Email Privacy

Does the government have the right to intercept and/ or monitor private e-mail communications?

By **Zanele Precious Majola**

Submitted as the dissertation component (which counts for 50% of the degree) in partial fulfilment of the requirements for the degree of Master of Laws in the Faculty of Law, University of Natal in 2003.

University of Natal

2003

Abstract

Section 14 of the Constitution provides for the right to privacy, which includes the right not to have the privacy of communications infringed. The right is also protected at common law – a breach of a person's privacy constitutes an *iniura.* E-mail communications are therefore protected by both, the common law and the Constitution.

The question that this work seeks to answer is, whether the Government has the right to intercept and/or monitor private e-mail communications.

The right to privacy is not absolute, case law and legislation show that this right can be limited. At common law, a valid defence will negate the unlawfulness of the invasion. In terms of the Constitution, the right to privacy can only be limited in accordance with the limitation clause – section 36. For each case, courts will have to balance, the government's interest in combating crime and that of the citizen to the privacy of their e-mail communications.

In seeking to answer the question, this work considers the protection afforded by the common law and the Constitution. It also considers statutes which limit the right to privacy, including whether these statutes are applicable to e-mail communications and if they are, whether they constitute a justifiable limitation of the right, for example: the Regulation of Interception of Communications and Provision of Communication-Related Information Act and the Criminal Procedure Act – which was enacted when the 'cyber-world' was non-existent. All statutes, applicable to e-mail communications, provide for some form of requirements or guidelines before communications can be intercepted or/ and monitored.

The right to privacy is also protected in foreign jurisdictions and is not absolute. There is protection *only* against *unreasonable* invasions of privacy.

In conclusion, both statutory law and common law permit the government, within limitations, to intercept or/ and monitor private e-mail communications. Where there are guidelines, regulating

this power, the circumstance under which and when it can be exercised. This will amount to a reasonable and justifiable limitation and therefore the right will not be violated.

Acknowledgements:

There is no better day which symbolises my happiness more than the 12th of September 2003, when I finally completed my dissertation.

This year has been very strenuous for me and my family. Writing this dissertation has been hard, involving a lot of sacrifices. Trying to finish on time kept my eyelids open even in the worst of Johannesburg's coldest winter nights.

The determination, strength and positive thoughts that kept me going cannot, however, be attributed only to myself. My family and friends kept me going. I would like to thank my Creator and my mother, Celestina Majola, for having given me the opportunity to write this work. Musa Mbuyisa, my partner, I will forever be grateful to him, for his time, support and constant advises, he kept me sane.

The thought of all the happiness this work would have brought to my family and friends, gave birth to this most difficult product. Thinking of graduation day eased the stress. One very important person in my life is no longer here to share the joys of finishing this work. It is therefore an honour to dedicate this work to the spirit and soul of my late sister, Thulisile Majola, who passed away just before the completion of this piece. Her soul saw me through the most difficult of times (of losing her as a sister) and with this work may she be happy wherever she is.

Last but not least, I would like to thank my supervisor, Professor David McQuoid-Mason, for all his guidance and patience. Thank you very much.

Finally I would like to thank my friends, Ntsako Mathebula, Nomkhosi Buthelezi and Nontu Made for being good listeners and supportive friends. It took a lot of courage to put up with all my whining. Thank you all.

E-mail Privacy

Does the government have the right to intercept and/ or monitor private e-mail communications?

Table of Content: **Page**

Chapter 1. Introduction:

Privacy is a basic human need, essential for the development and maintenance both of a free society and a mature and stable personality for an individual.[1] It is clear in our law that as individuals we have a right to privacy. This right is not only found in the common law but forms part of the Constitution.[2] The right to privacy is also recognised in the constitutions of many foreign jurisdictions.[3]

In terms of South African law the infringement of private communications constitutes an invasion of privacy.[4] The rapid growth and increasing use of the internet give rise to many and complex privacy issues. Every e-mail message contains a header with information about the sender and the recipient.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act[5] (the Regulation Act) has the following as its preamble:

> To regulate the interception of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information; to regulate the making of applications for, and the issuing of, directions authorising the interception of communications and the provision of communication-related information under certain circumstances; to regulate the execution of directions and entry warrants by law enforcement officers and the assistance to be given by postal service providers, telecommunication service providers and decryption key holders in the execution of such directions and entry warrants; to prohibit the provision of telecommunication services which do not have the capability to be intercepted; to provide for certain costs to be borne by certain telecommunication service providers; to provide for the establishment of

