infringement of the latter's right to privacy in accordance with section 14 of the Constitution. Commissioner Van Dokkum applied the limitation clause test to determine whether the limitation was justified or not pursuant to section 36 of the Constitution. This was achieved by considering the principles set out by the court in the *Goosen* and *Protea Technology* judgments, together with section 8 of the Canadian Charter.

---

[46] Nazreen Bawa (2006), *The Regulation of Interception of Communications and Provision of Communication-Related Information Act: Telecommunications Law in South Africa* 298.

[47] (1999) 20 *ILJ* 464 (CCMA).

Commissioner Van Dokkum held that in the circumstances the employee had a legitimate expectation of the right to privacy in relation to the telephone calls he made at the workplace. In addition, the employer had other means of obtaining evidence against the employee. This according Commissioner Van Dokkum did not justify the limitation of the employee's right to privacy. Thus, the limitation in the circumstances did not pass the limitation clause test pursuant to the provision of section 36 o the Constitution. This case does not bind the courts but it has a persuasive effect in the construction of the provisions of RICA, in an attempt to determine whether same satisfies the provisions of section 36 of the Constitution or not. These principles in my view are correctly applied and considered by Commissioner Van Dokkum because they show the significance of protecting the employees' right to privacy in the workplace.

Recently, in *NM v Smith*[48] the Constitutional Court had to consider whether or not there had been an infringement of the right to privacy of the three HIV positive applicants, whose names were published in the Patricia De Lille's biography by New Africa Books (Pty) Ltd, without their consent. Madala J concluded that everyone has a reasonable expectation of privacy. This right can only be limited if there is a need for such limitation. Madala J held that in the circumstances the limitation of the three applicants' right to privacy was not justified. Madala J suggested that the first respondent was required to obtain consent from the three applicants before publishing the biography without the latter's consent. In addition, the first respondent could have avoided using the names of the applicants by using pseudonyms. The publication of the applicants' HIV status was therefore an infringement of the applicants' right to privacy.

Madala J made another submission that the first respondent knew that she had not obtained the necessary express consent from the applicants, but nevertheless she still continued to publish their HIV status, without their consent. Having said that, Madala J further submitted that the first respondent failed to take steps to find out whether an unlimited consent had been obtained or not. Sachs J concurred with Madala J in so far as the issue of using pseudonyms was concerned.

[48] NM and Others v Smith and Others (CC) (CCT69/05) 2007 ZA CC6 (4 April 2007).

Sachs J went further and concluded that the information relating to the applicants' HIV status was sensitive; therefore the first respondent should have ensured that "there were no stones unturned." [49]

O'Regan J dissenting, affirmed the significance of protecting the right to privacy. O'Regan J clustered the protection of the right to privacy with the right to liberty and dignity "as the key constitutional rights which construct the understanding of what it means to be a human being."[50] Another relevant submission made by O'Regan J is that, if personal information is regarded as intimate, it is pertinent that the right to privacy must be protected. Therefore, the decision to disclose such information must be made by the person concerned. O'Regan J also pointed out that the protection of the right in question is however not absolute, as it can be limited based on the circumstances of the case.

The respondent had assumed that the necessary consent had been obtained because the applicants' name and their HIV status had already been published in the Strauss Report. The important issue in this judgment in relation to this paper is whether or not written or implied consent can be regarded as a legitimate reason to limit the employees' right to privacy. The exposition to this issue is provided later in chapter four. This judgment has been criticized by J Steinberg. Steinberg utters that "something went wrong in this case. The fact that two judges dissented from majority opinion is unremarkable in itself; disagreement about constitutional interpretation is what the court's work is about. Under common law violation of privacy because of negligence is not liable"[51]

I support the majority judgment because same does not only enforce the right to privacy but it also affirms the principle that where a person does not give consent whether expressed or implied, his or her right to privacy should be protected.

---

[49] *Ibid.*

[50] *Ibid.*

[51] Jonny Steinberg 2007, Generous judgment instils stigma [Online] Available http://www.businessday.co.za/PrintFriendly.aspx?ID=BD4A445289

This judgment is pertinent to the construction of section 5 and 6 of RICA and these sections are discussed later in chapter four. The other important issue this judgment raises is whether the provisions of RICA, by permitting employers to intercept or monitor employees' electronic communications, if same consents to such interception, satisfies the limitation clause test in section 36 of the Constitution.

Moreover, one can argue that employment contracts that are concluded between employers and employees, where there are clauses that permit the monitoring of the electronic communications, do not necessarily mean that such employees waive their right to privacy. Another argument that can be advanced is whether or not our courts should measure contracts of employment against the compelling public interest. What happens in circumstances where there are no provisions in the employment contracts concluded, whether orally or in writing, and there are no policies in place that permit such interception? Is there an infringement of the employee's right to privacy in such circumstances? The answer in my view is in the affirmative but our courts have followed a different approach. This is explored later in chapter four.

In *Magajane v Chairperson North West Gambling Board*[52], the Constitutional Court had to consider whether or not there had been an infringement of the right to privacy in relation to inspections conducted in terms of legislation without a warrant in order to obtain evidence. The court applied the principles set out in the *Bernstein* judgment and concluded that "the right to privacy extends beyond the inner sanctum of the home".[53] The Constitutional Court applied the proportionality test and held that the application of this test would be achieved by considering the breath of the legislation together with the factors set out in section 36 of the Constitution. The Constitutional Court found that "the expectation of privacy will be more attenuated the more the business is public, closely regulated and potentially hazardous to the public. Legislation may not be so broad so as to have the real potential to reach into private homes".[54]

[52] 2006 5 SA 250 (CC); 2006 2 SACR 477 (CC).

[53] *Ibid.*

[54] *Ibid.*

These principles illustrate that the courts should apply the proportionality test to determine whether or not the conduct of an employer infringes on an employee's right to privacy when intercepting or monitoring the latter's electronic communications.

In *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd*[55], Langa DP concluded that:

> "The right to privacy, however, does not relate solely to the individual within his or her intimate space. Thus, when people are in their offices, in their cars or on mobile telephones, they still retain a right to be left alone by the state unless certain conditions are satisfied".[56]

Langa DP further reinforced the principle that has recently been articulated by the Constitutional Court in the *NM v Smith* judgment by affirming that the decision to disclose personal information must only be made by the person who would be affected by such disclosure and everyone else should respect his/her decision. The principles set out above should find application via the provisions of section 39(2) of the Bill of Rights. It is debatable whether the principles set out in this judgment imply that employees still retain their right to privacy, when they are in their offices and RICA is regarded as one of certain condition upon which this right may be limited. Chapter 4 will attempt to provide a solution to this question.

In *S v Jordan*[57], Chaskalson CJ affirmed the principle of the limitation of the right to privacy. The court balanced the right to privacy against prohibition on prostitution which at the time was regarded as unlawful. The court refused to accept the argument that those who engaged in commercial sex could claim a right to privacy. In *Financial Mail (Pty) Ltd v Sage Holdings Ltd*[58], Corbett CJ had to decide whether or not the placing of a device in the first respondents' telephone invaded on their right to privacy.

---

[55] *In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smith NO and others* 2001 1 SA 545 (CC).

[56] *Ibid.*

[57] 2002 6 SA 642 (CC).

[58] 1993 2 SA 451 (A).

The court held that the tapping of the first respondents' telephone was indeed an invasion of the first respondents' directors' right to privacy. The court found that the invasion of privacy may take two forms, "the first is the unlawful intrusion upon the privacy of another and the unlawful publication of private facts about a person". [59] The above judgments illustrate the importance of the recognition and the protection of the right to privacy by our courts. At the same time, the judgments also denote that our courts consider the circumstances of each case, before enforcing the protection of the right in question. In addition, more emphasis is put on having a legitimate expectation to privacy before one can claim the protection of the right to privacy. It would appear that when the courts in future, have to determine whether or not there has indeed been an infringement of an employee's right to privacy, when an employer monitors the latter's electronic communications, they would invoke the principles that have been applied in the above judgments. This would affirm the principle of judicial precedent.

7. **Interception and Monitoring Prohibition Act 127 of 1992**

In terms of the IMP Act, its object was:

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

The following definitions in section 1 of the above Act are important:

> **"monitor"** includes the recording of conversations or communications 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, device or equipment, to listen to or record any conversation or communication

Section 2(1) of the IMP Act provided for the prohibition of interception and monitoring.

---

[59] *Ibid.*

This section states that:

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

Section 8 of the IMP Act provided for offences and penalties to those who contravened the provisions of section 2(1) of this Act. The provisions of this Act have been tested by our courts in *S v Dube; Tape Wine Trading* and *Protea Technology* judgments as well as other judgments referred to in this paper. The question is whether the courts would apply the same principles in interpreting RICA, in light of the protection of the right to privacy that is now entrenched in the 1996 Constitution. The exposition to this issue is provided later in chapter four.

In *Lenco Holdings Ltd v Eckstein*[60], Hurt J had to consider whether or not there had been contravention of the provisions of the IMP Act. *In casu* briefly, the respondent's telephone conversation was recorded without consent. It was argued that the respondent was contravening a restraint of trade agreement hence the recording was necessary. The respondent argued that the evidence obtained by such recording was unlawful because the recording was done without the latter's consent or knowledge. Hurt J reinforced the principle that the courts have the discretion to decide whether or not evidence should be admissible based on the circumstances of each case. This case shows that consent is required to intercept employees' electronic communication.

In *Waste Products Utilization (Pty) Ltd v Wilkes*[61] Lewis J had to determine whether there had been a contravention of the IMP Act or not. Lewis J held that the interception of the communication in the circumstances was a contravention of the IMP Act as well as an infringement of the right to privacy. The rationale behind this finding was based on the fact that it had been admitted that the recording had been unlawfully executed.

---

[60] 1996 2 SA 693 (N).

[61] 2003 2 SA 515 (W).

In *S v Kidson*[62] the court had to consider whether there had been an infringement of the right to privacy or not. *In casu* the accused had argued that the evidence obtained by the tape recording of the meeting between him and the third party by the police was in contravention of the IMP Act as well as an infringement of the right to privacy. The court found that the recording in the circumstances was participant monitoring therefore not prohibited. These judgments illustrate the approach that had been followed by our courts in determining whether or not there had been an infringement of the right to privacy in the context of the IMP Act. They also illustrate the limitation of the right to privacy when the circumstances of the case call for such limitation.

8. **RICA**

Nazreen Bawa[63] describes the likelihood of an infringement of the right to privacy pursuant to the provisions of RICA as including interception of the employee's emails, both at the workplace and in private life. Bawa further argues that the employee's right is not protected by RICA. In addition, there is a risk that employers might abuse the employee's right to privacy in the process of complying with the provisions of RICA. It is important to begin with one of the most relevant objectives of RICA that is pertinent to the protection of the right to privacy. Thus, same aims at regulating the interception of certain communications.

The definitions of RICA that are pertinent to the paper are:

> **"direct communication"** means an-
>
> > (a) oral communication, other than an indirect communication, between two or more persons which occurs in the immediate presence of all the persons participating in that communication; or
> >
> > (b) utterance by a person who is participating in an indirect communication, if the utterance is audible to another person who, at the time the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication;

[62] 1999 1 SACR 338 (W).

[63] *Ibid.*

"indirect communication" means the transfer of information, including a message or any part of a message, whether-

(a) in the form of-

(i) speech, music or other sounds;
(ii) data;
(iii) text;
(iv) visual images, whether animated or not;
(v) signals; or
(vi) radio frequency spectrum; or

(b) in any other form or in any combination of forms, that is transmitted in whole or in part by means of a postal service or a telecommunication system;

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

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

and **"interception"** has a corresponding meaning;

"interception device" means 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, but does not include-

(a) any instrument, device, equipment or apparatus, or any component thereof-

(i) furnished to the customer by a telecommunication service provider in the ordinary course of his or her business and being used by the customer in the ordinary course of his or her business;

(ii) furnished by such customer for connection to the facilities of such telecommunication service and used in the ordinary course of his or her business; or

(iii) being used by a telecommunication service provider in the ordinary course of his or her business; or

(b) a hearing aid or similar device being used to correct below normal hearing to not better than normal, and a reference to an **"interception device"** includes, where applicable, a reference to a **"monitoring device"**;

"monitor" includes to listen to or record communications by means of a monitoring device, and "monitoring" has a corresponding meaning;

"monitoring device" means 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;

"party to the communication", for purposes of-

(a) section 4, means, in the case of-

(i) a direct communication, any person-

(aa) participating in such direct communication or to whom such direct communication is directed; or

(bb) in whose immediate presence such direct communication occurs and is audible to the person concerned, regardless of whether or not the direct communication is specifically directed to him or her; or

(ii) an indirect communication-

(aa) the sender or the recipient or intended recipient of such indirect communication;

(bb) if it is intended by the sender of an indirect communication that such indirect communication be received by more than one person, any of those recipients; or

(cc) any other person who, at the time of the occurrence of the indirect communication, is in the immediate presence of the sender or the recipient or intended recipient of that indirect communication; and

(b) section 5, means, in the case of-

(i) a direct communication, any person participating in such direct communication or to whom such direct communication is directed; or

(ii) an indirect communication-

(aa) the sender or the recipient or intended recipient of such indirect communication; or

(bb) if it is intended by the sender of an indirect communication that such indirect communication be received by more than one person, any of those recipients;

Section 2 of RICA provides that:

> Subject to this Act, 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

Section 4 of RICA provides for interception of communication by a party to such communication.

Section 5 of RICA provides employers may intercept employees' electronic communication if such employees consent to such interception.This section provides that:

> (1) 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.

Section 5(1) is pertinent because it denotes the likelihood of an invasion of an employee's right to privacy by an employer, when the latter monitors employees' electronic communications.

Section 6(1) of RICA discussed *infra* addresses the issue of consent to a certain extent, as RICA requires the system controller to take all reasonable steps to inform the user of a telecommunication system that indirect communication may be intercepted or the interception may be permitted by the expressed or implied consent. Most academic writers embrace the notion that consent in the employment law context is incorporated in employment contracts or employer's policies. The courts have concluded that there is no infringement of the right to privacy where one party consents to the interception. It had been found by our courts and the CCMA that an employee may not claim a protection of the right to privacy, if there are policies in place.

This is illustrated in *Toker Bros Pty Ltd and Keyser*[64] where an employee was allegedly charged with abusing the employers' internet. Commissioner Van Niekerk 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. According to Commissioner Van Niekerk, the employee could have used common sense thus "the employee could have reasonably be expected to know that they should not abuse employers electronic facilities. If this happens, employees are expected to know that abusing employers facilities would in most cases result in disciplinary proceedings against them. In addition, in applying the reasonableness test, Commissioner Van Niekerk concluded that rules do not necessary have to be made known to employees, employees at times must use common sense.

Section 6 of RICA provides that employers may intercept employees' indirect communication if this is done in the course of carrying on of any business. In addition, this section requires employers to take reasonable steps to notify employees that their electronic communication would be intercepted or monitored.

[64] 2005 26 ILJ 1366 CCMA.

The following questions are relevant in the construction of the provisions of section 6: (a) what is regarded as ordinary course of business? (b) What is meant by section 6(1)(a) to (c)? What is meant by confidential voice-telephony? (c) What are reasonable efforts? In *Sage Holding Ltd v Financial Mail (Pty) Ltd*[65], the court found that "the right to carry on business included the right to regard confidential oral or written communications of directors and employees sacrosanct. Furthermore, in appropriate circumstances it would be entitled to enforce the confidentiality of such oral or written communications".[66] This decision was however overturned by the Supreme Court of Appeal.

In the *Hyundai Motors*[67] judgment, the Constitutional Court concluded that:

> "The right to privacy guaranteed in s 14 of the Constitution, did not relate solely to the individual within his or her intimate space. When persons moved beyond this established 'intimate core', they still retained a right to privacy in the social capacities in which they acted. Thus, when people were in their offices, in their cars or on mobile telephones, they still retained a right to be left alone by the State unless certain conditions were satisfied.

The question is, can the courts construe the course of carrying on business in light of what was said in these judgments? This question is answered later in chapter four.

Section 49 makes provisions for unlawful interception of communication. It states that:

> (1) Any person who intentionally intercepts or attempts to intercept, or authorises or procures 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, is guilty of an offence.
> (2) Subsection (1) does not apply to the-
> (a) interception of a communication as contemplated in section 3, 4, 5,6,7,8 and 9; or
> (b) monitoring of a signal or radio frequency spectrum as contemplated in section 10 and 11.

Section 51 provides that it is an offence to contravene the provisions of section 6(2) of RICA.

---

[65] 1991 2 SA 117 (W).

[66] *Ibid.*

[67] *Ibid.*

Carl Mischke[68] expresses the view that employers ought to accept the reality that employees' right to privacy at the workplace must be respected. Furthermore, employees do not waive their right to privacy by virtue of being in the employers' premises. This to my mind is correct because employees have reasonable expectation to privacy at the workplace. Mischke further asserts that the employer may protect the employees' right to privacy by obtaining consent from the latter before intercepting their electronic communications. This is pertinent because RICA has not yet been tested by our courts notwithstanding the academic debate that has been created by its promulgation. The constitutionality of the provisions of RICA in light of the employment law context is discussed in detail in chapter four.

9. **EC Act**

The only pertinent provision in this Act, which relates to the paper in my view, is the definition of electronic communications and this is provided in section 1 of the Act. The said section provides that:

> **"electronic communications"** means the emission, transmission or reception of information, including without limitation, voice, sound, data, text, video, animation, visual images, moving images and pictures, signals or a combination thereof by means of magnetism, radio or other electromagnetic waves, optical, electro-magnetic systems or any agency of a like nature, whether with or without the aid of tangible conduct, but does not include content service.

The construction of this definition means that electronic communications includes telephone and video recording; emails and internet use when applying provisions of RICA.

[68] Carl Mischke *Workplace privacy, email interception and the Law Contemporary Labour Law* Vol 12 No. 8 2003.

10. **ECT Act**

The following definitions are relevant for the purpose of this paper. These definitions are provided in section 1 of this Act:

"data" means electronic representations of information in any form;
"data controller" means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject;
"data message" means data generated, sent, received or stored by electronic means and includes:

(a) voice, where the voice is used in an automated transaction; and
(b) a stored record;

"data subject" means 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 communication" means a communication by means of data messages;

"e-mail" means electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication;

"personal information" means information about an identifiable individual, including, but not limited to:

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual;
(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
(c) any identifying number, symbol, or other particular assigned to the individual;
(d) the address, fingerprints or blood type of the individual;
(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;
(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the individual;

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years;

Section 2 of the Act provides that:

> One of the objects of this act is to enable and facilitate electronic communications and transactions in the public interest…

Section 50 provides for protection of personal information. This section provides for the scope of the protection and states that:

> (1) This Chapter only applies to personal information that has been obtained through electronic transactions.
>
> (2) A data controller may voluntarily subscribe to the principles outlined in section 51 by recording such fact in any agreement with a data subject.
>
> (3) A data controller must subscribe to all the principles outlined in section 51 and not merely to parts thereof.
>
> (4) The rights and obligations of the parties in respect of the breach of the principles outlined in section 51 are governed by the terms of any agreement between them.

Section 51 sets out principles that ought to be followed in intercepting electronic communications. This section provides that:

> (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.

(5) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.

(6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorised to do so in writing by the data subject.

(7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.

(8) The data controller must delete or destroy all personal information which has become obsolete.

(9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party.

The provisions of both the EC and the ECT Act are construed later in chapter four to determine whether or not employers infringe on an employee's right to privacy when monitoring the latter's electronic communications.

11. **The Protection of Personal Information Bill ("The Bill")**

The Bill seeks to protect personal information and enforce the protection of the right to privacy pursuant to the provisions of section 14 of the Constitution. The object of this Bill is illustrated as:

> To give effect to the constitutional right to privacy by safeguarding a person's personal information when processed by public and private bodies; in a manner which balances that right with any other rights, including the right in the Bill of rights in Chapter 2 of the Constitution, particularly the right to access to information: subject to justifiable limitations, including but not limited to effective efficient and good governance and the free flow of personal information particularly transborder transfers.

The Bill defines processing as:

> Any operation or any set of operations concerning personal information, including in any case the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form merging, linking as well as blocking erasure or destruction of information.

The provisions of chapter three of the Bill are akin to the provisions of section 51 of the ECT Act, therefore would not be repeated. The Bill further provides that:

> Personal information may only be processed where, given the purpose(s) for which it is collected or subsequently processed, it is adequate, relevant and not excessive.

In addition, the Bill provides that:

> Personal information may only be processed where the data subject, has given consent for the processing; or processing is necessary for the performance of a contract or agreement to which the data subject is party or for actions to be carried out at the request of the data subject, and which are necessary for the conclusion or implementation of a contract; processing is necessary in order to comply with a legal obligation to which the responsible party is subject … or processing is necessary for upholding the legitimate interests of the responsible party or a third party to whom the information is supplied.

Section 14(1) of the Bill provides for further processing not incompatible with the purpose of collection. The said section provides that:

> 14(1) Personal information must not be further processed in a way incompatible with a purpose for which it has been collected in terms of principle 2.
> 14(2) For the purpose of assessing whether processing is incompatible, as referred to under subsection (1), the responsible party must take account of the following –
> (a) the relationship between the purpose of the intended further processing and the purpose for which the information has been obtained;
> (b) the nature of the information concerned;
> (c)the consequences of the intended further processing for the data subject;
> (d) the manner in which the information has been obtained; and
> (e) any contractual rights and obligations existing between the parties.

Section 14(2) provides that:

> Further processing of personal information must not be regarded as incompatible as referred in subsection one, if the processing of the information for that other purpose, is authorized by the data subject or the information is publicly available.

Section 14(3) provides that:

> Steps referred to above must be taken before the information is collected or, if that is not reasonably practicable as soon as reasonably practicable after the information is collected.

Section 14(4) provides that:

> A responsible party is not required to take steps referred to in subsection 2 of this section in relation to the collection of information from a data subject, if a responsible party has previously taken those steps in relation to the collection from that data subject of the same information or information of the same kind.

Section 16(2) provides that:

> Where a responsible party collects personal information about a data subject, *the responsible party must take such steps as are, in the circumstances, reasonably practicable to ensure that the data subject is aware of the fact that the information is being collected* (my emphasis); the name and address of the responsibly party; whether or not the supply of the information by that data subject is voluntary or mandatory and the consequences of failure to reply; and where the collection of information is authorized or required under any law, the particular law to which the collection is subject.

Section 63 of the Bill provides that:

> An interference with the protection of personal information of a person in relation to that person constitutes a breach of privacy principle.

The analysis of the provisions of the Bill brings a deduction that the legislature indeed recognizes the right to privacy as one of the most fundamental rights pursuant to section 14 of the 1996 Constitution. The above provisions of the Bill further evince that the processing of information is permitted, if the data subject (employees are regarded as data subjects) consents to such processing, or if it is necessary to process such information but even then, the data subject must be aware of such processing. The application of the provisions of the Bill implies that employers may only intercept or monitor employee's electronic communications, if employees consent to such interception or if they are aware of the interception where they have not consented to the latter. These provisions of the Bill are akin to the provision of section 5 and 6 of RICA, as they also require employers to take reasonable steps to inform employees of the interception of their electronic communications.

The Bill also provides guidelines in section 14 that ought to be considered to determine whether there has indeed been an infringement of the employee's right to privacy or not. Namely, the relationship between the purpose of intercepting the employee's electronic communications and the consequences of the interception, which in most cases result in disciplinary proceedings being instituted against those employees, who are found to be abusing the employers' electronic communications. There is no doubt that if this Bill becomes law, it would to a certain extent protect the employees' right to privacy. The Bill however fails to define or describe reasonably practical steps that responsible parties are required to take.

12. **LRA**

The heart of this legislation is to regulate the relationship between an employer and an employee. The relevant provisions of this Act that are pertinent to this paper are discussed later in chapter four. The LRA seeks to enforce the provisions of the Bill of Rights because this Act requires the courts to interpret its provision in line with the provisions of the 1996 Constitution.

This appears to enforce the protection of the right to privacy pursuant to section 14 of the Constitution by ensuring that in an employment relationship context, employers do conform to the provisions of the 1996 Constitution.

Item 7 of Schedule 8 of the LRA are discussed in detail later. These items provide principles that determine whether an employee has broken any rule or not. Employers may only institute disciplinary proceedings against employees, if the latter breaks a reasonable or existing rule, which he/she has been made aware of or should reasonably been made aware of. Thus, an employer may only institute disciplinary proceedings against an employee who for example, abuses the use of internet or accesses child phonography from employers' computer, if such an employee is aware of the prohibition of the internet abuse or ought to reasonably be aware of such prohibition. In the case of accessing child phonography it is well known that accessing child phonography is unlawful. In such instances employees ought to reasonable know that accessing child phonograph could result in disciplinary proceedings being instituted against them. Such employees therefore cannot claim to have a legitimate expectation to privacy. The meticulous exposition of the provisions of the LRA is illustrated later in chapters four.

13. **Principles of interpreting statutes**

Professor de Ville[69] utters that the first principle that ought to be applied by the courts in interpreting any statutes, is the application of the golden rule principle. This principle according to Professor de Ville means that statutes must be interpreted according to their ordinary meaning. If however the statute is ambiguous, the contextual interpretation approach must be invoked.

Professor de Ville describes the contextual approach as meaning that the courts must take due regard; the title, the preamble, the object, the heading, the history of the legislation, the language of the statute and the intention of the legislature, when interpreting statutes.

[69] JR de Ville, *Constitutional & Statutory Interpretation* (2000) p94.

For the purpose of constructing the provisions of RICA to determine whether same infringes on the employee's right to privacy or not, the provisions of section 39 of the Constitution should also be invoked and these are explored later in chapter four. The discussion would include the application of the principles of purposive approach as this approach is important in a constitutional context.

14. **Conclusion**

The analysis of the privacy polemic in light of the provisions of RICA, denotes that same has not only created an academic debate, but it also calls upon the judiciary to consider the above principles, to determine whether or not there has indeed been an infringement of the right to privacy, when employers monitor employees' electronic communications. It is explicit that the right to privacy has been recognized and protected in terms of the common law, the 1993 and 1996 Constitutions as well as by our courts, as is apparent in the judgments discussed above. The above discussion shows that the right to privacy is not absolute as such right is subject to the limitation clause provided in section 36 of the Constitution and the limitation should be based on the law of general application.

The courts express the view that an employee must first have a legitimate expectation to a right to privacy, before he or she may claim such protection. Taking due regard the provisions of section 5 of RICA, it can be deduced that, if employees have consented to the interception of their electronic communications, they cannot claim to have a legitimate expectation of the right to privacy. It is submitted that consent whether express or implied should not be the only means of ensuring that employees are aware of the interception or monitoring of their electronic communications by employers. Other means of informing employees about the interception of their electronic communications are available to employers. Thus, drafting policies that are explicit enough to make employees aware that their right to privacy is waived, and employers must ensure that employees read and sign such policies as asserted by most writers. This would eliminate unnecessary arguments or litigation based on whether or not employees were aware of the existence of such policies.

It stands to reason, that Collier's view in so far as it relates to the amount of time that is spent by employees in the workplaces is correct and calls for some form of protection of their right to privacy. This is due to the fact that it is known that employees do engage in personal matters during official working hours. This often happens when employees' use employers' electronic facilities, namely telephones, emails or internet, to communicate with their financial institutions, friends and family members.

In addition, the *NM* judgment evinces the entrenched protection of the employees' right to privacy in relation to the issue of consent, which is a subject matter in section 5 of RICA. Other judgments that are discussed in this chapter are just as equally important to be considered in order to determine whether an employer infringes on an employee's right to privacy or not, when intercepting or monitoring the latter's electronic communications. These judgments are considered in the following chapters. The impact and the effect of the provisions of RICA in light of section 14 of the Constitution in an employment law context are also discussed later in chapter four. The next chapter considers international and foreign jurisdictions that are pertinent in the construction of the provisions of RICA.

CHAPTER THREE

15 Introduction

Connelly[70] argues that employees' computers are subject to employers' scrutiny with or without their consent or knowledge. International and foreign jurisprudence in this chapter is significant because same would be applied later in the construction of the provisions of RICA. The reason for such application is due to the fact that the provisions of RICA have not yet been tested by our courts. Section 39(1)(b) of the 1996 Constitution places an obligation on the courts to consider international law and it provides that the courts may consider foreign law when interpreting the Bill of Rights. This chapter begins by considering general international literature. This is followed by the discussion in the United Kingdom, United States of America, Canadian Law and Australian Law. Lastly, a brief synopsis of the pertinent principles of the international jurisprudence is later illustrated at the end of this chapter.

16 General Literature

Buys & Cronje[71] argue that the 1995 Directive (Directive 95/46/EC) regulates the interception of the electronic communications in the European Union under the notion of data protection. The principles set out in the Directive seek to protect the right to privacy in so far as the latter relates to the collection, storage; processing and how personal information should be used. In addition, the protection of the right to privacy is also enforced by the 1997 Telecommunications Directives. These however have been replaced by Directive on Privacy and Electronic Communications. This protection is illustrated in Article 1 of the said Directive. Article 1 provides that the member states must ensure that the right to privacy is protected when processing electronic communications.

---

[70] Nan Connelly (200),*Work computers not protected by privacy rule* [Online] Available http://www.usatoday.com/tech/nes/internetprivacy/2005-05-27-tech-privacy-x.htm.

[71] Buys & Cronje 2004 188.

It has been pointed out that Directive 95/46/EC was primarily concerned with the protection of data stored in databases and was only indirectly relevant to interception of communications. [72] The preamble includes that:

> Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

Article 1 provides that:

> In accordance with this directive, Member States shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.

Directive 1995 evidently put emphasis on the protection of the right to privacy in the process of intercepting electronic communications.

Directive 97/66/EC

Article 5 – of the 97 Directive provides that:

> Member States ensure via national regulations the confidentiality of communications by means of a public telecommunications network and public available telecommunications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorised.

This provision affirms the importance of the protection of the right to privacy where there is no consent given for such interception. Interception without consent would however be permitted if the latter is permitted by law.

---

[72] European Parliament (1999); *Development of Surveillance Technology and Risk of Abuse of Economic Information* [Online} Available. http://cryptome.org/dst-2.htm.

17. International Conventions

Article 8 of the European Convention of Human Rights provides that:

> (1) Everyone has the right to respect for his private life and correspondence.
> (2) There shall be no interference by a public authority with the exercise of this right except as far as is 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 or morals, or for the protection of the rights and freedom of others.

The provisions of Article 8 are akin to the provisions of section 36 of the 1996 Constitution.

Article 12 of the Universal Declaration of Human Rights provides that:

> No one shall be subjected to arbitrary interference with his privacy … or correspondence …everyone has the right to the protection of the law against such interference…

Article 12 emphasises the significance of protecting one's right to privacy.

Article 17 of the International Covenant on Civil and Political Rights provides that:

> No one shall be subjected to arbitrary or unlawful interference with his privacy… and that:
>
> Everyone has a right to the protection of the law against such interference…

The SALRC in the Discussion Paper 109 Project 124 illustrates that other International Conventions that seek to protect the right to privacy are: The United Convention on the Rights of the Child; United Nations Convention on Migrant Workers as well as American Declaration on Rights and Duties of Mankind. Article 7 of the Data Protection Convention provided that appropriate security measures be taken to ensure that personal data is protected against unauthorized access or dissemination. The United Kingdom has recognized the protection of the right to privacy in light of the interception of electronic communications regardless of the fact that the right in question had been limited when circumstances called upon such limitation.

18. United Kingdom

In the United Kingdom section 5 of the Wireless Telegraphy Act 1949 prohibits interception of electronic communications without consent. This principle was later enforced in the Interception of Communications Act of 1985. Further, section 1 of the Computer Misuse Act of 1990 makes it an offence to access information on a computer without employees' consent or knowledge.[73] The European Parliament discussion paper illustrate that the Data Protection Act of 1984 [this Act has been repealed by the Data Protection Act of 1998] protects natural person's right to privacy. This Act provides that electronic communications may be intercepted, if data subjects consent to such interception. The exception is when the interception is conducted in accordance with the legal obligation, namely protecting the secrecy of the state or to protect the business interests of the data controller. These exceptions however may not be carried out, if the interception would prejudice the data subject or natural person whose electronic communications is being processed or monitored.

18.1 The relevant provisions of the Data Protection Act of 1998

The following definitions of the Data Protection Act are pertinent to this paper.

> **"data"** means information which –
>
> (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;
>
> (b) is recorded with the intention that it should be processed by means of such equipment;
>
> (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or
>
> (d) does not fall within paragraph (a), (b) or (c) but form part of an accessible record as defined by section 68.
>
> "data controller" means subject to subsection 4, a person who (either alone or jointly or in common with other persons) determines the purpose for which and the manner in which any personal data are, or are to be processed;

[73] *Ibid*.

In the case of this paper, the data controller would be regarded as the employer because he/she decides the purpose and the manner of intercepting or monitoring employees' electronic communications. In most cases, employers intercept or monitor employees' electronic communication to monitor the performance of employees.

> "**data processor"** in relation to personal data, means any person (other than an employee of data controller) who processes the data on behalf of the data controller.
> "data subject" means an individual who is the subject of personal data.
> **"personal data"** means data which relate to a living individual who can be identified -
> (a) from those data; or
> (b) from those data and other information which is in the possession of, or is likely to come into possession of the data controller,
> and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
> "processing" in relation to information or data, means obtaining recording or holding the information or data or carrying out any operation or set of operations on the information or data including –
> (a) organization, adaptation or alteration of the information or data;
> (b) retrieval, consultation or use of the information or data;
> (c) disclosure of the information or data by transmission, dissemination or otherwise making available; or
> (d) alignment, combination, blocking, erasure or destruction of the information or data.
> "obtaining" or "recording" in relation to personal data, includes obtaining or recording the information to be contained in the data.

The construction of the above definition shows similarities between RICA; IMP Act and the Data Protection Act of 1998.

Section 7(1) of the same act provides that:

> Subject to the following provisions of this section and to sections 8 and 9, an individual is entitled-
> (a) to be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller,
> (b) if that is the case, to be given by the data controlled a description of –
> (i) The personal data of which that individual is the data subject;
> (ii) the purposes for which they are being or are to be processed; and

(iii) the recipient or classes of recipients to whom they are or may be disclosed.

(c) to have communicated to him in an intelligible form –

(i) the information constituting any personal data of which that individual is the data subject; and

(ii) any information available to the data controller as to the source of those data; and

(c) where the processing by automatic means of personal data of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision-taking.

Section 7(2) provides that:

A data controller is not obliged to supply any information under subsection (1) unless he has received –

(a) a request in writing; and

(b) Except in prescribed cases, such fee (not exceeding the prescribed maximum) as he may require.

The provisions of this section in my view appear to be in line with the Promotion of Access to Information Act.

Section 8(1) of the said act provides that:

The secretary of state may by regulations provide that, in such cases as may be prescribed, a request for information under any provision of subsection (1) of section 7 is to be treated as extending also to information under other provisions of that subsection.

Section 8(2) provides that:

The obligation imposed by section 7(1) (c) (i) is expressed in term which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.

Section 9 of the same act provides that:

> (1) Where the data controller is a credit reference agency, section 7 has effect subject to the provisions of this section.
>
> (2) An individual making a request under section 7 may limit his request to personal data relevant to his financial standing, and shall be taken to have so limited his request unless the request shows a contrary intention.
>
> (3) Where a data controller receives a request under section 7 in a case where personal data of which the individual making the request is the data subject are being processed by or on behalf of the data controller, the obligation to supply information under that section includes an obligation to supply information under that section includes an a obligation to give the individual making the request a statement, in such form as may be prescribed by the Secretary of State by regulations, of the individuals' rights –
>
> (a) Under section 159 of the Consumer Credit Act 1974; and
>
> (b) To the extent required by the prescribed form, under this Act.

Section 11 of the said act provides that:

> An individual is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purpose of direct marketing personal data in respect of which he is the data subject.

The analysis of the above provisions of the Data Protection Act in relation to RICA, illustrates that employers ought to inform employees when monitoring their electronic communications. At the same breath, employees are also entitled to request from their employers, information that has been processed or collected by the latter which relates to employees. This seems to be in line with the provisions of the Promotion of Access to Information Act 2 of 2000 (this act is discussed later in chapter 4). This Act was promulgated to conform to the provisions of section 34 of the 1996 Constitution.

18.2 The approach of the European Courts

In *Malone v United Kingdom*[74], the court had to consider whether or not there had been an infringement of the right to privacy. The Home Secretary had issued a warrant that authorized the tapping of the applicant's telephone without the latter's consent or knowledge. The applicant was charged with dishonesty in respect of handling stolen items. It was argued that such interception was contravening article 8 of the Convention. The court held that the interception of the applicant's telephone fell within the ambit of the protection of the right to privacy, pursuant to the provision of article 8 of the Convention. Such interception according to the court amounted to an interference of the right to privacy.

The court considered whether the limitation of the right to privacy was in accordance with the law and justifiable. In coming to its conclusion, the court first considered what was regarded as law by international jurisprudence. The court held that the word 'law' included written and unwritten law. This law ought to be accessible to the citizens in order for it to be considered as reasonable and justifiable. This case demonstrates a principle that ought to be enforced and applied by our courts. Thus, consent must or employees must have knowledge that their electronic communications would be intercepted.

In *Khan v The United Kingdom*[75], the court had to determine whether or not there had been an infringement of the right to privacy. The accused was convicted based on evidence obtained by placing a listening device in the telephone without his knowledge or consent. The accused argued that such interception impinged on his right to privacy pursuant to the provisions of article 8 of the Convention. The court held that there was no statute that regulated the interception at the time. Thus, the interception was indeed an invasion of the accused's right to privacy. However, in balancing the competing rights the court found that the admissibility of the evidence against him outweighed his right to privacy because he had been involved in serious crimes.

[74] 1983 WL 215891 (Eur Comm HR)(1983) 5 E.H.R.R.385.

[75] Khan v United Kingdom ECHR/2000/195.

This judgment illustrates that employees who are involved in criminal activities may not seek the protection of the right to privacy. This principle is akin to the principle set out by the court in *S v Dube.*

In *Halford v United Kingdom*[76] the court had to consider whether or not there had been a violation of the applicant's right to privacy in accordance with the provisions of article 8 of the European Convention on Human Rights 1950. The applicant argued that the police had intercepted her telephones at her office and at home. The court held that the applicant's right to privacy had been infringed. Furthermore, the applicant had reasonable expectation to privacy in relation to the calls she made at the business premises. This according to the court fell within the protection of the right to privacy in article 8 of the Convention. Coming to the issue of whether the limitation of the applicant's right to privacy was reasonable and justifiable or not, the court held that the interception of the latter's calls was not in accordance with the law, pursuant to article 8(2) of the Convention. In the same breath, there were no other provisions that regulated such interception. This case illustrates the importance of applying the principle of reasonable expectation to privacy in the work place, which has been affirmed by South African courts.

In *Amann v Switzerland*[77] the court also affirmed the principle of protection of the right to privacy where telephone calls had been intercepted in the business premises. The court also affirmed the principle that had been set out in the *Halford* judgment, that calls made in the business premises were protected by the provision of article 8 of the Convention. In *Kopp v Switzerland*[78] the applicant had been investigated by the Swiss Federal Council for an alleged breach of the duty not to disclose official secrets. The applicant's telephone had been intercepted and he argued that such interception invaded his right to privacy in accordance with article 8 of the Convention. The court held that the interception amounted to gross violation of the applicant's right to privacy pursuant to the provisions of article 8 of the Convention. In addition, if the applicant's right to privacy had to be limited, the limitation would be based on a law that would be precise.

---

[76] 1998 WL 1104805 (ECHR).

[77] 2000 30 E.H.R.R 843.

[78] 1998 WL 1043110 (ECHR), 4 B.H.R.C. 277.

Consequently, the limitation in the circumstances was not considered to be in accordance with law that was precise. Although these cases illustrate general application of the provisions of article 8 of the Convention, they stiffen the recognition of the protection of the right to privacy by the European Courts when there has been an interception of electronic communication..

In *Attorney General's Reference*[79] certain police officers were investigated for disclosing sensitive information to some criminals. The investigation was conducted by intercepting the said police officer's telephone calls. It was argued that such interception amounted to invasion of that police officer's right to privacy. The court considered the provisions of the Regulations of Investigatory Powers Act which criminalized the intentional unlawful interception of communications. The court found that evidence obtained by intercepting private telecommunications was admissible in criminal proceedings, provided that the courts took into account the circumstances of the case.

In *Re an Employer's Call- Monitoring System*[80] the court articulated the principle of protecting the right to privacy in an employment law context. In this case the employer had recorded the employee's telephone calls. Before this happened, the employer had agreed with employees that it would install telephone system to reduce costs. The recording of the employees' telephone calls was not communicated to the said employees. Subsequently, the employer recorded both private and business calls of these employees without their knowledge or consent. It was argued that the recording of these employees' telephone calls amounted to an invasion of their right to privacy.

The court restated the principle that telephone calls made in the business premises fell within the protection of the provisions of article 8 of the Convention. In addition, the court held that the reduction of costs and managing of the employees' time did not justify the limitation of the employees' right to privacy in the circumstances. The interception of such employees' telephone calls could have had adverse effect on their dignity because they subsequently became aware that they were being monitored.

[79] 2004 4 All ER 901.

[80] 2002 WL 32093079 (OGHA), 2004 E.C.C..4.

The court articulated that "technical long-term surveillance is in principle impermissible, unless the employer can demonstrate a superior legally protected interest."[81] Consequently, the employer infringed on these employees right to privacy and "the protection was relevant when the employees' action were being observed over a long period of time or systematically."[82] The court however pointed out that, if employees were instructed to make telephone calls by their employers and same monitors such calls to ensure that the instruction had been carried, such interception would not be regarded as an infringement of the right to privacy. This judgment shows the link between the protection of the right to privacy and dignity as it has been recognized by common law.

In *Hughes v Carratu International PLC*,[83] the applicant's documents relating to financial matters were seized based on a search warrant issued by the Information Commissioners Office. The applicant applied to the court for a disclosure of such documents, which were in possession of the respondent. The applicant argued that his right to privacy had been infringed and the search was as in contravention of the provisions of the Data Protection Act. The court found that there had indeed been an invasion of the applicant's right to privacy. This judgment is significant because it illustrate the general principle of protecting the right to privacy.

In *Associated Newspapers Limited v His Royal Highness the Prince of Wales*[84] in this case, a summary judgment had been granted regarding the journals wherein Prince Charles had recorded all his activities. An employee made copies of these journals; and provided them to the appellant in breach of her employment contract, and the extracts of these journals were later published. The court held that Prince Charles' right to privacy had been infringed by the publication of the extracts from these journals by the appellant. Consequently, there was a contravention of the provisions of article 8 of the Convention. Although this case denotes general principles of privacy, same shows the significance of protecting the right to privacy by the courts.

---

[81] *Ibid.*

[82] *Ibid.*

[83] 2006 EWHC 1791 QB.

[84] 2006 EWCA Civ 1776.