---

[1] G. E. Devenish, *A Commentary on the South African Bill of Rights* 1999 135.
[2] Constitution of the Republic of South Africa Act 108 of 1996 (the Constitution).
[3] See for example the Constitution of Angola, art 24; Argentina, art 29; Mauritius, art 3(c); Mexico, art 16; Mozambique, art 64 and Namibia, art 13.
[4] Devenish (above note 1) 153; see also Chapter 2 below for a discussion on the common law and constitutional right to privacy.
[5] Act 70 of 2002.

interception centres, the Office for Interception Centres and the Internet Service Providers Assistance Fund; to prohibit the manufacturing, assembling, possessing, selling, purchasing or advertising of certain equipment; to create offences and to prescribe penalties for such offences; and to provide for matters connected therewith.

The above quotation demonstrates that there are instances or circumstances where the law permits some form of an invasion of privacy. There are therefore circumstances where communications can be monitored or intercepted. Thus, there is a need to clarify whether the government can be justified in intercepting and/ or monitoring private e-mail communications. In doing so, there is a need to look at how the courts balance the government's interest to combat crime against the right to privacy provided for by the common law and the Constitution.[6] There is a need for clarity as to what remedies, if any, are available to aggrieved individuals in cases where there has been an *unjustified* invasion of privacy.[7]

The following work therefore seeks to address these issues. In Chapter 2 the writer will be looking at how the common law and constitutional right to privacy protect individuals against the interception and monitoring of e-mail communications. Chapter 3 deals with legislation authorising the interception and monitoring of private communications. Chapter 4 is a discussion of the position in foreign jurisdictions namely, the United States; Canada, the United Kingdom and the European Commission experience. The writer will also compare these countries with the South African experience. Thereafter in Chapter 5 the writer will look at whether there is a need for legal change or clarity in South Africa- making a few recommendations. Finally, Chapter 6 will be the conclusion.

[6] The Constitution (note 2 above) s 14.
[7] It will be seen from the discussion to follow that the law prohibits only those invasions to the right to privacy that are proved to be unjustifiable in law. See also the discussion on the limitation clause below Chapter 3.4.

Chapter 2: The Right to privacy:

The *Oxford English Dictionary*[8] defines privacy as the state or condition of being alone, undisturbed, or free from public attention, *as a matter of choice or right*; *freedom from interference or intrusion.* [Emphasis added]

2.1. The Common law right to privacy:

Prior to the inception of the 1993 Constitution[9] South African common law recognised an action for an invasion of privacy.[10] Section 13 of the Interim Constitution created a constitutional right to privacy. This right is now enshrined in s 14 of the Final Constitution. The fact that South Africa has embodied the right to privacy in its Constitution does not, however, mean that "all previous notions of privacy will be forgotten and fall into disuse".[11] McQuoid-Mason states that the courts in this new situation [constitutionally guaranteed right to privacy] will continue to employ those common law actions which are in harmony with the values of the Constitution.[12]

In this regard the Constitutional Court has said, in the *Pharmaceutical Manufacturers*[13] case, per Chaskalson P, that:

> "The common law supplements the provisions of the written Constitution but derives its force from it. It must be developed to fulfil the purposes of the Constitution and the legal order that it proclaims – thus, the command that law be developed and interpreted by the courts to promote the "spirit, purport and objects of the Bill of Rights." This ensures that the common law will evolve within the framework of the Constitution consistently with the basic norms of the legal order that it establishes. There is, however, only one system of law

[8] 5th Edition 1995.
[9] Constitution of the Republic of South Africa 200 of 1993 (the Interim Constitution).
[10] Devenish (note 1 above) 145.
[11] D McQuoid-Mason 'Privacy' in A Chaskalson et al (eds) *The Constitutional Law of South Africa* 18-1.
[12] Ibid.
[13] *Pharmaceutical Manufacturers of SA; In ex parte Application of the President of RSA* 2000 (2) SA 674 (CC); 2000 (3) BCLR 241 (CC).

and within that system the Constitution is the supreme law with which all other law must comply."[14]

The writer is in agreement with the view expressed by McQuoid-Mason and applied by the Constitutional Court in the *Pharmaceutical* case above. The enactment of the Constitution could not have been intended to discard all existing common law principles. The text of the Constitution itself does not favour such an approach. Instead, it provides that only laws that are inconsistent with the Constitution are invalid.[15] Therefore from the wording of the Constitution, it is clear that the Legislature intended to remove or invalidate only those laws that are proved to be inconsistent with the Constitution and this can only be done if a court of law failed to develop the "inconsistent" law to be in accordance with the Constitution as provided by s 39 of the Constitution.[16] Therefore, courts will inevitable retain existing common-law principles which are in harmony with the values embodied in the Constitution.

Burchell[17] submits that in the Roman law, there was no sophisticated concept of privacy however, the Roman jurists recognised a number of specific instances where a remedy (usually under the *actio injuriarum*) was provided for a wrong which could be interpreted as an impairment of privacy, as an example he states that a remedy for an invasion of the sanctity of the home. He submits that during the nineteenth and early twentieth centuries in South Africa there was no recorded case law which gave any substance to the concept of privacy, but from the 1950s onwards a right to be free from public disclosure of private facts and unreasonable intrusions into the private sphere had been recognised. It is submitted that this view is incorrect. In the

---

[14] Ibid 49.

[15] Section 2 of the Constitution states that:

> 2. Supremacy of Constitution.—
>
> 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.

[16] Section 39 of the Constitution states that:

> (2) 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

[17] Jonathan Burchell *Personality Rights and Freedom of Expression* (The Modern *Actio Injuriarum*). Juta (1998) 372.

nineteenth century South African courts already recognised and protected privacy. In *De Fourd v Town Council of Cape Town*[18] De Villiers C J held that:

> "I cannot refrain from saying a word as to the conduct of the police in entering the private bedrooms of the women in the house for the purpose of ascertaining whether they were carrying on the trade . . . of prostitution. Even these abandoned women have their rights, and without their permission or a legal warrant no policeman is justified in interfering with their privacy."[19]

This clearly shows a recognition of the right to privacy.

The common law, as has been stated, recognises the right to privacy. This right is recognised as an independent personality right, which the courts consider to be part of the concept of a person's '*dignitas*'.[20]

At common law the breach of a person's privacy constitutes an *iniuria*.[21] De Waal et al[22] state that an invasion of a person's privacy may take the form of either an unlawful intrusion on someone's personal privacy or an unlawful disclosure of private facts about a person.[23] This work only deals with intrusions upon personal privacy of others and does not cover the unlawful disclosures of private facts about a person.

Courts have said the following regarding the right to privacy:

> The concept of privacy is an amorphous and elusive one which has been the subject of much scholarly debate. The scope of privacy has been closely related to the concept of identity and it has been stated that "rights, like the

---

[18] 1898 SC 399.
[19] *De Fourd* 402.
[20] *S v A and Another* 1971 (2) SA 293 (T) at 297, see also *Bernstein and Others v Bester and Others NNO* 1996 (4) BCLR 449 (CC); 1996 (2) SA 751 (CC); *Jansen Van Vuuren and Another NNO v Kruger* 1993 (4) SA 842 (A) 849E; J. de Waal, I, Currie & G, Erasmus, *The Bill of Rights Handbook*, 4ed (2001) 268 and G. E. Devenish (above note 1).
[21] Ibid 243.
[22] Ibid. See also *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another* 1993 (2) SA 451 at 462 E-H.
[23] See also *Financial Mail* (above note 22) 462 F-G.

right to privacy, are not based on a notion of the unencumbered self, but on the notion of what is necessary to have one's own autonomous identity".[24]

In *R v Umfaan*[25] Innes C.J had the following to say about the common law right to privacy:

> "If we look at the essentials of *injuria* we find . . . that they are three. The act complained of must be wrongful; it must be intentional; and it must violate one or other of those real rights, those rights *in rem*, related to personality, which every free man is entitled to enjoy. Chief Justice De Villiers says: "With these ingredients to hand it will be found that there are three essential requisites to establish an action of injury. They are as follows - (1) an intention on the part of the offender to produce the effect of his act; (2) an overt act which the person doing it is not legally competent to do; and which at the same time is (3) an aggression upon the right of another, by which aggression the other is aggrieved and which constitutes an impairment of the person, dignity or reputation of the other."