Bastiaan Bruyndonckx[85] discusses a judgment that illustrates how the Belgian Court of Appeal enforced the limitation of the employees' right to privacy in the workplace in relation to the use of the employers' email and internet facilities. Bryndonckx illustrates that the employee in this judgment had visited sites to access pornography and traded shares during official working hours. Bruyndonckx indicates that the Belgian Court of Appeal found that an employee had no reasonable expectation to privacy in the workplace because employers were entitled to monitor the latter's activities.

Moreover, the employer was justified to summarily dismiss an employee who had abused the employer's internet or emails facilities, during official working hours. The employee in question argued that his right to privacy had been infringed by such interception. The court however did not accept this argument because it was of the view that the employee had failed to honour his contractual obligation to carry out his activities "honestly, accurately and carefully."[86] Therefore, the interception of the electronic communications in the circumstances according to the court did not amount to an invasion of the employee's right to privacy.

Didler Wallaret[87] discusses the *Arbeidshof (Antwerpen) 2ek,* unreported Belgium judgment. He illustrates that there had been a collective bargaining agreement concluded between the employer and the employees that regulated the interception of their electronic communications. The employer in the said case intercepted the employees' emails and chat logs without obtaining consent or making the employees aware about such interception. It was argued that evidence obtained by such interception was in violation of the employees' right to privacy and contrary to the terms of the collective bargaining agreement. The court agreed and found that the limitation of the right to privacy was permitted, if the interception was conducted for specific purpose.

---

[85] Bastiaan Bruyndonckx (2006). Belgium: *Data Privacy-Monitoring of Communications,* [Online] Available http://international.westlaw.com/result/documenttext.aspx?=2fWelcome %WLIGen…

[86] *Ibid.*

[87] Didler Wallaret (2006) Belgium: Data Protection-Employment Law, [Online] Available http://international.westlaw.com/result/docuemnttext.aspx?rp=%2fWelcome%2fWLIGen

The court applied the proportionality test and held that:

> "This proportionality test recognized that access to individualized emails might interfere with the employee's personal privacy. Such interference must be necessary in order to collect the required information and should be kept to a minimum. In light of these the employer could not use the evidence obtained by such monitoring, to support the on-the-sport dismissal of the employee".[88]

Recently, in *Copland v The United Kingdom*,[89] the provisions of Article 8 of the Convention in light of monitoring an employee's electronic communications were tested. *In casu* briefly, an employee's email and internet use was intercepted by the employer. The employee also discovered that the employer had contacted her step-daughter and requested her to provide information relating to her communication and the employee in question. The employee's colleagues advised her that the employer was intercepting her electronic communications. The court found that at the time of the interception of the employee's electronic communications, there was no policy in place that regulated the interception.

The court concluded that "at the relevant time there was no general right to privacy in English Law". [90] In addition, the Regulation of Investigatory Powers Act 2000 regulated the interception of electronic communications. According to the court, The Telecommunications Regulations 2000 that were promulgated under the 2000 Act also regulated the interception of electronic communications. These Regulations permitted the limitation of the right to privacy by setting out circumstances, wherein electronic communications could be intercepted, without obtaining the necessary consent. However, employers had an obligation to advise employees that their electronic communications might be monitored. The court applied the principle set out in *Malik v Bank of Credit and Commerce International SA*[91], which articulates the significance of enforcing the employment contractual obligation.

---

[88] *Ibid.*

[89] Case reference application no. 62617/00 European Court of Human Rights 2007.

[90] *Ibid.*

[91] 1997 IRLR 462.

Thus;

> "as a matter of law, a general term is implied into each employment contract that an employer would not without reasonable and proper cause, conduct itself in a manner calculated and likely to destroy or seriously damage the relationship of confidence and trust between employer and employee". [92]

The court further affirmed the application of provisions of the Data Protection Act in so far as they relate to the interception of electronic communications. The employee in question had argued that the employee had infringed her right to privacy because "the conduct of the college was neither necessary nor proportionate." [93] The employee argued that the employer could have avoided the infringement of her right to privacy by drafting policies that regulated the interception of the latter's electronic communications. The court held that telephone calls made in the business premises were also protected by the provisions of article 8 of the Convention. Thus, such an employee had a reasonable expectation to privacy in relation to such calls, as it had been found by the court in the *Halford* judgment.

Further, the interception of emails also fell within the protection of the right to privacy pursuant to article 8 of the Convention. The employer had failed to advise the employee of the interception of her emails. The court also invoke the principle set out in the *Malone* judgment that:

> "the use of information relating to the date and length of telephone conversations and in particular the numbers dialled, can give rise to an issue under article 8, as such information constituted an integral element of the communications made by telephone. The fact that these data might have been legitimately obtained by the respondent, in the form of telephone bills, is no bar to finding an interference with rights guaranteed under article 8 of the Convention". [94]

In addition, in so far as the application of article 8 in the circumstances was concerned, the court further applied the principles set out in the *Amann* judgment that interception of electronic communications fell within the protection provided in article 8 of the Convention.

---

[92] *Ibid.*

[93] *Ibid.*

[94] *Ibid.*

Consequently, the employer had indeed infringed on the employee's right to privacy by intercepting her electronic communications without her consent or knowledge.

In determining whether the interference was in accordance with the law or not, the court invoked the object and purpose of article 8 of the Convention. Thus, the law must "be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by Article 8"[95]. The court held that it was not necessary in the circumstances to consider whether the limitation was reasonable and justifiable because there were no domestic laws that regulated the interception of the employee's electronic communications at the time. Consequently, there had indeed been a violation of Article 8 of the Convention. In *Microsoft Corpn v McDonald*[96] the court reinforced the principle of obtaining consent before intercepting employees' electronic communications, pursuant to the provisions of regulation 22 of Privacy and Electronic Communications Regulations 2003.

In *Sovereign Business Integration Plc v Trybus*[97] the protection of the right to privacy in an employment law context was at issue. An employee had been dismissed after the employer intercepted the latter's electronic communications to confirm allegations of misconduct. The employer discovered that the employee had forwarded confidential business information to his home email address. The employer held a disciplinary inquiry in the absence of the employee and he was thereafter dismissed. The employee argued that the interception of his electronic communications invaded his right to privacy. The Employment Tribunal Appeal held that the employee's behaviour was regarded as unprofessional but there was no need for the employer to take such drastic action against him. The appeal was accordingly dismissed.

In *R v Stanford*[98] the employees' emails were intercepted without their knowledge or consent. The former Deputy Chairman who was responsible for such interception had been charged for unlawful interception of electronic communications.

---

[95] *Ibid.*

[96] 2007 Bus.L.R.548.

[97] 2007 WL 1685225.

[98] 2006 2 Cr App.R.5.

The interception was said to be contrary to the provisions of section 1(2) of the Regulations of Investigatory Powers Act 2000. The court affirmed that it was necessary *in casu* to protect the employees' right to privacy because by criminalizing unlawful interception, the intention of the legislature was to enforce the protection of the right to privacy. Accordingly, the interception violated the employees' right to privacy.

The United Kingdom seems to follow the approach that is similar to the South African approach in protecting the right to privacy. Thus, an employee should first have a reasonable expectation to privacy before she/he can claim the protection of such a right. Furthermore, employees should give consent to the interception of their electronic communication or they should have knowledge of the interception. The jurisprudence illustrated *supra* shows that the limitation of the right in question would be justified, if such limitation is reasonable and justifiable in an open and democratic society.

19. **United State of America (USA)**

The protection of the right to privacy in the USA is enshrined in the Fourth Amendment. Buys & Cronje[99] argue that the protection of the right to privacy in the USA is contained in the provisions of the Electronic Communications Privacy Act of 1986. This protection is however subject to certain limitations provided in the same Act. Employees' right to privacy is also embraced in the provisions of the said Act. Evidently, the USA approach is akin to the South African Courts approach that rights are not absolute because they are subject to limitation clause test.

Ronald Standler [100] illustrates that the interception of emails is prohibited in terms of federal wiretap statutes. Mickler also embraces the notion that the ECPA does protect the employee's right to privacy but this right is subject to be limited.

---

[99] *Ibid.*

[100] Ronald B Standler (1998).Privacy of E-Mail in the USA [Online].Available http://www.rbs.2.com/email.htm.

Furthermore, the ECPA permits the interception of employees' electronic communications, if such interception is conducted for business use or employees' consent has been obtained for such interception. Mickler denotes that business use includes the protection of the business interest of the employer. This averment is similar to the provisions of section 6 of RICA, thus in the course of carrying on any business.

The US Supreme Court in *Katz v United States*[101] affirmed the protection of the right to privacy. In this case, the conversation of the accused was recorded by the police without his knowledge. He was later convicted of being involved in illegal gambling as a result of such recording. The accused argued that his right to privacy had been infringed by such recording pursuant to the provisions of the Fourth Amendment. The evidence obtained by the recording of his conversation was, thus inadmissible according to the accused.

Chief Justice Earl Warren reaffirmed the principle of legitimate expectation to privacy in accordance with the provisions of the Fourth Amendment. Justice Stewart concurred with Chief Justice Earl Warren and held that "the Fourth Amendment protected people not just places".[102] Furthermore, the interception of the accused conversation violated the right to privacy. Accordingly, such violation was contrary to the provisions of the Fourth Amendment. Justice Harlan also concurred with the above Justices. Justice Black, however, dissenting argued that the extent of the protection of the right to privacy "was not meant to protect personal privacy". [103] This judgment illustrates the application of the principle of legitimate expectation to privacy.

In *Olmstead v United States*[104], the accused conversation was recorded. It was argued that evidence obtained by such recording should not be admissible, as it impinged on the accused' right to privacy. Chief Justice Taft considered jurisprudence and concluded that the court must exclude evidence obtained contrary to the provisions of the Fourth Amendment.

---

[101] 389 U.S 347 1967.

[102] *Ibid*.

[103] Ibid.

[104] 277 U.S 438.

However, the recording of the accused' telephone in the circumstances did not fall within the protection provided in the Fourth Amendment. Accordingly, the rights in the USA are also subject to be limited depending on the circumstances of the case.

In *Watkins v LM Berry & Company*[105] the United States Court of Appeals had to consider whether or not there had been an infringement of the Fourth Amendment. In this case, the employee's telephone conversation relating to a job offer she had received was intercepted without her knowledge. The employer subsequently advised the employee that he did not want to lose her. This surprised the employee because she was not aware where this concern had come from but she was nevertheless dismissed. The employee argued that the employer had violated her right to privacy by intercepting her telephone conversation with her friend. The Court of Appeals held that the employer had infringed on the employee's right to privacy.

The monitoring, according to the court, went beyond than "what was necessary to determine whether the calls were made personal or not." [106] In addition, the court averred that "an employee's knowledge of employer's capability of monitoring her private telephone conversation, by itself, could not be considered implied consent to such monitoring."[107] Moreover, the Court of Appeal articulated that the employer could intercept employee's telephone conversation, if the latter is conducted within ordinary course of business, or to determine whether the calls made by such an employee are personal or not. The Court of Appeal expressed the view that the employer was not permitted to intercept the content of the employee's telephone conversation. The principles set out in this case affirm the provisions of section 5 and 6 of RICA.

[105] 704 F2d 577.

[106] *Ibid.*

[107] *Ibid.*

The Court of Appeal further considered the following:

> "The employer had an established policy, of which all employees were informed of monitoring solicitation calls as part of its regular training program; The monitored calls were reviewed by the employer to improve sales techniques; This monitoring was accomplished with standard extension telephone, located in the supervisor's office, which shared lines with telephones in the employee's office; and employees were permitted to make personal calls on company telephones and they were told that personal calls would not be monitored except to the extent necessary to determine whether a particular call was of personal or business nature". [108]

These are the factors that could be considered by our courts to determine whether the conduct of an employer infringes on an employee's right to privacy when monitoring electronic communications. Standler denotes that the principles set out in the *Watkins* judgment were subsequently contrasted by the same court in another judgment. The court according Standler was of the view that the recording of the employee's conversation was not unlawful as it (the interception) had been conducted during office hours. The calls were thus not personal according to the court. This to my mind is clearly a contradiction of what had been said in the *Watkins* judgment, and I fail to understand the rationale behind this finding. Standler submits that employers should draft policies that permit the interception of the employees' electronic communications. This would prevent any claims of the violation of the employee's right to privacy by the interception of his/her electronic communications.

In *Shoars v Epson*[109] the employee was dismissed after the interception of his electronic communications. It was argued that the interception was violating the employee's right to privacy and against public policy. The court agreed and granted summary judgment to the employee in question. The court however pointed out that employers were entitled to intercept communications in the workplace.

---

[108] *Ibid.*

[109] *Ibid.*

In *Bonita Bourke v Rhoda Hall*[110] the employer discovered that two employees were sending inappropriate emails that also contained pornography. One of the employees was dismissed and the other employee resigned. It was argued that the interception of these employees' electronic communications amounted to a violation of their right to privacy. The court granted summary judgment for the employer and the ratio was based on the application of the provisions of the ECPA and the Canadian Law.

Standler expresses the view that the court in *Smyth v Pillsbury*[111] did not protect the employee's right to privacy after finding that the employee's email was intercepted in a computer owned by the employer. The employee sent an email to his manager, which contained "threats to kill backstabbing bastard" [112]and the latter was subsequently dismissed. The court held that the employee could not claim to have reasonable expectation to privacy because same had sent the emails voluntarily. The right to privacy therefore under the circumstances could not be protected. The court balanced the two competing interests and found that the interest of the employer to protect its business interest outweighed the employee's right to privacy. Besides, the comments made by the employee in the circumstances, to his supervisor were unprofessional and inappropriate. Therefore the interception according to the court was indeed justified.

In *Bohach v City of Reno*[113] the court affirmed the principle of reasonable expectation to privacy illustrated by the *Katz test* and held that the interception of electronic communications was within the ordinary course of business pursuant to the provisions of the ECPA. Standler indicates that another well known case that reinforces the protection of the right to privacy is *U.S v Maxwell.* Standler argues that the said case has a persuasive effect because it was decided under the Military Rules of Evidence, but the courts could apply its principles. In this case, the reasonable expectation to privacy principle was affirmed.

---

[110] No.YC-003979 (Cal.Super.Ct, LA Cty) 1993.

[111] 914 F Supp.97 (E.D.Penn.1996).

[112] *Ibid.*

[113] 932 F Supp.1232 (D.Nev.1996).

In *Anderson v UOP*[114] the employee's emails he sent to the Wall Street Journal were intercepted. The employee argued that his right to privacy had been intercepted by the interception of the content of his email. The court however dismissed this averment because the email system of the employer was not available to the public. In *United States v Councilman*[115] the employer intercepted all emails including employees' emails, before they reached the recipients, because the latter contemplated that the intercepted emails could be used for commercial advantage. It was argued that such interception violated the provisions of the Wiretap Act. The court found that the legislature intended to give lesser protection to electronic communications than wire and oral communications. Judge Lipez dissenting rejected the Councilman's claim that "Congress only intended to protect email when it was traveling through cables and not when it was being processed by electronic switches and computers during transit and delivery".[116]

The Catholic University of America[117] reiterates the application of the two exceptions provided in the ECPA, thus, consent and business extension exemption in the employment law context. The US writers, namely Standler and other writers express[118] the view that employees should give express consent because it could be difficult to prove implied consent. It has been pointed out that the courts have followed different approaches in determining what is regarded as implied consent. In one case, the court held that knowledge that one's electronic communications might be intercepted does not suffice to be considered as implied consent. [119] Proper consent would be considered to have been given, if employers draft policies that regulate and permit the interception of the employee's electronic communications.

---

[114] 1998 L 30703 (N.D.III.26 Jan 1998).

[115] No.03-1383 (1st Cir.decided June 29 2004).

[116] *Ibid*.

[117] The Catholic University of America, *Summary of Federal Laws* [Online] Available http://www.counsel.cua.edu/fedlaw/Ecpa.cfm

[118] *Ibid*.

[119] From the Lectric Law Library's stacks*: Electronic Privacy Rights*: *The Workplace* [Online] Available http://www.lctlaw.com/files/emp41.htm

In addition, the mere fact that employees consent to the interception of telephone calls for business purposes, does not necessarily mean that same consents to the interception of his/her personal calls. The Lectric Law Library writers aver that employers should give employees notice of the interception of their electronic communications and the latter must acknowledge in writing that such notice has indeed been given.

The Publishing Law Center[120] indicates that the court in *O'Connor v Ortega*[121] reiterated the principle of reasonable expectation to privacy but the circumstances of the case would determine the reasonableness of the limitation of the right in question. Furthermore, the application of this principle had been followed subsequently by the courts in *Schoewengerdt v General Dynamics Corp.*[122]

Recently, in *Warshak v United States of America*[123], the United States Court of Appeals had to determine whether there had been an infringement of the plaintiff's' right to privacy or not. It was argued that there had been an infringement of the right to privacy as the searches conducted were contrary to the provisions of the Fourth Amendment. The plaintiff's electronic communications in the circumstances had been intercepted by the government. The United States Court of Appeals held that the plaintiff had reasonable expectation to privacy, as emails, as mode of communication fell within the protection provided in the Fourth Amendment. The Fox News[124] illustrate that this judgment "answered a question that had been dangerously open and it applies the provisions of the Fourth Amendment to electronic privacy rights of citizens ".[125]

---

[120] The Publishing Law Center, *The Right to Privacy* [Online] Available http://www.publaw.com/privacy.html

[121] *Ibid*.

[122] *Ibid*.

[123] No.06-4092 U.S. Crt.App. (Decided June 18, 2007).

[124] Fox News.com *Court Rules E-mail Search Without Violates Fourth Amendment* [Online] Available http://www.foxnews.com/printer-friendly-story/0,3566,284193,00html.

[125] *Ibid*.

Bryan Knowles[126] indicates that employees' electronic communications are likely to be intercepted by employers in the workplace, with or without their consent or knowledge. The interception according to Knowles is a manner of monitoring employees' performance and protecting the employer from criminal liability. Knowles argues that some employers do not advise their employees that their electronic communications might be intercepted. Such interception according to Knowles is regarded as an infringement of the employees' right to privacy pursuant to the provisions of the Fourth Amendment.

Knowles further expresses the view that has indirectly been illustrated by the Constitutional Court in the *NM v Smith* judgment. Thus "electronic communications or communications, especially of a private nature, are the property of individuals." [127]On the other hand, Knowles argues that employees should conform to contractual obligations by ensuring that they are being productive during working hours instead of accessing internet or writing or sending personal emails.

Dice[128] articulates that employers could be held liable for the conduct of employees that could result in criminal liability against the employee in question. This according to Dice raises the need to monitor these employees' electronic communications. Dice also illustrates that employees on the one hand seek to protect their right to privacy when employers intercept their electronic communications, by bringing action against their employers. However, the employers' right to intercept employee's electronic communications is limited. Connelly, Roberts & Mc Givney LLC[129] indicate that the ECPA does not explicitly protect the right to privacy. Furthermore, employers apply the exceptions provided in the ECPA to protect their business interests, thus, consent and ordinary course of business.

---

[126] Bryan Knowles (2000) Are Employers Violating Worker's Privacy with Electronic Monitoring? [Online] Available http://www.speakout.com/activism/issue-brief/1300b-1.html.

[127] *Ibid.*

[128] Dice *Workplace privacy versus computer abuse prevention :which prevails?* [Online] Available http://www.articles.techrepublic.com.5102-10878-144095.html

[129] Connelly, Roberts & Mcivney LCC *Priavcy Issues in a Hi-Tech W*orkplace [Online] Available http://www.library.findla.com/1998/Mar/1/130358.html.

The application of these exceptions had been affirmed by the US Courts in *Briggs v American Air Filter Co*[130] ;*James v Newspaper Agency Cop*[131]*; United States v Long*[132]. In the latter case the emails revealing drug dependency relating to the accused were intercepted without her consent. It was argued that such interception was an infringement of the accused' right to privacy, therefore, contravened the provisions of the Fourth Amendment. Wagner J asserted that the interception was conducted for the purpose of obtaining evidence and the court was satisfied that the accused had not given the necessary consent.

However, the accused had reasonable expectation of privacy in relation to the emails intercepted in the circumstances. Accordingly, there was no violation of the Fourth Amendment in the circumstances regardless of the fact that it had been discovered that the interception had been conducted without lawful authorization, but such error could not be considered prejudicial. Wagner J reinforced the principle set in the *O'Connor* decision, that "the right to privacy extends beyond the traditional boundaries of private homes and persons and reaches into the workplace, including government offices".[133] Wagner J considered one of the factors that guard against the violation of the employee's right to privacy as taking necessary steps to protect the employees right to privacy in the process of intercepting the latter's electronic communications.

Wagner J had to further consider an argument that was advanced in contrast that:

> "The employer owns and operates the computer network, the employee uses the network to send and receive emails, if the employer has warned that the electronic information in the system is not confidential and may be viewed by network administrators and others, and then the employee cannot claim an expectation of privacy. An expectation of privacy does not have to be an all or nothing idea. An expectation of privacy also need not be an expectation that the subject item or information is completely private from all third party knowledge.

[130] 455 F Supp.179 (N.D.Ga.1978).

[131] 591 F.2d 579.

[132] 61 M.J.539.

[133] *Ibid*.

> The appellant's use of the password system provided precautions necessary to safeguard her privacy in her emails, as well as her ability to exclude others from her email account". [134]

The above discussion evinces that the USA courts consider the protection of the right to privacy within the ambit of the Fourth Amendment, with specific reference to search and seizures. In addition, the ECPA does recognize the protection of an employee's right to privacy, although this protection is subject to the application of the exceptions provided in the ECPA, thus, consent and ordinary course of business. Put differently, employers may intercept employees' electronic communication during ordinary course of business. It is explicit that the application of the legitimate expectation to privacy principle gives rise to a claim of the protection of the right to privacy.