From the *dictum* of Innes CJ in *Umfaan*[26] it is therefore clear that in order for a plaintiff to prove an invasion of privacy, at common law, he or she must show that there was an unlawful and intentional infringement of the plaintiff's right to privacy. The unlawfulness of a factual infringement of privacy is judged in the light of the contemporary *boni mores* and the general sense of justice of the community as perceived by the court. As a result of the political process of democratic transformation a new ethos prevails in South Africa. Devenish submits that this must inevitably influence the content of a contemporary *boni mores*.[27]

The presence of a ground of justification (such as statutory authority) means that an invasion of privacy is not wrongful.[28] If wrongfulness has been established a

---

[24] *Bernstein (*above note 20).
[25] 1908 T.S. 62, 66.
[26] Ibid.
[27] Devenish (above note 1) 146.
[28] J, Neethling, J.M, Potgieter & P.J, Visser: *Law of Delict* 4th Ed (2001) 355. See a discussion on this below.

presumption of *animus inuiriandi* arises which may be rebutted by the defendant. If he fails to do this then the *actio iniuriarum* is available to the plaintiff.[29]

Quoting McQuoid-Mason, Devenish also provides an apt definition of the common law right to privacy.[30] This is defined as an intentional and wrongful interference with another's right to seclusion in his or her private life. The element for an invasion the right to privacy are thus the following: (a) violation of privacy; (b) wrongfulness; and (c) fault in the form of intention.

Some examples of wrongful intrusion which have been acknowledged at common law are entry into a private residence, the reading of private documents, listening in to private conversations, the shadowing of a person.[31] As mentioned earlier, the focus in this work is only on the monitoring or interception of private electronic communications. Therefore from these examples, of relevance to this work is the reading of private documents (as will be the case with e-mails) and listening to electronic communication (for example in *S v Naidoo*[32]).

The writer agrees with the views expressed by Burchell that with the availability of sophisticated technology such as telephoto lenses, video cameras, micro tape-recorders and computers, the fear of intrusion into the private sphere is a very real one.[33] These days computers can retain vast quantities of personal information on disk and very often the subject of the information is oblivious of the existence of the collection of data relating to his or her financial state, education or other confidential material. The subject should not be denied knowledge of the information on himself or herself and the ability to control the extent of its dissemination.[34]

Apart from the question of *animus iniurandi*, the determination of whether an invasion of the common law right to privacy has taken place is a single enquiry. It essentially involves an assessment as to whether the invasion is unlawful.[35]

---

[29] Ibid 356, See also *Kidson v S.A. Associated Newsxpapers* 1957 (3) SA 461 (W) 468.
[30] Devenish (note 1 above) 145.
[31] Neethling *et al* (above note 28) 355-356.
[32] Discussed later in this work.
[33] Burchell (above note 17) 395.
[34] Ibid 395-396.
[35] De Waal (note 20 above) 268-9.

Ackerman J warned in *Bernstein* that caution must be exercised when attempting to project common law principles onto the interpretation of fundamental rights and their limitation; it is important to keep in mind that at common law the determination of whether an invasion of privacy has taken place constitutes a single enquiry, including an assessment of its unlawfulness. Endorsing what has been said above, he stated that as in the case of other *iniuriae* the presence of a ground of justification excludes the wrongfulness of an invasion of privacy. In constitutional adjudication under the Constitution, by contrast, a two-stage approach must be employed in deciding constitutionality of a statute.[36]

In *National Media Ltd and Another v Jooste*[37], quoting Neethling[38], Harms JA said[39] the following:

> "Absent a will to keep a fact private, absent an interest (or a right) that can be protected. The boundary of a right or its infringement remains an objective question. As a general proposition, the general sense of justice does not require the protection of a fact that the interested party has no wish to keep private."

This view is in accordance with the "legitimate expectation of privacy test" adopted not only by South Africa, but also in other foreign jurisdictions, for example, the United States; United Kingdom and Canada.[40] Therefore, the right to privacy protects only those aspects of privacy where an individual has a legitimate expectation of privacy. It is important to note that such an expectation must be reasonable. It has been held that a right to privacy encompasses the competence to determine the destiny of private facts.[41]

---

[36] *Bernstein* (above note 20) 71.
[37] 1996 (3) SA 262 (A).
[38] J Neethling, J Potgieter and P Visser *Deliktereg* 5th Ed (2002) 344 note 239.
[39] At 271.
[40] See Chapter 4 below for a discussion
[41] Harms JA in the *National Media* case (above note 37) 271.

Quoting Warren and Brandeis[42], Harms J stated the following:

> "The intensity and complexity of life, attending upon advancing civilisation, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."

Before the Constitution came into force, there seem to have been confusion or lack of clarity as to whether the right to privacy at common law was available only to natural persons or whether legal (or artificial) persons could also invoke the right. In *Financial Mail*[43] the Appellate Division (as it then was) clarified this issue. Corbett CJ held that the court a quo had been wrong in holding that:

> ". . . the right to privacy, being a real right of personality, only applies to natural persons and does not apply to a company".

At 460E-F Corbett CJ held that the view expressed by the lower court was incorrect. He held[44] that as a matter of general policy, the Courts have, in the sphere of personality rights, tended to equate the respective positions of natural and artificial (or legal) persons where it is possible and appropriate for this to be done. The Constitution now makes it clear that the rights in the Bill of Rights (including the right to privacy) protect both natural and juristic persons.[45]

From what has been said so far, the conclusion is that at common law, infringements of private communications have long been regarded as wrongful. The courts have

---

[42] A quote by Harms JA in *National Media v Jooste* above note 37 from Warren and Brandeis 'The Right to Privacy' (1890) 4 Havard Law Review 193.
[43] Above note 22.
[44] At 461F-G.
[45] Section 8(2) of the Constitution provides that:

> A provision of the Bill of Rights binds a natural or a juristic person if, and to the extent that, it is applicable, taking into account the nature of the right and the nature of any duty imposed by the right.

recognised that the unreasonable use of eavesdropping and electronic surveillance by private detectives in matrimonial disputes may result in a criminal invasion of privacy.[46]

However, it must be remembered that like the constitutional right to privacy, the common law right to privacy is not absolute. The wrongfulness of a violation of privacy is suspended by the presence of a ground of justification.[47] Some of the grounds of justification are necessity[48]; private defence[49]; consent to injury[50] and performance in a statutory or official capacity[51]. Defences that exclude fault (intention) include mistake[52]; rixa[53]; jest[54]; and any defence which shows subjectively that the defendant did not have the intention to injure, such as insanity or intoxication.

---

[46] See for example *S v A* (above note 20) where the court held that it was unlawful to install listening devices without the knowledge and consent of the person whose communication was to be monitored and recorded.

[47] J Neethling, J Potgieter, P Visser, *Neethling's Law of Personality* (1996), 262.

[48] Necessity is present when the defendant by *vis major* is put into such a position that he can protect his legitimate interests (or those of others) *only* by infringing another's legal interests (in this particular case, another's privacy). If there was a reasonable alternative available to the defendant, the violating act would not be justified. See Neethling *et al* (above note 47) 263.

[49] Private defence is present when the defendant defends himself against another's actual or imminently threatening wrongful act in order to protect his or her own legitimate interests or such interests of someone else. However Neethling says that acts of private defence justifying an invasion of privacy seldom occur. See Neethling *et al* (above note 47) 264.

[50] Consent as a ground of justification plays an important role in the field of protection of privacy because facts are excluded from public knowledge. Consequently, where a person determines that other persons may be informed of private facts, he actually consents to such acquaintance, which is then lawful. See also Neethling *et al* (above note 47) 274.

[51] The state generally protects or maintains the public interest when, by virtue of its greater power, it lays down conditions restricting the rights and freedoms of its subordinates in the public interest. These instances of restriction of the right to privacy fall within the ground of justification of statutory or official capacity. This ground of justification is especially appropriate in the upholding of law and order, the prevention of crime and disorder, state security, public health, morality and welfare. The lawfulness or unlawfulness of a violation of privacy by exercising these capacities must be determined with reference to the relevant permissive statute or common law rule. The right to privacy is violated when the defendant transgresses his capacity. As factor which plays an important role in the question whether or not the particular capacity has been transgressed, is whether the extent of the conduct concerned was reasonably necessary. See also Neethling *et al* (above note 44) 266 - 267.

[52] Mistake will be a good defence to an action for invasion of privacy where as a result of a mistake the defendant was unaware that he or she was invading the plaintiff's privacy (ie. he or she had no intention to injure), but not where he or she bona fide believed that the invasion was made with a lawful purpose (ie. was not conscious of the wrongfulness of the act). See also McQuoid-Mason (above note 11) 18-7 – 18-8.