20. **Canadian Law**

Gail Lasprogata *et al*[135] assert that the Canadian Constitution does recognize and protect the right to privacy. This protection is provided in section 8 of the Charter of Rights and Freedoms of 1982. Section 8 of the Charter provides that "everyone has a right to be secure against unreasonable search and seizure". Lasprogata *et al* indicate that the Charter of Rights and Freedoms does not specifically guarantee a right to privacy but the Canadian Courts have accepted that the protection of the right to privacy is embraced within the provisions of section 8 of the Charter. The protection of the right to privacy in Canada is regulated by the Privacy Act of 1982.

---

[134] *Ibid.*

[135] Gail Lasprogat, Nancy J King & Sukanya Pillay Regulation of Electronic Employee Monitoring: Identify Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada, Stanford Technology Law Review [Online] Available

http://www.//stlr.stanford.edu/STLR/Articles/04-STLR-4 .

In addition, Lasprogata *et al* further argue that the application of the protection of the right to privacy had been extended by the Supreme Court of Canada, to the employment law context. Moreover, the employee's right to privacy may be limited by applying the standard of reasonableness test based on the circumstances of each case.

The application of this test according to Lasprogata *et al* would determine whether the employee has a reasonable expectation to privacy or not and the Canadian Courts have considered the application of this test in one the Canadian judgments. In this Canadian Court judgment the Supreme Court held that the interception of electronic communications was indeed an infringement of the right to privacy. However, the application of the standard of reasonableness test justified its limitation. This principle was later affirmed in *Re Doman Forest Products Ltd*[136]. The court in the said case went further and held that "the standard of reasonableness test requires balancing of the right of individual employee to be left alone and the right of employers to intrude in furtherance of their legitimate business interest." [137]

The standard of reasonableness test was subsequently considered and applied in *R v M*.[138] The court held that the protection of the employee's right to privacy could not be claimed where one had been aware that his/her electronic communications was being intercepted. The court articulated that the following were the factors that determined whether the intrusion to one's right to be left alone was reasonable or not: "whether it was reasonable to request surveillance; whether the surveillance was conducted in a reasonable manner; and whether any other alternatives to surveillance were available to the employer or not." [139]

Lasprogata *et al* illustrate that the principles set out above had been frequently referred to by the Canadian writers. In addition, the Canadian Courts might consider these principles in the process of determining whether or not the interception of employees' electronic communications violated their right to privacy.

---

[136] 1990 3 L.A.C. (B.C) (4TH 275.

[137] *Ibid*.

[138] 2005 BCSC 385.

[139] *Ibid*.

These principles could be invoked by the courts when applying section 36 of the 1996 Constitution, to determine whether RICA passes the limitation clause test or not. Evidently, the South African Courts may also invoke the standard of reasonableness test when balancing the competing rights.

Lasprogata *et al* assert that the Privacy Act of 1982 provides for the right to access information relating to a person, which is held by the federal government. The same Act also protects one's right to privacy in that it prevents unauthorized disclosure of personal information. Buys & Cronje embrace Lasprogata *et al*'s averment in so far as they relate to the provisions of the Privacy Act. The discussion in this paragraph indicates the likelihood of invoking the provisions of the Promotion of Access to Information Act, after the employer has intercepted or monitored the employee's electronic communications.

Lasprogata *et al* further illustrate that the right to privacy in Canada in relation to the interception of electronic communications, is further protected by the promulgation of the Personal Information Protection and Electronic Documents Act (PIPEDA). The pertinent provision of PIPEDA illustrates that personal information may not be intercepted without consent or knowledge. Lasprogata *et al* argue that the aim of PIPEDA from the outset was to protect the right to privacy by incorporating provisions that would limit the right to intercept one's electronic communications. More importantly, the regulation of the interception of electronic communications also applies in employment law context.

Employers therefore ought to obtain consent from the employees before intercepting the latter's electronic communications. At the same breath, employees must also ensure that employees are aware about the interception of their electronic communications. Furthermore, Lasprogata *et al* indicate that the fact that Canada is a party to the International Covenant on Civil and Political Rights is an illustration of recognizing the need to protect the right to privacy. In addition, the right to privacy in Canada has been defined as the fundamental right, and this had been affirmed in *Dagg v Canada*[140].

[140] *Ibid.*

Lasprogata *et al* argue that “although privacy is not a right specifically guaranteed by the Canadian Charter of Rights and Freedom, the notion of a right to privacy emerges from democratic ideals regarding the individual, the state and the fundamental freedoms requisite to democracy.” [141] Lasprogata *et al* further illustrate that interception of one's electronic communications without obtaining the necessary consent or knowledge is considered to be a criminal offence in terms of the Canadian Criminal Code. Further, the provisions in the said code "do not apply to interception in which a party to the communications has consented as is likely to be the case when an employee agrees to an employer's policy on electronic monitoring". [142] Accordingly, the Canadian Courts also enforce the provisions of section 5 and 6 of RICA.

In *St Mary's Hospital v H.E.U*[143], employees were monitored by their employer by installing hidden cameras. When employees became aware of such monitoring, they lodged a grievance against the employer. The employer argued that surveillance was necessary to investigate theft of certain documents. The court applied the proportionality test and affirmed that “the employers’ legitimate business interests must be balanced against the employees' concerns and the test required employers to exhaust all available alternatives before intruding on employees' privacy".[144] Consequently, the court held that there had been a violation of the employee’s right to privacy, because the employer had failed “to exhaust all available alternatives first”[145] in order to obtain evidence relating the theft.

[141] *Ibid.*

[142] *Ibid.*

[143] 64 L.A.C.(4TH) 382.

[144] *Ibid.*

[145] *Ibid.*

Lasprogata *et al*, argues that the application of the reasonable expectation to privacy principle had been affirmed by the Supreme Court of Canada in *R v Wong*[146]. In *R v Weir*[147] , the court found that the interception of emails fell within the protection afforded by the provisions of section 8 of the Charter. The court further found that "although email communications are expected to be private, the nature of the technology leaves it vulnerable to exposure".[148]

Mac-Alexandre Poirier [149]opines that the interception of the employees' emails could affect the latter's reasonable expectation to privacy. Poirier justifies the interception of employees' electronic communications, without consent or knowledge because the emails sent or received by the employee could be business-related, hence the limitation of the employee's right to privacy in the workplace, in most cases, is reasonable and justified. Further, employers must protect their business interest by exercising some level of control over employees and this could be achieved by intercepting the latter's electronic communications.

Poirier argues that the scope of the protection of the right to privacy in an employment relationship context means that "an employee's renunciation of the right to privacy cannot be inferred from the existence of the work relationship."[150] In addition, if employers have policies in place that permit the interception of employees' electronic communications, the latter's right to privacy, would be limited. Thus, such employees would not have legitimate expectation to privacy.

[146] 1990 3 S.C.R.36.

[147] *Ibid*.

[148] *Ibid*.

[149] Mac-Alexandre Poirier (2000) *Employer Monitoring of the Corporate E-mail System: How Much Privacy Can Employees Reasonable Expect?* [Online]. Available http://www.law.uiuc.edu/publications/CLL-PJ/archive/vol-24/issue-3/EltisArticle24-4.

[150] *Ibid*.

The same applies in instances where the interception of electronic communications had been a long-established practice, “especially in industries where such interception had been regarded as an integral part of the ordinary business”, the expectation of the right to privacy in such circumstances, would be diminished.[151] Poirier further argues that employees may claim legitimate expectation to privacy wherein employers provide passwords to access the use of their computers.

Charles Morgan[152] supports the notion that the right to privacy is not absolute as it can be limited, depending on the circumstances of the case. Morgan embraces the principle of applying the proportionality test, when balancing the employers’ right to promote his/her business interest on the one hand and the employees’ right to privacy. Morgan further argues that the Canadian Courts have accepted the notion that the interception of the employees’ electronic communications must be conducted pursuant to the law. Morgan argues that in a certain case, the interception of an employee’s electronic communications was conducted without consent or knowledge. The issue before the court was whether the evidence obtained by such interception would be admissible or not. The court affirmed that such evidence was indeed admissible.

In *Oullet v Cuisirama Inc.*[153] the plaintiff’s conversation was intercepted without his knowledge. The court had to decide whether or not such interception violated the plaintiff’s right to privacy. The Labour Commissioner emphasized the importance of protecting the right to privacy in instances wherein the information intercepted was personal in nature. Morgan reiterates that employers must first obtain consent from their employees before they intercept the latter’s electronic communications. In the alternative, the employees should inform employees of the interception of their electronic communications. This, according to Morgan, would be achieved by drafting policies that would be explicit enough and the employer “should not intercept or monitor its employees' use of email and internet to any great extent than it has set out clearly in its monitoring policy".[154]

---

[151] *Ibid.*

[152] Charles Morgan, *Employer Monitoring of Employee Electronic Mail and Internet Use* 1999, 44 McGill L.J.849.

[153] *Ibid.*

[154] *Ibid.*

Furthermore, Morgan embraces the notion that is expressed by most writers that "employees should sign a form in which, they acknowledge that they have read the policy and consent to abide by its terms".[155] This view seems to be akin to the provisions of section 5 of RICA. The analysis of the above discussion denotes that the protection of the right to privacy is guided by the principle of a reasonable expectation, in respect of the monitoring electronic communications. It is explicit that the right in question is not regarded as an absolute one, because it can be limited when circumstances call for such limitation. Most Canadian writers embrace the notion of obtaining consent before embarking in the process of monitoring electronic communications, as this would prevent claims of an infringement of employees' right to privacy.

21. **Australian Law**

The Australian Law Reform Commission (ALRC) [156] shows the recognition of the protection of the right to privacy. The ALRC illustrates that the protection of the right to privacy regarding the interception of electronic communications is regulated by the provisions of Privacy Act of 1988. Greg Taylor in the Melbourne University Law Review [157] argues that Article 17 of the International Covenant on Civil and Political Rights places an obligation on States who are signatory of the Covenant to protect the right to privacy. It is averred that because Australia signed this Covenant, it is obliged to enforce the protection of the right to privacy. In A*ustralian Broadcasting Corporation v Lenah Game Meats Pty Ltd*,[158] the High Court for the first time in Australia recognized the need to protect the right to privacy and developed the common law.

---

[155] *Ibid*.

[156] Australian Law Reform Commission, Overview of ALRC Issues Papers 31 & 32, Review of Privacy [Online] Available http://www.austlii.edu.au//cgi-bin/disp.pl/au/other/alrc/publications/issues/31-32-overview...

[157] Greg Taylor Melbourne University Law Review (2005) *A Tort of Invasion of Privacy in Australia*, MULR 11.

[158] 2001 208 CLR 199.

Greg Taylor indicates that “in New South Wales, the Workplace Surveillance Act 2005 came into effect on 7 October 2005". The purpose of this Act is to regulate surveillance of employees at work and for other purposes.

Section 10 of the same Act provides that:

> Surveillance of an employee must not commence without prior notice in writing to the employee.

This provision is similar to the provisions of section 6 of RICA as same requires employers to give employees notice that their electronic communication would be intercepted. Therefore, a deduction can be made that employees in Australia have a reasonable expectation to privacy.

Subsection 6 of the same section provides that:

> Notice to an employee is not required under this section in the case of camera surveillance at a workplace of the employer that is not a usual workplace of the employee.

Section 14 of the said Act provides that:

> Surveillance of an employee is taken to comply with the requirements of this part, if the employee (or a body representing a substantial number of employees at the workplace) has agreed to the carrying out of surveillance at the premises or place where the surveillance is taking place for a purpose other than surveillance of employees and surveillance is carried out in accordance with that agreement.

Section 16 of the said Act provides that:

> An employer must not carry out or cause to be carried out surveillance of an employee of the employer using a work surveillance device when the employee is not at work for the employer, unless the surveillance is computer surveillance of the use by an employee of equipment or resources provided by or at the expense of the employer. A work surveillance is a device used for surveillance of the employee when at work for the employer.

Section 19 of this Act provides that:

> An employer must not carry out or cause to be carried out, covert surveillance of an employee while the employee is at work for the employer, unless the surveillance is authorized by a covert surveillance authority.

Section 20 of the same Act provides that:

> A covert surveillance authority that is issued to an employer or employer's representative authorizes the covert surveillance generally of any employees while at work for the employer, but only for the purpose of establishing whether or not one or more particularly employees are involved in any unlawful activity while at work for the employer.

Subsection 3 of the same section provides that:

> A covert surveillance authority does not authorize the carrying out, or causing to be carried out of covert surveillance of any employee for the purpose of monitoring the employee's performance.

Section 26 of the said Act provides that:

> A Magistrate must not issue a covert surveillance authority, unless same has had regard to whether covert surveillance of the employee concerned might unduly intrude on their privacy or the privacy of any other person.

This provision denotes the recognition of the right to privacy.

Greg Taylor argues that the interception of employee's right to privacy is not regulated in some Australian jurisdictions. In addition, the Commonwealth Privacy Amendment (Private Sector) Act 2000 regulates the interception of electronic communications to a certain extent. This writer argues that "at most, the Act may require employers to inform employees, if their email and net user is being monitored although this is questionable".[159]

[159] *Ibid.*

The analysis of the Australian Law evinces that consent and knowledge of the interception of electronic communications are significant factors that should be considered to determine whether or not there has been an infringement of an employee's right to privacy. This appears to be similar to the principles set out in the Protection of Personal Information Bill that is discussed in chapter two as well as the provisions of section 5 and 6 of RICA.

22. **Conclusion**

There is no doubt that international and foreign jurisprudence illustrated *supra* is significant to the judiciary as well as the legislature in the process of enforcing the protection of the right to privacy, in an employment law context. It is explicit that the International Conventions illustrated in this chapter recognize the protection of the right in question. It is also evident that various jurisdictions apply different approaches in protecting the right to privacy in sofar as same relates to the monitoring of the employees' electronic communications.

In the United Kingdom, as evident from the discussion in this chapter, the protection of the right to privacy in relation to the monitoring of electronic communications is enshrined in the provisions of the Data Protection Act. Furthermore, the United Kingdom courts have reinforced the protection of such right and this is illustrated in the *Copland v United Kingdom* judgment, together with all other judgments that are discussed in this chapter. It is also evident that employees ought to have a reasonable expectation of privacy in the workplace before claiming the protection of such a right. This principle is akin to the approach followed by the South African courts. This principle is now incorporated in the provisions of section 5 and 6 of RICA.

In the United States of America, the protection of the right to privacy in relation to the monitoring of electronic communications is protected by the Fourth Amendment as well as the ECPA. The *Katz* judgment together with all other judgments that are discussed in this chapter illustrate that the US courts does indeed recognize the protection of the right to privacy in relation to the monitoring of electronic communications, but this is subject to certain limitations.
The Canadian Courts appear to follow the UN and the South African Law approach of applying "the reasonable expectation to privacy principle" in protecting the right to privacy.

The Canadian Statutes namely, Privacy Act and PIPEDA seek to protect the right in question. In Australia the protection of the right to privacy is contained in the Privacy Act, Workplace Surveillance Act as well as the International Conventions.

It is observed that international and foreign jurisprudence reiterates the significance of obtaining consent and ensuring that employees have knowledge of the interception or monitoring of their electronic communications, to protect the right to privacy. Furthermore, if the monitoring of electronic communications is conducted during an employer's course of business, the latter would be permitted. These principles are akin to the provision of section 5 and 6 of RICA. The application of the principles discussed in this chapter is illustrated in chapter four. In light of what has been discussed above, the question is whether or not RICA passes the limitation clause test pursuant to section 36 of the 1996 Constitution.

CHAPTER FOUR

23. Introduction

"Is an employee obliged to tolerate his employer (literally or figuratively) peering over his shoulder as he works?[160] Is that not an infringement of the dignity which is an inseparable element of personal privacy"?[161] This chapter discusses in detail how the infringement of an employee's right to privacy relates to the employment law context, with specific reference to the interception of an employee's electronic communications. This is accomplished by constructing the provisions of section 4, 5 and 6 of RICA.

This chapter applies the principles that are illustrated in the previous chapters which are pertinent to employment law context, including principles of interpreting statutes as well as the constitutional interpretation. The chapter begins by discussing general principles of common law relating to the employment law context and how the courts apply these in relation to the interception of an employee's electronic communications. This is followed by the discussion of the relevant provisions of the LRA; RICA as well as the relevant provisions of the Constitution. The application of the principles of interpreting statutes is incorporated in the construction of RICA as well as the constitutional interpretation.

24. Common law principles relating to employment relationship

An employee's contractual relationship is regulated by common law and labour law statutes. Grogan[162] argues that "there is an implied term that the parties to the contract shall respect each other's privacy".[163] Grogan further argues that contracts concluded between employers and employees place an obligation on each party to respect the right to privacy.

---

[160] J F De Beer (2003) *Employee Privacy: The Need for Comprehensive Protection*, Saskatchewan La Review, Vol.66(2), p383.

[161] *Ibid*.

[162] Grogan (2003) 53.

[163] *Ibid*.

In addition, both employers and employees are expected to conduct themselves in a manner that would not jeopardise the employment relationship. This could be achieved by adhering to the terms of employment contract; the rules and policies of employers as well as conforming to the provisions of the Bill of Rights.

Grogan further indicates that common law obligations are emphasised by the provisions of the section 1of the LRA. The reciprocal contractual obligations were affirmed by the court in *Malik v Bank of Credit and Commerce International SA*[164]. The court asserted the significance of avoiding the destruction of the employment trust relationship by all means. The court averred that in most cases, this obligation is not expressly provided in the terms of the employment contract. Thus, this obligation is implied into the terms of the employment contract concluded between the parties. This principle was recently affirmed by the UN Courts in the *Copland* judgment.

25. **The LRA**

The heart of this legislation is to regulate the employment relationship between an employer and an employee.

Section 1 of this Act provides that:

> The purpose of this Act is to advance economic development, social justice, labour peace and the democratisation of the workplace by fulfilling the primary objects of this Act, which are –
>
> (a) to give effect to and regulate the fundamental rights conferred by section 27 of the Constitution;
>
> (b) to give effect to obligations incurred by the Republic as a member state of the International Labour Organisation;
>
> (c) to provide a framework within which employees and their trade unions, employers and employer's organisations can –
>
> (i) collectively bargain to determine wages, terms and conditions of employment and other matters of mutual interest; and
>
> (ii) formulate industrial policy…

[164] 1997 3 All ER 1.

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 provision reinforces the common law principles illustrated above. Therefore, both employers and employees ought to respect the contractual obligations. This means, employers should protect the employees' right to privacy and employees must not abuse the employees electronic facilities.

Item 7 of Schedule 8 provides that:

> Any person who is determining whether a dismissal for misconduct is unfair or not should consider –
> (a) whether or not the employee contravened a rule or standard regulating conduct in, or of relevance to, the workplace; and
> (b) if a rule or standard was contravened, whether or not –
> (i) the rule was a valid or reasonable rule or standard;
> (ii) the employee was aware, or could reasonably be expected to have been aware of the rule or standard;
> (iii) the rule or standard has been consistently applied by the employer; and
> (iv) dismissal was an appropriate sanction for the contravention of the rule.

This item is significant because if it alleged that a certain employee has abused the employer's electronic communications, it must be determined whether or not that employee was aware that he/she was not suppose to abuse such employer's electronic communications before disciplinary proceedings are instituted against him/her, having due regard to the circumstances of the case.

26. **Promotion of Access to Information Act 2 of 2000**

The above Act provides that its object is to:

> Give effect to the constitutional right to access to information, held by the state, and any information that is held by another person pursuant to section 32 of the Constitution. In addition, this Act is required for the exercise or protection of any rights; and to provide for matters connected therewith…the right to access to any information held by a public or private body may be limited, to the extent that the limitations are reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom as contemplated in section 36 of the Constitution.

It is my contention that this Act is pertinent because it grants an employee a right to claim access to information pertaining to him, held by his employer, which has been obtained through monitoring the latter's electronic communications. The High Court has held that this right is however subject to limitation, as it had been affirmed in *Phato v Attorney-General*[165]. It is argued that an employee cannot automatically expect an employer to provide access to information, if such information has been obtained through monitoring the latter's electronic communications. The Privacy Act in Canada also provides that employees are entitled to have access to information held relating to them by their employers.

[165] *Eastern Cape, and Another: Commissioner of the South African Police v Attorney-General, Eastern Cape, and Others* (1995) 1 SA 799 (E).

27. **How do courts apply the common law principles relating to employment relationship context in light of monitoring electronic communications?**

In *Lawrence v Kuper & Co*[166], the Industrial Court put emphasis in the trite principle that "an employee is required to serve his employer honestly and faithfully, and this includes furthering the employer's business interests and avoiding a clash between his personal interest and those of the employer."[167] The same Industrial Court illustrated that employees must render their services lawfully to their employers. Thus, employees must avoid engaging themselves in unlawful activities during official working hours.

In *Toker Bros (Pty) Ltd and Keyser*[168] the employee's electronic communications were intercepted by the employer. It was argued the employee had abused the employer's internet and made derogatory statements about same. The employee argued that the interception violated his right to privacy and he had obtained permission from his employer to arrange a school reunion. The employee denied the allegation that he had abused the employer's facilities. The employer on the other hand denied that it had permitted the employee to use its facilities to arrange a school reunion. In addition, the employer argued that the time spent on internet by the employee exceeded the amount of time he spent on producing his work.

The employer further argued that the employee had destroyed the employment trust relationship because he had been employed in good faith; however he had failed to conform to his contractual obligation. Instead he abused his employer‘s facilities by spending excessive amount of time surfing the net for his personal use at the expense of the employer. More importantly, the employee had been aware that his conduct was inappropriate and unacceptable.