[53] This indicates a lack of intention where the defendant acts: (a) without premeditation, (b) in sudden anger on provocation by the plaintiff, and (c) does not subsequently persist in the conduct. See also McQuoid-Mason (above note 11) 18-8.

[54] Words spoken [or things done] in jest or fun should not give rise to an action for invasion of privacy if they were intended and understood as such. See also McQuoid-Mason (above note 11) 18-8.

The remedies available to the aggrieved party for an invasion of privacy at common law are damages and interdicts. A plaintiff suing for damages under the *actio injuriarum* claims sentimental damages for *solatium* or satisfaction, not for pecuniary loss that can be calculated accurately in monetary terms. However, in the case where pecuniary loss can also be proved, the plaintiff may bring a 'rolled up' action for sentimental damages and actual patrimonial loss.[55] For an interim interdict the applicant must show:

1. a prima facie right;
2. a well grounded apprehension of irreparable if the interim relief is not granted;
3. the balance of convenience favours the granting of the interim interdict; and
4. the applicant has no other satisfactory remedy.

In order to obtain a final interdict, the plaintiff must show that he or she has

1. a clear right;
2. suffered actual injury or a well grounded apprehension of irreparable injury; and
3. no other satisfactory remedy is available.[56]

From the foregoing, the following is clear that South African citizens have a common law protection against privacy violations. Privacy violations at common law can, amongst other ways, be in a form of intrusions which surely do include reading private documents such as e-mails. The constitutional right to privacy embodied in s 14 of the Constitution does not mean that there is no longer a right to privacy at common law. Assuming a court of law had to find that the common law right to privacy is inconsistent with the Constitution, this will however not mean that there is no longer a common law right to privacy. Section 39(2) of the Constitution enjoins courts to develop the common law in order to make it consistent with the "spirit, purport and objects" of the Bill of Rights. The Constitutional Court in *Carmichele v*

[55] McQuoid-Mason, *Invasion of Privacy: common law v constitutional delict- does it make a difference.* Acta Juridicta (2001) 227, 234 – 235.
[56] Ibid 235 – 236.

Minister of Safety and Security and Another[57] decided that, a court, in deciding whether a common law principle should be developed, is obliged to undertake a two stage enquiry.

The court held:

> "The first stage is to consider whether the existing common law, having regard to the section 39(2) objectives, requires development in accordance with these objectives. This inquiry requires a reconsideration of the common law in the light of section 39(2). If this inquiry leads to a positive answer, the second stage concerns itself with how such development is to take place in order to meet the section 39(2) objectives. Possibly because of the way the case was argued before them, neither the High Court nor the SCA embarked on either stage of the above inquiry."[58]

It is submitted that South Africa still has a common law right to privacy. Therefore if all the elements that have been stated above are proved, the plaintiff will get the relief that he or she will be seeking be it in a form of damages or an interdict.

On this basis therefore, in a delictual action for an invasion of privacy, if the government[59] can show that one of the defences available in a common law action for privacy, is present, the plaintiff will not be successful. What this therefore means, is that if a government official can prove the presence of a statutory duty, this will amount to a valid defence exempting him or her from liability for a delictual action.

It submitted that there will be very limited instances where individuals can invoke the common law right to privacy. Firstly because of the presence of a wider protection afforded by s 14 of the Constitution.[60] Secondly, if the common law delictual action is followed, the writer submits that it will be very easy for government officials to

---

[57] 2001 (10) BCLR 995 (CC); 2001 (4) SA 938 (CC), 40.
[58] Ibid.
[59] It must be remembered that for the purposes of this work, we are only dealing with invasions of privacy by government officials or bodies.
[60] To be discussed below in this Chapter under 2.2.

raise a statutory duty defence in light of all the South African statutes[61] authorising invasions of privacy. The statutes will however have to be consistent with the Constitution.

What is to follow is an examination of the constitutional protection of the right to privacy (s 14).

[61] See Chapter 3 below for a discussion of legislation authorising the interception and monitoring of private communications.