---

[166] Pty Ltd t/a Kuper, as a member of Investec (1994) 15 ILJ 1140 (IC).

[167] *Ibid.*

[168] 2005 26 ILJ 1366 (CCMA).

Commissioner Van Niekerk found that there were no rules that regulated the use of internet facilities. The employee was however expected to use his discretion in the manner in which he used the facilities and the amount of time spent on surfing the net. Commissioner Van Niekerk took into account the evidence presented that confirmed the abuse of the employer's facilities and held that the employee could have reasonably be expected to be aware that he was not allowed to abuse his employer's facilities.

Furthermore, Commissioner Van Niekerk noted that the provision of section 14 of the Constitution prevented the employer from intercepting the employee's electronic communications without his consent or knowledge. However, the interception in the circumstances was conducted to investigate the allegations of abuse of employer's facilities. Such interception was "not malicious but incidental to the investigation".[169] Accordingly, the employee's right to privacy had not been infringed and the evidence obtained by such interception was admissible, regardless of the fact that there had been no rules permitting the interception. Further, the employee could have used common sense because rules do not necessarily have to be made known to the latter.

Another important submission made by Commissioner Van Niekerk was that, in some instances, the level of qualification and experience of an employee places some obligation on same to observe unwritten rules. Commissioner Van Niekerk considered the fact that the employer had to protect its business interest as same could have been held vicariously liable. That justified the limitation of the employee's right to privacy. This limitation was in accordance with the limitation clause test provided in section 36 of the Constitution.

[169] *Ibid.*

Commissioner Van Niekerk affirmed the principle that it has been accepted by our courts as well as the writers that rights are not absolute, because they are subject to the limitation clause test provided in section 36 of the Constitution. Commissioner Van Niekerk considered the principles set out by Heher J in the *Protea Technology* judgment that evidence obtained by intercepting employee's electronic communications could be admissible in court, if the interception was conducted to investigate or affirm allegations of misconduct, regardless of the manner in which it had been obtained. This however would depend on the circumstances of the case. Commissioner Van Niekerk asserted the views expressed by Collier that employers may be held either criminally or vicariously liable for the conduct of their employees in the workplace, hence in some instances, it is necessary to intercept the employee's electronic communications. The principle set in this CCMA award shows that employers may intercept employees' electronic communications to investigate certain allegations pertaining to the employee's misconduct.

In *Van Wyk v Independent Newspapers Gauteng (Pty) Ltd*[170], the court had to consider whether or not there had been an infringement of the employee's right to privacy, after the interception of the latter's electronic communications. In this case, an employee had an argument with her editor and the rest of the management team and she criticised them in an email she circulated later wherein she vented all her frustrations in respect of the incident. The employee was invited to attend a disciplinary inquiry and she was subsequently dismissed, regardless of the fact that she had subsequently apologised to her managing director.

The issue before Revelas J was whether or not the interception of the emails in the circumstances contravened the provisions of the IMP Act. Revelas J held that the employer's policy explicitly advised the employees that their electronic communications could be intercepted. Consequently, the employee's right to privacy in the circumstances had not been impinged. The limitation was thus reasonable and justifiable in accordance with the provisions of section 36 of the Constitution. I am of the view that Revelas J had correctly decided in this judgment because the employee's conduct in the circumstances did not warrant the protection of the right to privacy, regardless of how emotional she had been at the time she circulated the emails.

[170] 2005 26 ILJ 2433 (LC).

Sending derogatory emails about one's manager in the work environment does not, in my view call upon the protection of the right to privacy. The conduct of the employer in these circumstances did not infringe on the employee's right to privacy.

In *Surgreen and Standard Bank of SA*[171] the employee's telephone conversation had been intercepted by the bank. It was discovered that the employee had accepted bribes from a service provider that had a contract with the bank, which she had authority over. The employee argued that her right to privacy had been violated by the interception of her telephone conversation without her knowledge. Therefore, the evidence that was obtained by such interception was inadmissible. Commissioner Rycroft concluded that the employer had a legitimate interest in the employee's electronic communications, particularly, if there had been allegations of misconduct. Due consideration was taken to the fact that such interception was conducted during business hours. That justified the limitation of the employee's right to privacy. Consequently, the employee's right in question was thus not infringed. The principles set out in this CCMA award is akin to the provisions of section 6 of RICA.

28. **General principles of interpretation of statutes**

Professor de Ville [172] argues that a statute must be construed by applying the golden rule principle. This principle involves a process of constructing a statute according to its ordinary meaning. However, if the statute is ambiguous, the courts must apply the contextual approach. The contextual approach is applied by considering the intention of the legislature and the language of the statute. De Ville utters that the courts must also take into account: the object, preamble, the headings of the statute, the history of the statute, the commission reports as well as the surrounding circumstances.[173]

---

[171] 2002 23 ILJ 1319 (CCMA).

[172] JR De Ville (2000). *Constitutional & Statutory Interpretation* p 94.

[173] *Ibid*.

These principles had been reinforced by the court in *Venter v R*[174] wherein the court affirmed that a statute should be interpreted to give its ordinary meaning by applying the golden rule principle. Du Plessis [175]asserts that the construction of the statute in an attempt to give it its ordinary meaning would be accomplished by consulting dictionaries. In *De Beers Industrial Diamond Division Pty Ltd v Ishizuka*[176], the court averred that the use of dictionaries can only be useful to guide the courts but it would not suffice where a statute is ambiguous. The court averred that it (the court) should not rely on dictionaries but it should also consider contextual interpretation according to the circumstances of the case.

The provisions of section 39 of the Constitution provides for an interpretive tool that ought to be invoked by the courts in the process of constructing the provisions of RICA. The provisions of this section are explored fully under the constitutional interpretation discussion later in this chapter.

29. **Interpretation of RICA**

There is no doubt that the regulation of the interception of electronic communications, through RICA, EC Act, ECTA and the IMP Act, the framers of RICA intended to prohibit unlawful interception. The wording of the provisions of RICA, EC Act, ECTA and the IMP Act, in my view illustrate that the legislature intended to protect the employee's right to privacy, by setting out conditions that the employers should first fulfil before intercepting the employees' electronic communications.

29.1 **Interpretation of section 4 of RICA**

The relevant provision in respect of this section is subsection one, because it relates to the interception or monitoring of employees' electronic communications in the employment relationship context, if an employee is a party to communication.

---

[174] 1907 TS 910.

[175] Du Plessis 2002 200.

[176] 1980 2 SA 191 (T).

Section 4(1) 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 purpose of committing an offence.

It is important to note that the application of the provisions of section 39(1) of the Constitution is pertinent when considering whether or not international and foreign jurisprudence should be invoked. The application of the golden rule principle in interpreting the above provision calls upon the consideration of the meaning of the words *"any person"*. The ordinary construction of these words means that employers as well as employees, who are party to the communication may intercept such communication, without consent or knowledge of other parties to such communication. This however does not necessarily mean that journalist may intercept employees' electronic communications.

De Ville illustrates that:

> "The word *"person"* is defined as including any divisional council, municipal council, village, management board or like authority; any company incorporated or registered as such under any law; and any body of persons corporate or unincorporated".[177]

This definition is reiterated in the provisions of the Interpretation Act 33 of 1957 and there is no doubt that employers and employees are included in this definition.

The construction of section 4 of RICA implies that, if an employer is advised by either a client or a colleague about certain conduct of an employee, that is perceived to be unbecoming, and the latter had been intercepted by a party who had been party to such communication that confirms such a conduct, such an employee cannot claim the protection of the right to privacy. This would be so in my view, if the said employee does not prove the contrary.

---

[177] JR de Ville (2000). *Constitutional & Statutory Interpreta*tion p108.

As it would be seen later in this chapter, the question as to whether or not an employee who is a party to the intercepted communication, has reasonable expectation to privacy, would depend on the circumstances of each case. In *United States v Long*[178] Wagner J averred that the principle of legitimate expectation to privacy did not prohibit the limitation of the right to privacy. There was a possibility that information obtained by the interception of electronic communications, could not *per se* be regarded as private.

29.2 **Interpretation of section 5 of RICA**

The most pertinent provision on this section is subsection one. Section 5 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.

The meaning of the words in this provision in my view is that an employer may intercept an employee's electronic communications if an employee gives an employer prior consent in writing. RICA does not define *prior consent in writing*. The Oxford Dictionary[179] defines the word *"consent"* as meaning an agreement or acceptance of something.[180] It is argued that an employer could incorporate terms in the employment contract that would explicitly permit an employer to intercept such electronic communications.

Alternatively, an employer could draft explicit policies that would permit the monitoring of the employee's electronic communications. The drafting of such policies would not suffice, in my view, if employees are not made aware of the existence of same. It is argued that one of the methods or means of ensuring that employees are aware of the existence of such policies is to include a disclaimer clause in the computer system. This according to most writers should expressly inform the sender as well as the recipient that their electronic communications might be intercepted.

---

[178] 61 M.J.539.

[179] The Oxford Advanced Leaner's Dictionary 2000.

[180] *Ibid.*

It has also been argued that this would waive the employee's right to claim the protection of privacy. The use by an employee of the employers system under these circumstances would be deemed as if prior consent in writing has been given, unless he/she proves otherwise.

The Protection of Personal Information Bill provides that consent must be obtained before the interception. This affirms the principle that an employer must first obtain consent from an employee, before intercepting the latter's electronic communications. In the *NM v Smith* judgment, Madala J affirmed that "express consent is a significant factor in determining whether there has indeed been an infringement of the employee's right to privacy or not".[181] Madala J further concluded that the publication of the applicants' HIV status, without obtaining the necessary consent was indeed an infringement of their right to privacy.

This judgment, in my view, illustrates that if an employer is aware that an employee has not consented to the monitoring of his electronic communications, yet continues with such interception, that would be regarded as an invasion of the employee's right to privacy. The question is, can such prior consent in writing be regarded as unlimited? What happens if an employee gives prior consent in writing under duress? The exposition to these questions is provided in the discussion below under the constitutional interpretation. Another question is, do the said provisions include implied consent, or instances where there are no express provisions incorporated in the employment contract or where there are no policies in place, notwithstanding the provisions of section 5 and 6 of RICA?

Furthermore, do the provisions in question include instances where employees only conclude oral contracts of employment? These questions are asked because there have been instances in practice where employers had no policies in place which permits the interception of the employees' electronic communications. In addition, employees in practice in certain circumstances do conclude oral employment contracts.

[181] NM v Smith 2007 (CC).

It could be argued that the intention of the legislature was explicitly to obtain prior consent in writing but not include instances; where there are oral contracts concluded and there are implied terms in the employment contracts. The provisions of section 5 of RICA in my opinion are not vague or ambiguous. So, the answer would evidently be no, thus the intention of the legislature was not to include instances where there are implied terms in the contract or instances where oral employment contracts are concluded. It could be argued that, if an employer intercepts an employee's electronic communications without obtaining prior consent in writing and there are no policies permitting such interception, an employer cannot raise implied consent as a defense, when an employee seeks the protection of the right to privacy. Such a conduct could be regarded as an infringement of such an employee's right to privacy. Thus, would be inconsistent with the right to privacy that is entrenched in the Bill of Rights. The issue whether such a right is absolute or not is provided in the exposition under the discussion of the constitutional interpretation *infra*.

The importance of obtaining written consent in general was affirmed in *Morgan v Brittan Boustred Ltd*[182]*; Torgos Pty Ltd v Body Corporate of Anchors Aweigh*[183], the court also affirmed the importance of obtaining consent where same is required. In *Cuje-Jakoby v Kaschub*[184] the applicants were required to obtain written consent from the owners of all other units before a garage's use could be changed pursuant to the provisions of section 44(2) of the Sectional Title Act of 1986. The respondent refused to give consent.

The court found that "the objections to the change of use were fanciful and irrational and her refusal to give consent was prejudicial to the applicant". [185] These judgments are relevant because they illustrate the importance of obtaining consent when one is obliged to obtain it for whatever reason in so far as this paper is concerned; consent is required for the interception of employees' electronic communications.

[182] 1992 2 SA 775 (A).

[183] 2006 3 SA 369 (W).

[184] 2007 3 SA 345 (C).

[185] *Ibid*.

This judgment illustrates that even if employees refuse to give prior consent in writing to the interception of their electronic communications, the test that would be applied by the courts to determine whether there has indeed been an infringement of such employees right to privacy or not, would be whether or not such refusal to consent would be rational and prejudicial to the employer. This would often occur where an employer seeks to protect its intellectual property right and a certain employee is suspected of infringing such a right, at the very same time, refuses to give prior consent in writing to the interception of his/her electronic communications. Consent under such circumstances, in my view, would be deemed to have been given or obtained.

Currie & de Waal[186] are of the view that an employee waives his/her right to privacy, if he/she expressly consents to the interception of his/her electronic communications. In the *Lenco Holdings Ltd* judgment, the employee's conversation was recorded without consent or knowledge. The court affirmed the significance of applying the principle that enforces the exertion of the discretion conferred on the courts, to determine whether there had been an infringement of the right to privacy or not. In the *Tokers Bros* award the CCMA puts emphasis on the principle of obtaining consent before the interception of employees' electronic communications. Evidently, the courts as well as the CCMA show the significance of obtaining consent before employees' electronic communication is intercepted.

It has also been argued that implied consent is possible but it is difficult to rely upon. It has been argued that consent would not casually be implied, as the intent of the law is to protect individual privacy.[187] In addition, some writers express the view that consent given to the monitoring of business calls should be considered to have been given to monitoring of personal calls. This in my view is akin to the provision of section 5 and 6(1) of RICA, because business calls could be intercepted during the ordinary course of business.

An inference can therefore be drawn that the intention of the legislature was to protect an employee's right to privacy by incorporating the words *"prior consent in writing"*, before the interception is conducted by the employer.

---

[186] Currie & de Waal(2005) *The Bill of Rights Handbook* p 318.

[187] *Ibid*.

This however, should not be construed as meaning that such consent cannot be challenged, in the event that it has been obtained under duress or misrepresentation of facts, or in any manner recognised by our law, pursuant to legal defences available relating to consent. Warren Beech[188] opines that consent must be given freely and voluntarily in the terms and conditions of employment. This would address interceptions contemplated in the consent, i.e. the scope of the consent and the manner in which it is drafted requires careful consideration.[189]

Beech also denotes that:

> "Employers should amend their terms and conditions of employment to provide for express written consent. Employers cannot force existing employees to accept new terms and conditions of employment. Implied consent would be regarded as being given where employees make use of the telecommunication system after being advised through their system controller, that their communication would be intercepted". [190]

It is argued that mere consent, does not on its own waive the employee's right to privacy; a court should still have discretion to decide whether or not such consent was obtained in a manner that violated an employee's right to privacy.

In *Microsoft Corpn v Mc Donald* the court affirmed the significance of obtaining consent before intercepting an employee's electronic communications. PIPEDA in Canada also embraces the principle of obtaining consent before the interception. Moreover, the employers are required to notify employees of the interception of their electronic communications. Morgan asserts that "employee consent must be clearly obtained and a company should not monitor its employee's use of email and internet to any greater extent than is set out in its monitoring policy".[191]
Morgan also supports the view that employees should acknowledge in writing that they would conform to the terms provided in such policy, after the latter has read and understood its provisions.

---

[188] Warren Beech (2005) *The Right of an Employer to Monitor Employees' Electronic mail, telephone calls, internet and other recordings.*26 ILJ.

[189] *Ibid*.

[190] *Ibid*.

[191] Ibid.

In Australia, the Workplace Surveillance Act affirms the principle that surveillance of an employee must not commence without prior notice in writing to an employee. Prior written notice and the subsequent acknowledgement in writing in my mind can be construed as including written consent. The principles illustrated above reiterate the importance of complying with the provisions of section 5 of RICA.Thus; employees should consent to the interception of their electronic communications. The use of the word knowledge is discussed under the construction of the provisions of section 6(2) of RICA *infra*.

29.3 **Interpretation of section 6(1) of RICA**

Section 6(1) of RICA provides for the interception of electronic communications, if such interception is done in the ordinary course of business and the employer has taken reasonable steps to inform the employee of such interception. The said section 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.* (my emphasis)

The meaning of the words *"in the course of carrying of business"* is not provided in RICA. The construction of the word *"any person"* means any person may intercept an employee's electronic communications, if such interception is conducted in the ordinary course of the carrying on of any business. The interception under such circumstances could be conducted by either a client of the employer, a fellow colleague or the employer himself/herself.

In *Sage Holding Ltd v Financial Mail (Pty) Ltd*[192], the court found that "the right to carry on business included the right to regard confidential oral or written communications of directors and employees sacrosanct. Further, in appropriate circumstances, it would be entitled to enforce the confidentiality of such oral or written communication". [193]

In *Gerald Robitaille v American Biltrite (Canada) Ltd*[194], the court had to determine what was meant by the term *"ordinary course of business"*. It was argued that the overdue payment between the debtor and the creditor was not made in the ordinary course of business. The court averred that the type of the industry in which the business operates, should determine whether the interception was conducted in the ordinary course of business or not. This principle indicates that it could be an accepted standard that the meaning of ordinary course of business relates to the period before the closer of business. This could be regarded as the period between 08h00am and 17h00pm. If, it could be established that an employer in the industry operating during the said period has conducted the interception of the employee's electronic communications beyond this said period, such a conduct could be regarded as an infringement of an employee's right to privacy.

The intricacy of determining the meaning of ordinary course of business is often found in industries akin to the legal profession, where employees do not have specific standard hours they are required to work, but instead they are required to meet specific budget per annum or per month, depending on the practice of each firm. The meaning of ordinary course of business in such circumstances would be determined by the circumstances of each case and the proposed test should be *"what would a reasonable employer have done in the circumstances of the case."* The court would be required to make a value judgement in such circumstances. Moreover, some writers opine that “ordinary course of business” is a phrase used to determine the routine record keeping and other procedures applied to the maintenance of something". [195]

---

[192] 1991 2 SA 117 (W).

[193] *Ibid*.

[194] 1985 I.S.C.R 290.

[195] US Legal Definitions, http://www.definitions.uslegal.com/o/ordinary-course-of-business/.

In *Bohach v City of Reno*, the court pointed out that the interception of emails was conducted in the ordinary course of business because it was relevant to technology.[196] This according to the court limited the application of the reasonable expectation to privacy principle. The averments made by Heher J in the *Protea Technology* judgment could also be construed as meaning that the interception of the employee's electronic communications in the circumstances of this case, was conducted during the course of carrying on of the business. Heher J illustrated that "the employee in question had been appointed in the position of trust and the monitoring of his telephone conversation was conducted from the applicant's premises and during business hours.

The respondent was entitled to require the first respondent to account for his activities during its time. In addition, the employee was making use of the telephone facilities provided and paid by the applicants". [197] The question is, does the use of employer's facilities grant the latter permission to intercept the employee's electronic communications because such interception is regarded as being conducted during the ordinary carrying of the business? The exposition to this question could be found in the *Hyundai* judgment. In this case the Constitutional Court averred that "when people were in their offices, in their cars or on mobile telephones, they still retained a right to privacy." Although this averment refers to the state, it could also be construed as applying to the private parties, thus, includes employers and employees.

In addition, in the *Re an Employer's Call-Monitoring System* judgment, the court averred that the interception of telephone calls was protected by the provisions of article 8 of the Convention on Human Rights. Furthermore, in the *Watkins* judgment the court averred that "personal telephone calls may not be intercepted in the ordinary course of business under business extension exemption from liability for intercepting wire or oral communication, except to the extent necessary to guard against unauthorised use of the telephone or determine whether a call is personal or not".[198] In contrast, the employer could argue that the provisions of the Data Protection Act could be construed as meaning that same is entitled to monitor an employee's electronic communications.

---

[196] *Bohach v City of Reno* 932 F.Supp 1232 (D.Nov.1996).

[197] Protea Technology Ltd v Wainer (1997) 9 BCLR.

[198] Watkins v L Berry & Company 704 F2d 577.

It is argued that the interception of an employee's electronic communications in the ordinary course of business applies, when an employee has no knowledge of the latter, but the circumstances of the case would determine whether or not such interception violates the employees' right to privacy. Mac-Alexandre Poirier expresses the view that "information contained in email messages at work is likely to be business-related and thus less deserving of privacy protection".[199]

The provisions of the Workplace Surveillance Act in Australia, which provide that surveillance of an employee is carried out to establish whether employees are involved in unlawful activity or not while at work, could be a justification of monitoring employees' electronic communications, without their consent or knowledge. This could be regarded as an indication that the interception in such circumstances would be conducted during the course of carrying out of business. The ECPA provisions discussed in chapter three could be construed as meaning that employers may monitor an employee's electronic communications, if they can argue that they were protecting their business interest. Namely, preventing claims of vicarious liability, or infringement of intellectual property rights or likelihood of criminal liability, resulting from the use of its system by an employee. The court in the *Briggs* judgment accepted the likelihood of intercepting employee's electronic communications in the ordinary course of business.

29.4 **Interpretation of section 6(2) of RICA**

The construction of this section is discussed below and this is done by considering each provision of the subsection. Section 6(2) provides that:

---

[199] Mac-Alexandre Poirier (2002). *Employer Monitoring of the Corporate E-mail System: How Much Privacy Can Employees Reasonably Expect?* [Online]. Available http://www.law.uiuc.edu/publications/CLL-PJ/archive/vol-24/issue-3/EltisArticle24-4.

(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;

The construction of the word *"only" and "if"* illustrates that the legislature intended to set out conditions under which the employer can intercept the employee's electronic communications. Firstly, the interception can only be conducted, if the system controller either expressly or impliedly consents to the interception of the employee's indirect communication. There is no need in my mind to construe the meaning of indirect communication. The system controller in relation to this paper is regarded as the Chief Executive Officer or the Director of the company who represents the employer.

(b) for purposes of-

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

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

Another condition or limitation set out by the legislature in this section is that such interception must be conducted to establish existing facts. This could be construed as meaning that an employer may only intercept an employee's electronic communications, if there are certain allegations levelled against such an employee. This interception could be conducted to either, confirm the allegations or to further investigate the possibilities of an employee's criminal liability. In addition, employers are required to take reasonable steps to inform employees about such interception.

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

This provision is construed as justifying an investigation that is conducted to confirm the substance of the allegations about the employee. This would often be the case in the abuse of internet, namely accessing child pornography during official working hours as also illustrated by Beech and other writers.

Even if employees access child pornography after official working hours, such accessing would still be regarded as an unauthorised access because accessing pornography is regarded as a criminal offence. Thus, justifies the interception of the employee's electronic communications.

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

This provision could be construed as permitting an employer to monitoring an employee's electronic communications to evaluate his/her performance or the amount of work that is produced by such an employee.

> (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 if they so choose;

The construction of *"confidential voice telephony"* could mean to include private or confidential telephone lines or facilities provided at work by the employer. Information or evidence obtained by intercepting an employee's electronic communications in this manner could be regarded as an infringement of an employee's right to privacy; because an employee could have important reasons for utilising such private or confidential voice telephony.

> if the telecommunication system concerned is provided for use wholly or partly in connection with that business; and

The question as to whether or not an employee's communication is wholly or partly connected with that business would depend on the circumstances of each case.

(d) if the system controller has made all *reasonable efforts* to inform in advance a person, who intends to use 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.

RICA does not define the meaning of the words "*reasonable steps"*. The SALRC discussion paper asserts that the IMP Act prohibited interception of electronic communications without knowledge or consent. The South African academic writers point out that employers should give notice to employees about the likelihood of the interception of their electronic communications. It might therefore be prudent to draft explicit policies that permit employers to monitor employees' electronic communications, as articulated by the writers referred to in this paper. It is contended that employers should ensure that employees sign some form of a declaration that affirms the knowledge of such monitoring, as averred by academic writers. These policies could be incorporated as an annexure(s) in employment contracts and these should simultaneously be signed by employees at the commencement of the employment contracts. It is argued that the courts should consider *what would a reasonably employer have done in the given circumstances*, to determine whether the employer has conformed to the provisions of the section in question.

One could argue that this could be accomplished by applying the *boni mores* principle. Thus, the courts must determine what would the legal conviction of a community regard as reasonable steps in each circumstance. In *Warwick University v De Graaf*, the court averred that the issue whether or not the employer had taken reasonable steps to advise the employee about the interception of the latter's electronic communications, would be determined by the circumstances of the case. It has been suggested by the academic writers that "reasonable steps include considering the size of the organisation against which a complaint that is made. In addition, the efforts include information and training made to ensure that staff knows of its existence and are familiar with its contents". [200]

[200] *Ibid.*

Section 16 of the Protection of Personal Information Bill also affirms that employers must take reasonably practicable steps to notify employees of the interception of their electronic communications. It is submitted that, if it has been a practise (as per Mac-Alexandre Poirier's views discussed in chapter three of this paper) to monitor employee's electronic communications and such interception is an integral part of the ordinary course of business, it would be deemed as if the employer took reasonable steps to notify of the interception, unless the employees prove otherwise. This could often occurs, if the banks or other financial institutions are employers wherein all telephone conversations are recorded and the clients are informed of such interception.

In the *Copland* judgment the court affirmed the significance of the obligation placed on employers to take reasonable steps to notify employees of the interception of their electronic communications. The court in *Schoewengerdt v General Dynamics Corp* correctly decided that "an employee had a reasonable expectation to privacy in work areas of exclusive use to the employee, such as the employee's office, unless the employer had previously notified the employee that the employee's office was subject to a work-related search on a regular basis".[201]
In *R v M*, the court held that "knowledge of the interception of one's communication diminishes one's reasonable expectation to privacy, and it is pertinent to illustrate the importance of ensuring that reasonable steps are taken to inform employees of the interception of their electronic communications". [202]

Moreover, PIPEDA in Canada reinforces the principle that employers must notify the employees of the interception of their electronic communications. Further, this would most probably be achieved by taking reasonable steps to inform employees of such interception. This principle is supported by Mac-Alexandre Poirier in chapter three of this paper and this writer expresses the view that employees, who are aware of the interception of their electronic communications, do not necessarily have a legitimate expectation to privacy.

[201] The Publishing Law Center, *The Right to Privacy* [Online] Available http://www.publaw.com/privacy.html.

[202] R v M 2005 BCSC 385.

Eisselaar opines that the clients must also be advised about the interception of electronic communications at the workplace. “Some ways of putting this into practice include email disclaimers and automated telephone messages indicating that the conversation may be recorded".[203]

Section 6(2) of RICA is pertinent in the application of the provisions of item 7 of schedule 8 of the LRA, because the latter requires that employers should only institute disciplinary proceedings against employees if such employees have broken an existing rule. Further, an employee must have been made aware of the existence of such a rule or such an employee ought to reasonably be aware of the existence of such a rule.

It is submitted that contextual interpretation of RICA may also be applied by the courts. This could be accomplished by considering RICA in its entire context, having due regard to its object or the purpose and the language of the statute. It might also be prudent to consider the provisions of the RICA Bill, which led to the promulgation of RICA. In addition, the provisions of the IMP Act might also be considered together with all the judgments decided under this Act. This would enforce the principle of judicial precedent. It could be necessary to take due regard the provisions of the EC and ECT Bills, which led to the promulgation of these two Acts.

Moreover, it could be important to consider the SALRC discussion papers relating to the prohibition of electronic communications monitoring or interception in light of protecting the right to privacy. Craig Bosch[204]avers that the contextual interpretation of statute can be accomplished by considering the language of the statue, the scope and purpose of the statute and this has been accepted by the courts. The courts therefore should not narrowly construe the provisions of RICA. The issue of whether or not the employee has a reasonable expectation to privacy would be determined by balancing the two competing rights. Thus, the employee’s right to privacy on the one hand and the employer’s right to trade freely on the other hand.

---

[203] *Ibid*.

[204] C Bosch (2006) *Can Unauthorized workers be regarded as employees for the purpose of the Labour Relations* Act? 27 ILJ 1342.

This balance is achieved by considering the constitutional interpretation in the discussion that follows.

30. **Constitutional interpretation**

The protection of the right to privacy is entrenched in section 14 of the Constitution. This right must be balanced with the right of an employer to trade freely as provided in section 22 of the Constitution. Section 8 of the Constitution provides that the Bill of Rights applies both horizontally and vertically. The horizontal application of the Bill of Rights is pertinent in this paper because it relates to the relationship between private parties, thus, an employer and an employee. As previously indicated, the courts as well as the writers embrace the notion that rights are not absolute and this limitation is provided in 36 of the Constitution.

Currie & de Waal (2005) Bill of Rights Handbook, assert that the courts apply the provisions of section 36 of the Constitution to balance the competing rights. The courts also take into account the scope of the right in order to determine whether the right to privacy has been infringed or not. Currie & De Waal state that there are two methods of interpreting the provisions of the Constitution. These are; purposive and generous interpretation. The difference between these is that purposive interpretation considers the core values of the Constitution. Whereas, generous interpretation considers the interpretation that would be in favour of the protection of the rights to those who seek the protection of the right in question than restricting it.

In Volume 10(1) of LAWSA, it is argued that purposive interpretation is embraced by the Canadian Courts because it reinforces the protection of the rights provided in the Constitution.

It would be correct in my view to apply a purposive approach when constructing the provisions of RICA. This is due to the fact that the right to privacy has been recognized under the protection of the right to human dignity, which has been regarded as the core value of one of the fundamental rights. The effect of applying the purposive interpretation in constructing RICA would be that employees' right to privacy in so far as the right relates to the interception of their electronic communication would be protected. It must now be determined whether RICA satisfies the limitation clause test. This is achieved by considering the provisions of section 39(2) as well as section 36 of the 1996 Constitution.

Section 39(2) provides that:

> When interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights.

The application of the provisions of this section could be accomplished by interpreting the statute in a manner that ensures that the provisions of section 39(2) of the Constitution are conformed to when statutes are interpreted. The meaning of this provision illustrates that when the courts interpret the provisions of RICA, they should do so by promoting the spirit, purport and the objects of the Bill of Rights.

Section 36 of the Constitution provides that:

> The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including -
>
> (a)the nature of the right;
> (b)the importance of the purpose of the limitation;
> (c)the nature and extent of the limitation;
> (d)the relation between the limitation and its purpose; and
> (e)less restrictive means to achieve the purpose.
> (2) Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.

RICA is regarded as a law of general application in my view regardless of the fact that the Act itself does not expressly state so. Currie & de Waal[205] assert that the court must apply the principle of the rule of law to determine whether or not the statute passes the limitation clause test provided in section 36 of the Constitution. Therefore, the limitation of the Bill of Rights must be in accordance with the law of general application as provided in section 36 of the Constitution.

[205] Currie & de Waal (2005)

Currie & de Waal further articulate that the test that determines whether the law is of general application or not is whether the law is sufficiently clear, accessible and precise. This precision must enable those who would be affected by its application to determine the extent of the protection of their rights.

In applying the above principles, RICA is in my view, a law of general application. This view is expressed regardless of the fact that RICA does not expressly provide that same applies to all. An inference is drawn from the use of the words *"any person*" or *"no person"*. These words are construed as meaning that the intention of the framers of RICA intended that same should apply to all. The question is, whether or not RICA is reasonable and justifiable in an open and democratic society or not. It could be argued that same is reasonable and justifiable. The reason for expressing this view stems from the incorporation of the conditions or limitations set out in section 4, 5 and 6 of RICA, which ought to be conformed to by employers before intercepting employees' electronic communications.

Namely, the use of the words "*prior consent in writing", "if", "only", "ordinary course of business", "express or implied consent" and "taking reasonable steps"*. Not only that, it is my contention that there are no arbitrary provisions that have been identified in RICA, save for the lack of the protection of the employee's rights to privacy. It is therefore argued that RICA satisfies the first part of the provision of section 36 of the Constitution. This however is subject to the consideration of the factors that are provided in the same section and these are discussed below.

30.1 **The nature of the right**

Currie & de Waal[206] indicate that the courts must apply the proportionality test to balance the two competing rights, by taking into account the context of the statute that limits the Bill of Rights. The circumstances of the case would determine which right must be overridden. This principle was affirmed by the Constitutional Court in *S v Makwanyane*.

[206] Currie & de Waal 2005 178.

The nature of the right to privacy in my view requires that one should first have a legitimate expectation to privacy before she or he can claim the protection of such a right. In the *Bernstein* judgment Ackerman J averred that “the truism that no right is to be considered absolute implies that from the outset of interpretation, each right is always already limited by every other right accruing to another case.” [207]

This principle to my mind could be regarded as meaning that an employee's right to privacy is already limited by an employer's right to trade freely. Further Ackerman J averred that “privacy is acknowledged in the truly personal realm, but as soon as a person moves into communal relations and activities, such as business and social interaction, the scope of personal space shrinks accordingly".[208] This in my view could be construed as meaning that an employee's right to privacy is limited as soon as same moves away from his/her home. The trite principle of a legitimate expectation to privacy was further affirmed by the Constitutional Court in the *Mistry; Magajane* judgments referred to in chapter two of this paper and the *Hyundai* judgment.

In the *Mistry* judgment, Chaskalson P affirmed that "the scope of a person's privacy extends only to those aspects to which a legitimate expectation of privacy can be harboured".[209] Chaskalson P went further and found that "a regulated business' right to privacy was attenuated the more its business was public, closely regulated and potentially hazardous to the public".[210]

In the *Magajane* judgment, the issue before Van Der Westhuizen J was whether or not the statute authorising the regulatory inspection infringed the right to privacy. Van Der Westhuizen J concluded that the application of the provisions of section 36 of the Constitution would guide the court to determine whether the right to privacy had been infringed or not. Van Der Westhuizen J averred that the circumstances of the case would confirm whether or not the limitation of the right to privacy is reasonable or justifiable pursuant to the provisions of section 36 of the Constitution.

---

[207] Bernstein v Bester NO 1996 2 SA 751 (CC).

[208] *Ibid*.

[209] Mistry v Interim National Medical and Dental Council of South Africa 1998 4 SA 1127 (CC).

[210] *Ibid*.

The question is, do the provisions of section 4, 5 and 6 of RICA constitute a significant intrusion on the employee's right to privacy? The answer in my mind is yes, unless the employer fails to conform to the said provisions. It could also be argued that the circumstances of the case would determine whether or not RICA constitutes a significant intrusion on an employee's right to privacy.

In *Financial Mail v Sage Holdings* Corbett CJ found that a person's right to privacy is infringed, if there is an unlawful intrusion of personal privacy or disclosure of private facts.[211] In the *Protea Technology* judgment Heher J affirmed that the application of the principle of legitimate expectation to privacy determines the extent of the scope of the right sought to be protected. In *Moonsamy v The Mailhouse*, although this case only has a persuasive value, Commissioner Van Dokkum averred that the nature of the employee's right to privacy was such that same had a legitimate expectation to privacy. The interception of the employee's telephone calls was a violation of the latter's right to privacy. Therefore, such interception did not pass the limitation clause test provided in section 36 of the Constitution.

In *S v Dube* Mc Call J averred that interception of the communication of employees who were involved in criminal or corrupt activities was not a violation of such employee's right to privacy. Consequently, these employees did not have the legitimate expectation to privacy. The limitation of the right in question according to Mc Call J was thus reasonable and justifiable. The conclusion drawn from this discussion is that employees who are engaged in criminal activities cannot claim that they have a legitimate expectation to privacy.

The limitation of their right to privacy would be justified if the evidence that shows the involvement in criminal activity is presented, which had been obtained by intercepting the employees' electronic communications.

[211] Financial Mail v Sage Holdings Ltd (1993)2 SA 451(A.)

30.2 **The importance of the purpose of the limitation**

Currie & De Waal (2005) Bill of Rights Handbook argue that the importance of determining the purpose of the limitation of the right to privacy is illustrated by the application of the standard of reasonableness. The limitation of the right would be justified, if such limitation is reasonable and justifiable in an open and democratic society in accordance with the provisions of section 36 of the Constitution. It is argued that it is pertinent in an employment relationship context, to take into account the interests of the employer, notwithstanding the protection of the employee's right to privacy. An employer has a right to protect himself from defamatory claims or vicarious liability claims or intellectual property infringement claims. The question is, does this mean that the interception or monitoring of the employee's electronic communications is reasonable and justifiable?

Taking due regard the provisions of RICA, it could be argued that by virtue of the use of the words such as " *prior consent in writing"* or *"a person may only intercept an indirect communication*" the framers of RICA contemplated the likelihood of the infringement of an employee's right to privacy by an employer, through the interception or monitoring of the latter's electronic communications, hence these words are incorporated in these provisions. The incorporation of these words to my mind could be regarded as an indirect enforcement of the protection of the employee's right to privacy.

In the *Moonsamy* CCMA award it was argued that the employer was entitled to protect its business interests by monitoring the employee's electronic communications. This according to the employer would enable "its financial self-preservation."[212] Commissioner Van Dokkum put emphasis on the protection of the employee's right to privacy in the workplace and applied the principles set out in the *Protea Technology* judgment. In the said case, Heher J identified the competing interests between the employee and the employer, as the employee's right to privacy versus the employer's right to economic activity. Heher J concluded that the protection of the employer's right to free economic activity that had been provided in the Interim Constitution was no longer incorporated in the provisions of the 1996 Constitution.

[212] Moonsamy v The Mailhouse (1999) 20 ILJ 464 CCMA.

Section 22 now provides that employers have a right to trade freely. The construction of these provisions according to Heher J affirms the intention of the legislature. This in my view means that the protection of the right to privacy should carry more weight than the protection of the right to trade freely. This averment should be considered when our courts invoke the contextual application in constructing the provisions of RICA. This analogy in my view denotes that the intention of the legislature was to protect the employee's right to privacy more than the interest of the employer. Thus, the employee's right to privacy could be regarded as overriding the employer's right to trade freely.

Does this imply that an employee's right to privacy would always override the employer's right to privacy? The answer is evidently no because the courts have averred that the circumstances of each case must be considered to determine whether or not there has indeed been an infringement of the right to privacy. This principle has also been supported by most writers.

30.3 **The relation between the limitation and its purpose**

Currie & de Waal (2005) Bill of Rights Handbook, indicate that the application of the legitimate expectation to privacy principle places an obligation on those who intend or contemplate to limit any person’s right to privacy, in any manner, to ensure that such limitation is reasonable and justifiable. “There must be a good reason for the infringement.”[213] This principle illustrates that it could be argued that there is a good reason why the provisions of section 4, 5 and 6 of RICA were incorporated in RICA. This reason was to protect both the employer's right to trade freely and the employee's right to privacy. The conditions or provisions that are set out in section 4, 5 and 6 of RICA, are an indication that it is prudent to limit the rights in question when circumstances call upon such limitation. These conditions in my view illustrate that the intention of the legislature was to balance the conflicting rights by incorporating such provisions in RICA. It can therefore be argued that an employee waives his/her right to privacy; if it is proved that the provisions of section 4, 5 and 6 of RICA are conformed to by the employer.

[213] Currie & de Waal 2005 183.

Article 29 of the Data Protection Working Party (2002) Working Document on the Surveillance of Electronic Communications in the Workplace, asserts that employees do have legitimate expectation to privacy at the workplace. These employees do not necessarily waive their right to privacy by virtue of being in the premises of the employer. The courts ought to apply the proportionality test as illustrated in the above discussion to determine, which of the competing rights override the other.

In the *Moonsamy* CCMA award Commissioner Van Dokkum found that the interception of the employee's electronic communications did not pass the limitation clause test pursuant to the provisions of section 36 of the Constitution. The rationale behind this finding was based on the fact that the employer had other means of obtaining evidence against the employee. The interception was therefore not justifiable. This implies that if an employer may only obtain evidence against an employee by intercepting his/her electronic communications, there would be a relation between the limitation of an employee's right to privacy and its purpose. It might thus be argued that RICA does satisfy the limitation clause test provided in section 36.

30.4 **Less restrictive means to achieve the purpose**

Currie & de Waal (2005) Bill of Rights Handbook, argue that the success of the application of the above factor would be accomplished by applying the proportionality test. If employers have other less restrictive measures to obtain evidence against an employee, the interception of the employee's electronic communications, would not pass the proportionality test provided in the provisions of section 36 of the Constitution.

In the *Moonsamy* CCMA award, Commissioner Van Dokkum averred that there was an infringement of the employee's right to privacy because the employer had other restrictive means to obtain evidence against such employee. In the *Makwanyane* judgment, the Constitutional Court found that, "where other methods of achieving these purposes exist that do not impose the same costs, it becomes difficult to claim that the method chosen is reasonable and justifiable".[214]

[214] S v Makwanyane 1995 3 SA 391 (CC).

Currie & de Waal argue that "the proportionality principle requires that personal data including those involved in monitoring must be adequate, relevant and not excessive with regard to achieve the purpose specified".[215]

It is argued that if an employer can obtain evidence against an employee by other means, but still continues to intercept such an employee's electronic communications, the conduct of such an employer would not satisfy the limitation clause test. This occasions when other employees can testify that they have observed that the employee who is subjected to the disciplinary proceedings, has abused the employer's electronic communications, by spending 80% of his/her time during working hours accessing pornography or child pornography. An employer in this instance would be regarded as having other less restrictive means of obtaining evidence against such an employee, as fellow employees could be subpoenaed to testify in the disciplinary proceedings.

It could however be argued that this does not fetter the inherent power of the court to exercise its discretion. This means even if it could be established that the employer had other less restrictive means to obtain evidence against the employee, and the court is satisfied that the failure to monitor such electronic communications under such circumstances would prejudice an employer in any manner, the court can still find that such an employee's right to privacy has not been infringed.

31. **Conclusion**

It is evident that both employers and employees have common law rights and/or obligations by virtue of the conclusion of the employment contract. This principle is articulated and reiterated in the provisions of the LRA. The horizontal application of the Bill of Rights affirms the relationship between the protection of the employer's rights to privacy and the employee's right to trade freely.

[215] Currie & de Waal 2005 184.

It is also evident that an employer may intercept an employee's electronic communications, if the latter is aware or ought to be aware of such interception pursuant to the provisions of schedule 8 of the LRA.

It is evident that the Promotion of Access to Information Act confers rights on an employee, whose electronic communications are intercepted by the employer, to have access to such information. It is also evident that the courts and jurisprudence affirm that the protection of the right to privacy is not absolute. The test that is applied by the courts to determine the nature and scope of the right to privacy is whether or not an employee has reasonable expectation to privacy and this would depend on the circumstances of the case.

It is observed that the wording of the provisions of section 4 of RICA indicates that an employer may only intercept an employee's electronic communications, if the latter is a party to communication. In addition, prior consent in writing pursuant to section 5 of RICA, is required to monitor the employees' electronic communications. Consent can be obtained in various ways and one of the methods is to incorporate a consent form or document as an annexure in the employee's contract of employment. The other method includes obtaining an acknowledgement in writing from an employee, wherein one of the terms of the oral contract concluded expressly waives an employee's right to privacy in so far as the interception of electronic communications is concerned. Such acknowledgment could be regarded as prior consent in writing.