2.2. Constitutional right to privacy:

The right to privacy in the Constitution is contained in s 14. This section reads as follows:

> 14. Privacy.—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 Bill of Rights applies to both natural and legal persons.[62] The Constitution makes it clear that companies can also claim the rights in the Bill of Rights which obviously include the right to privacy. Such a conferment of the right to privacy on juristic persons is, in my view, in keeping with the imperative of equality and equal treatment. However, the Constitutional Court has warned in *Bernstein v Bester* that since the right to privacy is linked to the right to dignity, companies will therefore have a lesser protection of their privacy then natural persons because they are considered to have less (if any) dignity). The right to privacy is protected both in relation to intrusion into a person's life by the state or by other individuals.[63]

Section 14 of the Constitution has two parts. The first guarantees a general right to privacy, the second part protects against specific infringements of privacy, namely, searches and seizures and infringements of the privacy of communications.[64] De Waal[65] state that in most cases when one's person, home or property is searched, or when one's possessions are seized or communications intercepted, s 14 will be infringed. However, he says that, because the right against searches and seizures is a

---

[62] Section 8(4) of the Constitution provide the following:

> "A juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of that juristic person."

See also *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2000 (10) BCLR 1079 (CC); 2001 (1) SA 545 (CC) 17 *(Hyundai* case) and see note 45 above.

[63] LAWSA First Reissue vol 5 part 3 para 45.

[64] See Devenish (above note 1) 138.

[65] De Waal (above note 20) 268.

subordinate element of the right to privacy, the Constitution's protection is triggered only when an applicant shows that a search, seizure or interception of communication has infringed the general right to privacy. This is correct, it is clear from the wording of s 14. The specific rights are placed within the parameters of the general right to privacy. What this means therefore, is that, communications may be intercepted, however, in order for an aggrieved party to seek protection in terms of the Constitution, the person will have to prove that such an interception violated his or her privacy (the general right).

De Waal et al[66] states that the right enshrined in s14 of the Constitution extends only to aspects of ones life or conduct in regard to which a legitimate expectation of privacy can be harboured. He says that a "legitimate expectation" means that one must have a subjective expectation of privacy that society recognises as objectively reasonable.[67] The reasonable expectation of privacy test comprises two questions. First, there must be a subjective expectation of privacy and, secondly, the expectation must be recognised as reasonable by society.[68] What amounts to "reasonable" will depend on the changing beliefs and values of the South African society. This will have to be in accordance with the spirit, purport and objects of the Constitution, having regard to other rights protected in the Constitution.

The question of a violation of the right to privacy involves a two stage enquiry. Firstly, the scope of the right to privacy must be assessed to determine whether law or conduct has infringed the right. If an infringement is proved then it must be determined whether it is justifiable under the limitation clause.[69] McQuoid says that the first constitutional enquiry is analogous to the policy-based enquiry into the unlawfulness stage of the common law. In both instances the subjective expectation of privacy must be reasonable. The second enquiry deals with the justification of the infringement of the right to privacy in terms of s 36 of the Constitution and must be discharged on a balance of probabilities.[70]

---

[66] De Waal (above note 20) 265. See also *Protea Technology Ltd and Another v Wainer and Others* 1997 (9) BCLR 1225 (W); *Bernstein* (above note 20) 792G – I.
[67] This is a test that is followed in the United States and Canada.
[68] See also *Bernstein* (above note 20) 793.
[69] McQuoid-Mason (above note 55) 246.
[70] Ibid 246 – 247.

In *National Coalition for Gay and Lesbian Equality v Minister of Justice and Others*[71] the Constitutional Court held that the right to privacy is closely related to the right to dignity.[72] Ackerman held that privacy recognises that we all have a right to a sphere of private intimacy and autonomy which allows us to establish and nurture human relationships without interference from the outside community.[73]

Sachs J, in the same case (*National Coalition)*, held that the right to privacy is not only a negative right but also a positive right.[74] The learned judge quoting an American case of *Bowers, Attorney General of Georgia v Hardwick et al*[75] had the following to say:

> It has become a judicial cliché to say that privacy protects people, not places. Blackmun J in *Bowers, Attorney General of Georgia v Hardwick et al* made it clear that the much-quoted "right to be left alone" should be seen not simply as a negative right to occupy a private space free from government intrusion, but as a right to get on with your life, express your personality and make fundamental decisions about your intimate relationships without penalisation. Just as "liberty must be viewed not merely 'negatively or selfishly as a mere absence of restraint, but positively and socially as an adjustment of restraints to the end of freedom of opportunity'", so must privacy be regarded as suggesting at least some responsibility on the State to promote conditions in which personal self-realisation can take place.[76]

Whether South Africa has acted on its responsibility to promote conditions in which personal self-realisation can take place, is another matter. With so much legislation being enacted to allow the government to intercept and monitor communications it is doubtful whether there is such promotion.