It is argued that, if it is established that the employer has not obtained consent from an employee, to intercept or monitor such employee's electronic communications, or if the interception has not been conducted in the ordinary course of business, and the employer failed to take reasonable steps to inform the employee of such interception, the conduct of such an employer would be regarded as an infringement of the employee's right to privacy. Furthermore, the provisions of section 51 of RICA would apply. Thus by failing to conform to the provisions of section 6(2), the employer would be guilty of an offence. It is submitted that, even if consent has been obtained under duress or based on misrepresentation of facts, the conduct of an employer would be regarded as an infringement of such an employee's right to privacy.

On the other hand, it could be argued that, if an employer does not conform to the requirements set out in section 4, 5 and 6 of RICA, but continues to intercept employees' electronic communications, such conduct cannot not be regarded as an invasion of the employees' right to privacy, if the court is satisfied that the failure to intercept such electronic communications, would prejudice the employer.

It is observed that RICA satisfies the limitation clause test pursuant to section 36 of the 1996 Constitution. It is observed that the court should not limit itself by narrowly constructing the provisions of RICA. Contextual interpretation should also be invoked, if the circumstances of the case call upon the application of same. The fact that RICA satisfies the limitation clause test in section 36 of the 1996 Constitution does not however mean that same cannot be challenged. The circumstances of each case would determine whether or not the infringement would be reasonable and justifiable in an open and democratic society, taking due regard the factors provided in section 36(1)(a) to (e) of the 1996 Constitution.

It is also evident that section 39(1) and 39(2) must be invoked when our courts construe the provisions of RICA. It is observed that purposive interpretation appears to be appropriate in the construction of the provisions of RICA. Taking due regard the above, do you consider your employer as conforming to the provisions of section 4, 5 and 6 of RICA? If the answer is no, do you think that your right to privacy is invaded by your employer?

The international instruments and jurisprudence discussed in this chapter and the previous chapters are important to determine whether or not RICA satisfies the limitation clause test in 36 of the 1996 Constitution. These instruments and jurisprudence affirm the principle of obtaining consent before intercepting one' electronic communications. In addition, one is required to give notice to employees whose electronic communications would be intercepted. These principles are akin to the provisions of section 5 and 6 of RICA. It has also been pointed out that the international courts consider whether or not one has a legitimate expectation to privacy when the protection of the right to privacy is sought.

CHAPTER FIVE

32. Introduction

"The right to privacy entrenched in section 14 of the Constitution, recognizes that human beings have a right to have a sphere of intimacy and autonomy that should be protected from the invasion". [216]This chapter illustrates the findings and recommendations based on the principles that are illustrated in the previous chapters. As the closing point, a copy of a draft proposed regulations is provided at the end of this chapter.

33. General findings

It is observed that the right to privacy has been recognized and protected by both common law as well as the Interim Constitution. This protection is now entrenched in section 14 of the 1996 Constitution. It has been argued by writers that this right is however not absolute, as it is subject to the limitation clause test provided in section 36 of the 1996 Constitution. It is observed that before an employee seeks the protection of the right to privacy he/she must first have a legitimate expectation to privacy.

A classical example would be in instances where an employee received an email from either his friend or family member that is marked private and confidential, and the employer intercepts such communication. Such interception would be regarded as an infringement of such an employee's right to privacy. Thus, an employee in such circumstances has a legitimate expectation of the right to privacy. If, however, an employee participates in any criminal activity with other parties and one of the parties intercepts such an employee's electronic communications, such interception would not be regarded as an infringement of such an employee's right to privacy. It is argued that an employee in such circumstances would not have a legitimate expectation to privacy.

---

[216] Tshabala-Msimang v Mondli Mkhanya Case No: 18656/07 (CC).

It is further observed that if the interception is conducted by a person who is not party to a communication, where an employee is a party to such communication, and the evidence against such an employee, is obtained by such interception, and the evidence is submitted to an employer for whatever reasons, such interception would be regarded as an infringement of such an employee's right to privacy. The interception in this circumstance would not fall within the provisions of section 4 of RICA, unless the contrary is proved.

It is observed that if an employer obtains prior consent in writing from an employer and such consent has been obtained under duress, the interception in such circumstances would be regarded as an infringement of such an employee's right to privacy. This would often be the case in instances where an employer forces an employee to give prior consent in writing, and where there are no policies in place to permit such interception nor terms incorporated in the employment contract that permit such interception.

Moreover, it is my contention that, where the interception of an employee's electronic communications is not conducted in the course of carrying business by an employer, such interception would be regarded as an infringement of an employee's electronic communications, unless same conforms to section 4 and 5 of RICA. This occasions where an employee accesses internet during the course of a weekend, and he/she is not contractually obliged to work on weekends, thus his/her working hours fall in the period between 08h00am to 17h00pm from Monday to Friday. Such interception would be regarded as an infringement of such an employee's right to privacy.

Another classical example is when the interception is not related to employers' business, namely an email marked private and confidential that is sent to an employee by his/her bank manager, and such an employer intercepts same that would constitute an infringement of such an employee's right to privacy.

Section 6(2) of RICA requires that an employer should take reasonable steps to inform an employee about the interception of his/her electronic communications. As previously pointed out, RICA does not define reasonable steps. It has been established from the discussion in previous chapters that; reasonable steps include instances where an employer has drafted policies and make these known to employees. It has been asserted that employees should sign these policies after reading them and this would be regarded as reasonable steps. It is my contention that it is pointless to have policies in place which employees are not aware about. It is observed that reasonable steps would also include instances where an employer incorporates a disclaimer clause in the employees' computer system, which informs employees that the latter's right to privacy would be waived by continuing to utilize such computer.

It is further observed that if an employer incorporates terms in the employee's contract of employment, which illustrates that an employer would be subject to the policies and procedures of the company without the express provisions that permit the employer to intercept such employees' electronic communications, nor without obtaining the necessary prior consent in writing from such employees, the incorporation of such terms on its own could be regarded as constituting reasonable steps. Thus, an employer would be regarded as if he/she has conformed to the provisions of section 6(2) of RICA. It has been articulated that an employer who notifies his/ her employees in any manner, that their electronic communications would be intercepted, such an employer would be deemed to have taken reasonable steps pursuant to the provisions of section 6(2) of RICA. It has been argued on the other hand that not all rules and policies have to be made known to employees, sometimes employees must use common sense and this should be weighed against the standard of reasonableness.

34. **Findings based on international and foreign law**

It is observed that Article 8 of the International Conventions recognizes and protects the right to privacy. The European courts have asserted that telephone calls received on private or business premises are covered by the notion of private life and correspondence, within the meaning of Article 8 of the International Convention.

Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights, as well as Article 7 of the Data Protection Convention also protect the right to privacy. It is also observed that the Directives do protect the right to privacy, notwithstanding the fact that these are not regarded as the law.

The Data Protection Act seeks to protect the right to privacy in the UK. This is illustrated by incorporating consent and knowledge as requirements for the interception of electronic communications. The UK courts as well as international jurisprudence maintain the enforcement of the principle that an employee should first have a legitimate expectation to privacy before he/she can claim the protection of such a right. The circumstances of each case would determine whether an employee's right to privacy has been infringed or not, by the interception of his/her electronic communications.

In the USA, the Fourth Amendment and the ECPA protects the right to privacy but at the same time it provides for few exceptions, namely business exception and consent. It is observed that employees waive their right to privacy if they give employers consent to the interception of their electronic communications. The same principle applies where an employee is aware of or has knowledge of the interception of his electronic communications. The US jurisprudence illustrates that, "if the monitoring is conducted within the regular course of an employer's business and the employer has vested interest on the subject-matter that would be regarded as the business exception".[217] This is akin to the provisions of section 6(1) of RICA which provides that an employer may intercept an employee's electronic communications, if such interception or monitoring is conducted in the ordinary course of business.

The USA courts have asserted that if an employer or any person intercepts employees' electronic communications same must be conducted in terms of the law. Thus, employers may not intercept employees' electronic communications just for the sake of doing so without the necessary authority.

[217] *Ibid.*

In addition, consent according to the USA courts cannot be casually implied because the framers of the legislation intended to protect the right to privacy. Furthermore, an employee who has consented to the monitoring of calls for business purposes should not be considered to have given consent to monitoring of personal calls.

The USA writers opine that the interception of an employee's electronic communications, gives an employee constant feeling that he/she might be watched and this might affect his/her dignity. This could somehow affect the quality and quantity of the performance. In addition, the USA courts do not readily protect an employee's right to privacy, unless he/she has an objective expectation to privacy. The USA courts have found that employers have the right to protect their business by monitoring employees' use of electronic devices. Furthermore, some writers also express the view that "an expectation of privacy also need not be an expectation that the subject item or information is completely private from all third party knowledge". [218]The right to privacy is then limited based on the circumstances of the case.

In Canada the protection of an employee's right to privacy is provided in the Canadian Charter; PIPEDA and the Privacy Act. It is uttered by Canadian writers that PIPEDA provides that employees should consent or have knowledge of the interception of their electronic communications. The Canadian writers further articulate that "knowledge of the interception diminishes one's reasonable expectation to privacy. Consent is a factor in determining the reasonableness of personal data, collection and dissemination, and the standard of reasonableness must be present in any restriction upon an employee's right to privacy."[219]

Some writers opine that information contained in “email messages at work, is likely to be business-related and thus less deserving of privacy protection.”[220] The Canadian courts had averred that employers' legitimate business interests must be balanced against an employee's concern.

---

[218] *Ibid.*

[219] *Ibid.*

[220] *Ibid.*

The test that is applied by the Canadian Courts is based on the principle that affirms that an employer must exhaust all available alternatives before he/she intrudes on an employee's right to privacy. This principle is akin to one of the factors provided in section 36 of the Constitution. Some writers argue that section 8 of the Canadian Charter reinforces the notion that an employee should have a reasonable expectation to privacy. It is an offence in Canada to willfully intercept private communication by means of any electronic device, save for the interception wherein a party to the communication has consented. These Canadian principles are akin to the provisions of RICA.

Further, some Canadian writers express the view that "if employees are advised of the circumstances in which their email may be intercepted, their reasonable expectation to privacy would significantly be diminished, if not completely negated."[221] This appears to be similar to the provisions of section 6(2) of RICA, which requires an employer to take reasonable steps to inform an employee of the interception of his/her electronic communications. Writers are divided on whether or not employees can personally expect that workplace email would remain private or not. It has been contended that that "employee consent ought to be clearly obtained and the monitoring of an employee's email must be to the great extent that is set out explicitly in the employers' monitoring policy". [222]

In Australia, the Privacy Act regulates the interception of an employee's electronic communications. Furthermore, the Workplace Surveillance Act regulates the surveillance of an employee and this Act provides that interception or surveillance must not be commenced without prior notice in writing to the employee. This principle seems to be akin to the provisions of section 6(2) of RICA.

[221] I*bid.*

[222] *Ibid.*

35. The relationship between an employer and an employee

It is observed that the provisions of the LRA reinforce the contractual obligation on both the employer as well as the employee. South African courts had averred that employees ought to render their services to the employee honestly and faithfully. This according to the South African courts could be accomplished by avoiding conflict of interests in the workplace, which could consequently, damage the relationship. The courts have also affirmed that they would not readily protect the right to privacy, if an employee abuses the employer's internet or email facilities.

Further, the South African courts have averred that, if the interception of an employee's electronic communications is "not malicious but incidental to the investigation into the abuse of internet facilities"[223], the courts would not regard the interception as an infringement of an employee's right to privacy. It is observed that the Promotion of Access to information Act, gives an employee whose electronic communications are intercepted, a right to access to information held by his/her employer.

The South African courts had also affirmed that employees should use their common sense at times because the rules do not necessarily need to be made known to employees. This could be regarded as conflicting with the schedule 8 provisions of the LRA, which provide that employers may only take disciplinary measures against an employee, if, such an employee has broken an existing rule that he has been made aware of. The same courts expressed the view that the level or degree of expectation relating to the application of the employee's common sense to those employees who are employed in managerial positions is much higher than those employed as ordinary employees.

[223] *Ibid.*

36. **Recommendations based on interpretation of RICA**

It is submitted that the interpretation of the provisions of RICA requires both the application of the golden rule principle as well as the contextual interpretation approach. The application of these principles would however vary according to the circumstances of each case. As RICA has not yet been tested, it is my contention that the wording of section 4 of RICA, illustrates that an employee's electronic communications may be intercepted by an employer himself/herself, colleague or employer's client who are party to such communication.

It is further submitted that the incorporation of the words *"prior consent in writing"* in section 5 of RICA is an illustration that this consent does not include instances, where an employee has concluded an oral contract of employment and same has given such prior written consent under duress. It is also observed that there are no provisions in RICA that provide for the possibility of withdrawing or terminating such consent, when it is established that an employer misrepresented facts to an employee, at the time when such consent was given. It is my contention that where there are no written policies in place and an employee has no knowledge of the interception of his/her electronic communications, such interception would be regarded as an infringement of such an employee's right to privacy.

It is recommended that the use of the words *"if"* and *"only"* in the provisions of RICA denotes that that the intention of the legislature was to limit the right to privacy, at the same time, limit the right of an employer to trade freely when same intercepts the employee's electronic communications. It is also submitted that the interception of an employee's electronic communications may be permitted, if the system controller either expressly or impliedly gives consent. In addition, the interception of the employee's electronic communications may be conducted to investigate existing facts or unauthorized use of the employer's facilities. This would often happen, if an employee is being investigated by the employer for abusing the latter's internet or email or for any other reasons relating to alleged misconduct.

It is submitted that the application of contextual interpretation of RICA involves a process of considering the intention of the legislature, the language of the statute, the purpose of the statute and the provisions of RICA in the entire context. This process would further require the consideration of the provisions of the IMP Act, as well as the Protection of Personal Information Bill or any other legislation that regulates the interception of electronic communications. If the Bill becomes law, the courts would be required to apply its provisions. These provisions appear to be akin to the provisions of section 51 of the ECTA. Further, an employer is also required to ensure that electronic communications interception or monitored by such an employer is kept confidential. It is my contention that the provisions of section 51 of the ECTA are reinforced by the guidelines provided in the Bill.

37. **Recommendations relating to the Protection of Personal Information Bill**

It is submitted that the Bill reinforces the provisions of section 14 of the Constitution. Further the same Bill articulates the significance of obtaining consent and informing employees about the interception of their electronic communications. The Bill also reiterates that those who intend or contemplate to intercept other persons' electronic communications should take reasonable steps to inform them that their electronic communications would be intercepted. It is also noted that the Bill requires that "reasonable steps be taken before the information is collected or, if that is not reasonably practicable possible as soon as reasonably practicable after the information is collected".[224] In addition, "the processing must be necessary for upholding the legitimate interests of the responsible party or third party to whom the information is supplied". These provisions of the Bill are akin to the provisions of section 51 of the ECT Act.

It is submitted that section 14 of the Bill provides guidelines that ought to be considered before the interception is conducted, that the courts must consider when constructing the provisions of RICA, to determine whether or not there has been an infringement of the employees' right to privacy.

[224] The Protection of Personal Information Bill.

38. **Recommendation relating to the approach that ought to be followed by the courts in protecting the right to privacy**

It is submitted that our courts should reiterate the significance of obtaining consent when it is legally or otherwise necessary to do so. Further, the Constitutional Court in the *Hyundai* judgment has affirmed that "when people are in their offices, cars or mobile telephones, they still retain a right to be left alone".[225] The courts had averred that *ordinary course of business* "included the right to regard confidential oral or written communication of directors and employees sacrosanct". [226]

It is further submitted that the test that should be applied by the courts to determine whether or not there has indeed been an infringement of an employee's right to privacy, in instances where there is refusal of consent, should be "whether such refusal would be rational and prejudicial to an employer or not".[227] Jurisprudence articulates that employees limit the application of the protection of their right to privacy, if same consent to the interception of electronic communications. It is further submitted that the court should not readily find for employees who are involved in criminal or corrupt activities. Evidence obtained by the interception of employees' electronic communications, would therefore be admissible in these circumstances. Each case however, should be adjudicated based on its own merits. Ultimately, the court should still exercise its discretion to determine whether or not there has been an infringement of the right to privacy.

[225] *Ibid.*

[226] *Ibid.*

[227] *Ibid.*

39. **Recommendations in light of constitutional interpretation**

It is submitted that the constitutional interpretation of RICA requires the balancing of the competing rights, in order to determine whether or not an employee's right to privacy has been infringed. Thus, the employer's right to trade freely and an employee's right to privacy should be balanced. This would be achieved by ascertaining whether the infringement of an employee's right to privacy would be reasonable and justifiable in an open and democratic society or not. It is submitted that RICA is a law of general application therefore same is reasonable and justifiable in an open and democratic society, but the circumstances wherein the interception of employees' electronic communications is conducted, should determine whether or not RICA passes the limitation clause test pursuant to the provisions of section 36 of the 1996 Constitution.

It is submitted that the interception of employees' electronic communications should not pass the limitation clause test, if the employer has other means of monitoring the employees' performance or obtaining evidence of misconduct against employees. It is submitted that purposive interpretation is more appropriate in constructing the provisions of RICA, because the application of purposive approach affirms the trite principle that the right to privacy is one of the fundamental rights that is entrenched in the 1996 Constitution.

It is submitted that the application of the provisions of section 39 of the Constitution requires the courts to apply international and foreign law instruments and jurisprudence to interpret the provisions of RICA. It is further observed that our courts have previously considered and applied previous judgments that had been decided under the provision of the IMP Act wherein the protection of the right in question was sought. This illustrates the significance of the application of the principle of judicial precedent. It is submitted that if, an employer conforms to the provisions of section 4, 5 and 6 of RICA, before conducting the interception of an employee's electronic communications, the latter's right to privacy would not be infringed.

The exception would be in instances where there has been misrepresentation of facts and/or where prior consent in writing was obtained under duress.

If an employer conforms to the provisions of RICA, an employee may not seek the protection of the right to privacy, unless he/she can prove that he/she gave the necessary consent under duress and /or based on the misrepresented facts.

40. **General recommendations**

General recommendations in this paper are explicitly illustrated in a copy of the draft proposed regulations that is attached as annexure A. These recommendations address all the problems that have been identified in RICA and need not further expansion. A classical example is the inclusion of the definition of “reasonable steps” which is lacking in RICA. These definitions and principles set out in the regulations are extracted from the principles set out by our courts; international and foreign instruments as well as jurisprudence. It follows that the provisions of the proposed regulations further express my submissions and principles that our courts should take into account when interpreting RICA in light of protecting the right to privacy.

41. **Conclusion**

It is explicit that the right to privacy has been recognized and protected by the common law and the Interim Constitution. This protection is now entrenched in section 14 of the 1996 Constitution. It is also evident that the said right is subject to the limitation clause test pursuant to the provisions of section 36 of the 1996 Constitution. It is observed that both the EC Act and the ECT Act regulate the interception of electronic communications to a certain extent. In the same breath, RICA regulates the interception of an employee's electronic communications and this regulation is explicitly provided in the provisions of section 4, 5 and 6 of RICA. Section 4 requires that one intercepts electronic communications, if he/she is a party to such communication.

The question that was asked in the beginning of this paper was whether or not the evidence that had been obtained pursuant to this section [s4] would be admissible. The exposition is that, the courts had admitted the evidence obtained in such a manner.

The answer is therefore yes, such evidence would be admissible. It is however submitted that the courts should consider the circumstances of the case and consider whether the party who intercept such an employee's electronic communications has any motive or not in applying the provisions of section 4 of RICA.

A classical example would be when an ex boyfriend/girlfriend intercepts the ex boyfriend/girlfriends communication where an employee is party to such communication and the latter incriminates himself/herself, and such communication is intercepted by such boyfriend/girlfriend because he/she wants to avenge himself/herself, and submit such intercepted communication to such an employee's employer, to be used as evidence against such an employer, in disciplinary proceedings or any criminal proceedings. The courts must therefore consider such evidence with circumspection. I express the view that if the court is satisfied that there was indeed a motive on the part of such a party who intercepted such communication such evidence should not be admitted.

In so far as the provisions of section 5 of RICA are concerned, it is evident that the legislature intended that an employer should first obtain prior consent in writing from an employee before intercepting the latter’s electronic communications. It is submitted that where an employee has signed a contract of employment, wherein there is a term that has been incorporated that illustrates that such an employee would be employed subject to general rules and procedures of the company, which do not necessarily permit the interception of such an employee's electronic communications, such an employee would be deemed to have given prior consent in writing by virtue of signing such a contract.

In instances where there has been an oral contract of employment concluded between an employer and an employee, and the employee acknowledges its terms in writing, subsequent to its conclusion, and one of the terms of such a contract provides that such an employee would be employed subject to the rules and procedures of the company, an employee would be deemed to have given the necessary prior consent in writing.

It is submitted that where consent has been obtained under duress or based on the misrepresentation of facts, and the employer continues intercepting such an employee's electronic communications, such conduct would be regarded as an infringement of such an employee's right to privacy.

This would often happen when an employer has forced an employee to give the necessary consent in writing, or an employee gives such consent under the impression that he/she is consenting to something else other than the interception of his/her electronic communications. Where an employee refuses to give the necessary consent in writing, it is submitted that the courts must determine whether or not the refusal is reasonable or rational or the refusal would prejudice the employer, in any manner, to determine whether or not there has been an infringement of the right to privacy.

A classical example would be wherein an employee refuses to give prior consent in writing and he/she abuses the employer's facilities, by conducting his/her own business during official hours, and at the same time is associated with the competitor of such an employer, the refusal in such instances would indeed be unreasonable, irrational and prejudicial to the employer in question. The interception would be necessary to protect the interest of such an employer from its competitor and to monitor the performance of such an employee. It is submitted that the existence of consent in writing terminates at the expiration or termination of the contract of employment. Thus, an employer may not continue to intercept an employee's electronic communications after he/she has left the company, if such an employer would still have access to such an employee's private computer or telephone or mobile telephone [electronic communications].

With regards to section 6 of RICA, it is submitted that common business practices should be used as the test to determine the meaning of ordinary course of carrying business. Namely, instances where a certain industry operates between 08h00am to 17h00pm, the interception of an employee's electronic communications could be accepted during this period. Any interception beyond this period would, in my view, be regarded as an infringement of an employee's right to privacy.

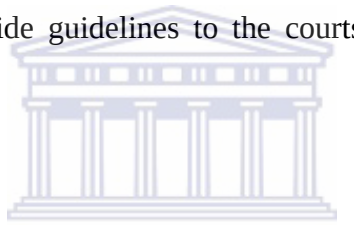
If an employee receives electronic communications, namely an email that has been marked private and confidential, it is my contention that an employer may not intercept such email; because such interception would not be conducted during the course of carrying of business as such communication would not be related to the interest of the business. The same applies in industries where an employee works flexible hours, which do not fall within the period between 08h00am to 17h00pm from Monday to Friday and his/her electronic communications is marked private and confidential, and such communication has not been sent by the employer's clients, such an employer may not intercept such an employee's email. It is contended that the conduct of such an employer in such circumstances, would be regarded as an infringement of such an employee's right to privacy, unless the employer proves otherwise.

Coming to the issue of whether or not an employer has taken reasonable steps pursuant to section 6(2) of RICA, it is submitted that an employer would be deemed to have taken reasonable steps to inform his/her employees of the interception, if he/she drafts explicit policies that permit such interception. In addition, if an employer incorporates a disclaimer clause at each employee's computer, which explicitly waives an employee's right to privacy, such an employer would be presumed to have taken reasonable steps to inform employees of such interception. It is also submitted that if an employer incorporates as an annexure, a notice in an employee's contract of employment that advises his/her employees of such interception, such employees would be deemed to have taken reasonable steps in accordance with the provisions of section 6(2) of RICA.

In sofar as the constitutionality of RICA is concerned, it is submitted that although RICA does not expressly provide for the protection of an employee's right to privacy, the application of the golden rule principle or the contextual approach, illustrates that the provisions in question of RICA, as they stand, are not regarded as unconstitutional. The limitation imposed on an employer to first conform to the provisions of section 4, 5 and 6 of RICA before intercepting an employee's electronic communications is reasonable and justifiable.

It is my contention that the application of international and foreign jurisprudence and the consideration of international and foreign instruments illustrated in this paper, as required by section 39 of the 1996 Constitution affirms that an employee should first have a legitimate expectation to privacy before he/she seeks the protection of the right in question.

The Bill also affirms the significance of obtaining consent and places an obligation on employers to advise employees that their electronic communications, would be intercepted before conducting such interception or as soon as reasonable practicable to do so thereafter. It is my last submission that all the principles pointed out in this paper illustrate that the conduct of an employer would be infringing on an employee's right to privacy, if the employer fails to conform to the provisions of section 4, 5 and 6 of RICA. Finally, it is prudent to express the view that the legislature and the judiciary should consider the principles pointed out in this paper, because these principles do not only provide guidelines to the courts, but they also contribute to the development of our law.



ANNEXURE A

PROPOSED REGULATIONS
REGULATION OF INTERCEPTION OF COMMUNICATIONS AND PROVISION OF COMMUNICATION-RELATED INFORMATION ACT 70 OF 2002

REGULATIONS SEEKING TO PROTECT THE RIGHT TO PRIVACY IN LIGHT OF INTERCEPTING ELECTRONIC COMMUNICATIONS

Published under Government Notice R…..in *Government Gazette* ……of …...

The Minister of Communications has in terms of section…….of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, made the regulations in the Schedule.

Schedule

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

ARRANGEMENT OF SECTIONS

CHAPTER 1 – DEFINITIONS

In these regulations any word or expression to which a meaning has assigned in the Act shall have the meaning so assigned, unless the context otherwise indicates:

"**confidential information**" - means any information that pertains to an employee or any person's life, medical records, financial statements, family or marital matters as well as intellectual property right documents;

"**prior consent in writing**" - includes any document signed by an employee or any person wherein he/she permits his/her employer or any person to intercept his/her electronic communications;

"**ordinary course of business**" - includes a period stipulated in an employee's contract of employment or any natural person's contract, as his/her official working hours or any common business practices in which an employer or any person's business operates;

"**reasonable steps**" - includes notices permitting interception of electronic communications, given by an employer or any person to an employee or any person, who intends to intercept such an employee or a person's electronic communications.

CHAPTER 2 – GENERAL

These regulations apply to an employer or any natural person who intends to intercept any employees, or any other person's, electronic communications.

An employee or any natural person, whose electronic communications is intercepted, is presumed to have a reasonable expectation to privacy in relation to such communication, unless the contrary is proved.

An employee or any person's right to privacy shall override any employer or any person's right to trade freely or economic interest, if such an employee or person's electronic communications received, is marked private and confidential.

An employer or any person may not obtain evidence against an employee or any person by intercepting such an employee or a person's electronic communications, if such an employer or a person has less restrictive means to obtain such evidence.

Subject to the provisions of the Act, interception of an employee, or any other person's electronic communications is prohibited if:

the information being intercepted relates to such an employee or person's medical records; or
the information relates to his/her financial statements; or

the information relates to his/her family or marital matters.

The above prohibitions can be rebutted, if an employer or any person establishes that such information is necessary to investigate a vicarious liability claim or to protect his/her intellectual property rights or any business interest.

CHAPTER 3 – CONSENT

An employee or any person is deemed to have given prior consent in writing, which permits his/her employer or any person to intercept his/her electronic communications, if he/she has signed a document to this effect, unless:

such a consent was given under duress; or

such consent was based on a misrepresentation of facts.

An employee or any person is deemed to have given prior consent in writing, if he/she has concluded a contract of an employment or any other contract, which explicitly provide that such an employee or person is employed subject to general company's rules and procedures, without incorporating expressed provisions that permit the interception of an employee or any natural person's electronic communications.

An employee or any person who has concluded an oral contract of employment or any oral contract would be deemed to have given prior consent in writing, if one of the terms of such contract of employment or any oral contract permits an employer or any person to intercept his/her electronic communications, and such an employee or a person has acknowledged such a term in writing. Such acknowledgement would be regarded as prior consent in writing.

If an employer or any person does not have any policies in place that permit the interception of an employee or any person's electronic communications, and no prior consent in writing has been obtained or given, such an employer or a person shall be deemed to have infringed such an employee or a person's right to privacy, unless it can be proved that such interception was conducted in the course of carrying of business or during ordinary course of business.

CHAPTER 4 – ORDINARY COURSE OF BUSINESS

An employer or any person shall be deemed to have intercepted his/her employee's or any other person's, electronic communications in the course of carrying on any business, if such interception is conducted between:

the period between 08h00 am to 17h00 pm from Monday to Friday or Monday to Saturday, if his/her industry operates between this period; or

if the interception is related to the protection of his/her intellectual property rights.

An employer or any person who operates in an industry where there are no standard working hours set, namely in the legal profession or any other profession, may only be permitted to intercept his/her employee or a person's electronic communications, if such an employee or a person has given consent or such an employer or a person has taken reasonable steps to inform such an employee or a person that his/her electronic communications would be intercepted, unless it can be proved that the interception is necessary to advance the interest of the business.

CHAPTER 5 - REASONABLE STEPS

An employer or any person who intends to intercept an employee or any person's electronic communications is deemed to have taken reasonable steps if:

he/she has drafted explicit policies that permit such interception; or

if he/she incorporates terms in an employee or a person's contract, which explicitly permit the interception of such an employee or a person's electronic communications; or

if he/she incorporates terms in an employee or any person's contract that expressly indicate that such an employee or person would be employed subject to general company's rules and procedures, without incorporating the express provisions that permit the interception of an employees' electronic communications; or

he/she places a disclaimer clause in his/her computer system that expressly waives an employee or any person's right to privacy, by virtue of using such a computer; or placing in his/her notice board, notices that inform an employee or any person that his/her electronic communications would be intercepted.

Short title

These regulations are called regulations seeking to protect the right to privacy in light of intercepting electronic communications.

BIBLIOGRAPHY

Statutes

42. The Constitution of the Republic of South Africa 108 of 1994.

43.Regulation of Interception for Communications and Provision of Communication-Related Information Act 70 of 2002.

44. Electronic Communications and Transaction Act 25 of 2002.

45. Electronic Communications Act 36 of 2005.

46. The Labour Relations Act 66 of 1995.

47. The Promotion of Access to Information Act 2 of 2000.

48. The Protection of Personal Information Bill.

49. Interception and Monitoring Prohibition Act 127 of 1992.

50. The Data Protection Act of 1984 (UK).

51. Wireless Telegraphy Act of 1949 (UK).

52. Computer Misuse Act of 1990 (UK).

53. Regulations of Investigatory Powers Act of 2000 (UK).

54. Electronic Communications Privacy Act of 1986 (USA).

55. Privacy Act of 1982 (Canada).

56. Personal Information Protection and Electronic Documents Act (PIPEDA - Canada).

57. Privacy Act of 1988 (Australia).

58. Workplace Surveillance Act of 2005 (Australia).

Table of cases

59. O'Keefle v Argus Printing and Publishing Co. Ltd 1954 3 SA 244 (C).

60. Jansen van Vuuren v Kruger 1993 4 SA 842 (A).

61. Bernstein v Bester NO 1996 4 BCLR 449 (CC).

62. Wheaton v Peters U.S 591 (1934).

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

64. R v Umfaan 1908 T.S.

65. S v I (1976) 1 SA 781 (RA).

66. Davis v Arthur (1970) 17 D.L.R 760.

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

68. Malone v Commission of Police of the Metropolis (1979) 2 All ER 620.

69. Katz v United States (1967) 389 U.S 34.

70. Rhodes v Graham (1931) 37 SW 2d 46.

71. Goosen v Caroline's Frozen Yoghurt Parlour (Pty) Ltd / Tru Food & Dairy Products Pty Ltd (1995) 4 LCD 152 (IC).

72. Mistry v Interim National Medical and Dental Council South Africa (1998) 4 SA 1127 (CC).

73. Janse van Rensburg NO v Minster for Trade and Industry NO (2001) 1 SA 29 (CC).

74. President of the Republic of South Africa v South African Rugby football Union (2000) 1 SA 1104 (SCA).

75. National Coalition for Gay and Lesbian Equality v Minister of Home Affairs (2000) 2 SA 1 (CC).

76. S v Dube (2000) 2 SA 583 (N).

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

78. Protea Technology Ltd v Waine (1997) 9 BCLR.

79. Case v Minster of Safety and Security; Curtis v Minster of Safety and Security (1996) 3 SA 617 (CC).

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

81. NM and Others v Smith and Others (CC) (CCT69/05) 2007 ZA CC6 (4 April 2007).

.

82. Magajane v Chairperson North West Gambling Board (2006) 5 SA 250 (CC); (2006) 2 SACR 477 (CC).

83. Investigating Directorate: Serious Economic Offences and Others v Hyundai Motors Pty Ltd and Others; In Re Hyundai Motor Distributors (Pty) Ltd and Others v Smith NO and Others (2001) 1 SA 545 (CC).

84. S v Jordaan (2002) 6 SA 624 (CC).

85. Financial Mail (Pty) Ltd v Sage Holdings Ltd (1993) 2 SA 451 (A).

86. Lenco Holdings Ltd v Eckstein (1996) 2 SA 693 (N).

87. Waste Products Utilization (Pty) Ltd v Wilkes (2003) 2 SA 515 (W).

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

89. Toker Bros (Pty) Ltd and Keyser (2005) 26 ILJ 1366 (CCMA).

90. Sage Holdings Ltd v Financial Mail (Pty) Ltd (1991) 2 SA 117 (W).

91. Malone v United Kingdom 1983 WL 215891 (Eur Comm HR) (1983) 5 E.H.R.R 385.

92. Khan v The United Kingdom (Application No.35594/97) = 20.

93. Halford v United Kingdom (1998) WL 1104805 (ECHR).

94. Amann v Switzerland (2000) 30 E.H.R.R 843.

95. Kopp v Switzerland (1998) WL 1043110 (E.G.H.R), 4 B.H.R.C 277.

96. Attorney General's Reference (No 5 of 2002) (2004) 4 All ER 901.

97. Re: an Employer's Call-Monitoring System 2002 WL 32093079 (OGHA), 2004 E.C.C.4.

98. Hughes Carratu International PLC (2006) EWHC 1791 QB.

99. Associated Newspapers Limited v His Royal Highness the Prince of Wales (2006) EWCA Civ 1776.

100. Copland v United Kingdom Case Reference application No. 62617/00 European Court of Human Rights 2007.

101. Malik v Bank of Credit and Commerce International SA 1997 IRLR 462.

102. Microsoft Corpn v Mc Donald 2007 Bus. LR. 548.

103. Sovereign Business Integration PLC v Trybus 2007 WL 1685225.

104. R v Stanford 2006 2 Cr App. R.5.

105. Olmstead v United States 277 U.S 438.

106. Watkins v LM Berry & Company 704 F2d 577.

107. Bonita Bourke v Rhoda Hall No. YC-003979 (Cal.Super.CT, LA City) 1993.

108. Smyth v Pillsbury Co. 914 F Supp. 97 (E.D.Penn.1996).

109. Bohack v City of Reno 932 F Supp.1232 (D.Nev. 1996).

110. Anderson v UOP 1998 WL 30703 (N.D.III.26 Jan 1998).

111. United States v Councilman No.03-1383 (1st Cir. decided on June 29 2004).

112. Warshak v United States of America No.06-4092 U.S.CRRT.App. (Decided on June 18 2007).

113. Briggs v American Air Filter Co. 455 F Supp.179 (N.D.GA.1978).

114. United States v Long 61 M.J.539.

115. R v Duarte (1990) 1 S.C.R 945.

116. Re Doman Forest Products Ltd (1990) 3 L.A.C. (B.C) 4th 275.

117. R v M 2005 BCSC 385.

118. St Mary's Hospital v H.E.U 64 L.A.C 4th 382.

119. R v Wong (1990) 3 S.C.R.36.

120. R v Adam 2006 BCSC 126.

121. Phato v Attorney General Eastern Cape, and Another; Commissioner of the South African Police v Attorney General, Eastern Cape, and Others (1995) 1 SA 799 (E).

122. Lawrence v IKuper & Co (Pty) Ltd t/a Kupers, as a member of Investec (1995) 4 LCD 42 IC.

123. Van Wyk v Independent Newspapers Gauteng (Pty) Ltd (2005) 26 ILJ 2433 LC.

124. Surgreen and Standard Bank of SA (2002) 23 ILJ 1319 (CCMA).

125. Venter v R 1907 TS 910.

126. De Beers Industrial Diamond Division Pty Ltd v Ishuka (1980) 2 SA 191 (T) 196.

127. Farrell v Alexander (1976) 2 All ER 721.

128. Morgan v Brittan Boustred Ltd (1992) 2 SA 775 (A).

129. Torgos (Pty) Ltd v Body Corporate of Anchors Aweigh (2006) 3 SA 369 (W).

130. Cuje-Jakoby v Kaschub (2007) 3 SA 345 (C).

131. Gerald Robitaille v American Biltrite (Canada) Ltd (1985) I.S.C.R 290.

132. Warwick University v De Graaf (1975) 3 All ER 284.

Textbooks

133. Grogan, J (2003).*Workplace Law*. Juta.

134. de Ville, JR (2000). *Constitutional & Statutory Interpretation*. Interdoc Consultants (Pty) Ltd.

135. du Plessis, L (2007). *Re-Interpretation of Statutes*. Butterworths.

136. Burns, Y (2001). *Communications Law*. Butterworths.

137. Currie, I & de Waal, J (2005). *The Bill of Rights Handbook*. Juta.

138. Buys, R & Cronje, F (2004). *The Law of the Internet in South Africa*. Van Schaik.

139. Neethling J, Potgieter JM & Visser PJ (2005). *Law of Personality*. Butterworths Durban.

140. Mac Qouid-Mason D (1978). *Law of Privacy in South Africa*. Juta.

Articles

141. Parry Aftab, ESQ. *Monitoring Employees Communications* [Online]. Available http://aftab.co./monitoringemployeescommunications.htm

142. From the Lectric Law Library's stacks. *Electronic Privacy Rights*: *The Workplace* [Online]. Available http://www.lectlaw.com/files/emp41.htm

143. S Nadasen (2002). *Data Protection is coming … time to start preparing; Insurance & Tax Law*, V 14(4).

144. Warren Beech (2005). *The right of an employer to monitor employee's electronic mail, telephone calls, internet usage and other recording*, 26 ILJ.

145. Ronald B Standler (1997). *Privacy in the USA* [Online]. Available http://www.rbs2.com/privacy.htm

146. The National Workrights Institute. *Electronic Monitoring in the Workplace: Common Law & Federal Statutory Protection* [Online]. Available http://www.workrights.org/issue-electronic/em-common-law.html

147. Neethling J (2005). *Personality rights: A Comparative overview*, CISA Vol 38(2.

148. Collier D. *Workplace Privacy in the Cyber Age* [Online].Available http://www.general.rau.ac.za/infosoci/www2002/Full-Papers/Collie%20D/Collier-WorkplacePrivacy

149. Neethling J (2004). *The protection of the right to privacy against fixation of private fact*, SALJ Volume 1211 Part 3.

150. Esselaar P (2005). *Interception of communications* [Online]. Available http://www.ghostdigest.co.za/A-784.html

151. Meiring R (2005). *Advisory 13: Interception of Private Communications in the Workplace* [Online]. Available http://www.ispa.org.za

152. Steinberg J (2007). *Generous judgment instils stigma* [Online]. Available http://www.businessday.co.za/PrintFriendly.aspx?ID=BD4A445289

153. Bawa N (2006). *The Regulation of Interception of Communications and Provision of Communication-Related Information Act: Telecommunications Law in South Africa,* Telecommunications Law in South Africa, STE publishers. .

154. Mischke C (2003). *Workplace privacy, e-mail interception and the law,* Vol 12 No.8.

155. Connelly N (2005). *Work computer not protected by privacy rules,* USA Today [Online]. Available nytimes.com/tech.

156. European Parliament (1999). *Development of Surveillance Technology and Risk of Abuse of Economic Information* [Online]. Available http://cryptome.org.dst-2.htm

157. Bruyndonckx B (2006). *Belgium: Data Privacy- Monitoring of Communications* [Online].Available http://international.westlaw.com/result/documenttext.aspx?=2fWelcome%WLIGen

158. Wallaret D (2006). *Belgium: Data Protection-Employment Law* [Online]. Available http://international.westlaw.com/result/documenttext.aspx?rp=2fWelcome%2%fWelocome WLIGen

159. Mickler. *Re: Employees Privacy and Eavesdropping in the Workplace.* [Online]. Available http://eziнearticle.com./?Employee-Privacy-and Eavesdropping-in-the Workplace &id=5

160. The Catholic University of America. *Summary of Federal Laws* [Online]. Available http://counsel.cua.edu/fedlaw/Ecpa.cfm

161. The Publishing Law Center. *The Right to Privacy* [Online]. Available http://www.publiclaw.com/privacy.html

162. Fox News.com. *Court Rules E-mail Search Without Warrant Violates Fourth Amendment* [Online]. Available http://www.foxnews.com/printer-friendly-story/0,3566,284193,00html

163. Knowles B (2000). *Are Employers Violating Worker's Privacy with Electronic Monitoring?* [Online]. Available http://speakout.com/activism/issue-briefs/1300b-1html

164. Dice. *Workplace privacy versus computer abuse prevention: which prevails*? [Online]. Available http://techrepublic.com/5102-10878-6144095.html

165. Connelly, Roberts & Mc Givney LCC (1998). *Privacy Issues in High Tech Workplace.* [Online]. Available http://library.findlaw.com/1998/Mar/1/130358.html

166. Lasprogata G, King NJ& Pillay S (2004). *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, Stanford Technology Law Review*. [Online]. Available http://stlr.stanford.edu/STLR/Articls/04-STLR-4.

167. Mac-Alexandre Poirier (2002). *Employer Monitoring of the Corporate E-mail System: How Much Privacy Can Employees Reasonably Expect?* [Online]. Available http://www.law.uiuc.edu/publications/CLL-PJ/archive/vol-24/issue-3/EltisArticle 24-4.

168. Morgan C (1999). *Employer Monitoring of Employee Electronic Mail and Internet Use*. 44 MacGill L.J.849.

169. Greg Taylor Melbourne University Law Reform Reform Recview (2205). *A Tort of Invasion of Privacy in Australia.* MULR.

170. De Beer FJ (2003). *The Need for Comprehensive Protection*. Saskatchewan Law Review. Vol. 66(2).

171. Bosch C (2006). *Can unauthorised workers be regarded as employees for the purpose of the Labour Relations Act?* 27 ILJ 1342.

172. Law of South Africa. *Introduction of the Bill of Rights primary involves attaching meaning*. Volume 10(1)-First Reissue volume.

173. Article 29-Data Protection Working Party (2002). *Working Document on the Surveillance of Electronic Communication in the Workplace* [Online]. Available http://wwweuropa.eu.int/comm/privacy.

Other references

174. South African Law Reform Commission (2005). *Privacy and Data Protection.* Discussion Paper 109 project 124. (2005).

175. Australian Law Reform Commission. Overview of ALRC Issues Papers 13 & 32, Review of Privacy [Online]. Available http:// www.austlii.edu.au//cgi-bin/disp.pl/au/other/alrc/publications/issues/31-32-overview