---

[71] 1998 (12) BCLR 1517 (CC); 1999 (1) SA 6 (CC).
[72] Ibid 30.
[73] Ibid 32.
[74] Concurring with the majority of the court but for different reasons.
[75] 478 US 186 (1985).
[76] Para 116.

In *Bernstein and Others v Bester and Others NNO*[77] the Constitutional Court was dealing with s 13 of the Interim Constitution.[78] The issue was the constitutionality of s 417 and 418 of the Companies Act[79]. These sections provided for the examination of persons and the disclosure of documents as to the affairs of a company in the course of a winding up. Ackerman J held that:

> "The relevance of such an integrated approach to the interpretation of the right to privacy is that this process of creating context cannot be confined to any one sphere, and specifically not to an abstract individualistic approach. The truism that no right is to be considered absolute, implies that from the outset of interpretation each right is always already limited by every other right accruing to another citizen. In the context of privacy this would mean that it is only the inner sanctum of a person, such as his/her family life, sexual preference and home environment, which is shielded from erosion by conflicting rights of the community. This implies that community rights and the rights of fellow members place a corresponding obligation on a citizen, thereby shaping the abstract notion of individualism towards identifying a concrete member of civil society. Privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly."[80]

This view is in accordance with the reasonable expectation of privacy test. As an example, it has been held that an employee using the resources of the employer (for example, e-mail facility), cannot legitimately have an expectation of privacy in the communications that he or she engages himself or herself in. The court has held that where the employee is discussing businesses of the employer with a third party, he or

---

[77] *Bernstein* (above note 20).

[78] Section 13 of the Interim Constitution was the equivalent section to s14 of the Final Constitution. Section 13 read as follows:

> "Every person shall have the right to his or her personal privacy, which shall include the right not to be subject to searches of his or her person, home or property, the seizure of private possessions or the violation of private communications." The difference, if any, between the two sections is not a matter for discussion in this work.

[79] Act 61 of 1973.

[80] *Bernstein* (above note 20) 67.

she cannot claim privacy in the event that the employer monitors or intercept his or her communication.[81]

In *Case and Another v Minister of Safety and Security and Others; Curtis v Minister of Safety and Security and Others*[82] the Constitutional Court had to decide on the constitutionality of s 2(1) of the Indecent or Obscene Photographic Matter Act[83] which provided that any person who had in his or her possession any indecent or obscene photographic matter shall be guilty of an offence and liable on conviction to a fine not exceeding one thousand rand or imprisonment for a period not exceeding one year or to both such fine and such imprisonment.

Didcott J for the court held that

> "What erotic material I may choose to keep within the privacy of my home, and only for my personal use there, is nobody's business but mine. It is certainly not the business of society or the State. Any ban imposed on my possession of such material for that solitary purpose invades the personal privacy which section 13 of the Interim Constitution (Act 200 of 1993) guarantees that I shall enjoy. Here the invasion is aggravated by the preposterous definition of "indecent or obscene photographic matter" which section 1 of the statute contains. So widely has it been framed that it covers, for instance, reproductions of not a few famous works of art, ancient and modern, that are publicly displayed and can readily be viewed in major galleries of the world. That section 2(1) clashes with section 13 seems to be indisputable."[84]

Mokgoro J, dissenting, disagreed with this view stating that:

> "I would, however, respectfully part company from Justice Didcott to the extent that any part of his opinion might be read to suggest that it is not in any circumstances the business of the State to regulate the kinds of expressive

[81] See for example *Protea Technology* (above note 66) in this regard.
[82] 1996 (5) BCLR 609 (CC); 1996 (3) SA 617 (CC).
[83] Act 37 of 1967.
[84] *Case* (above note 87) 91.

material an individual may consume in the privacy of her or his own home. It may be so that, as in England, a "South African's home is his (or her) castle." But I would hesitate to endorse the view that its walls are impregnable to the reach of governmental regulation affecting expressive materials. I therefore associate myself with the caveat expressed by Justices Langa and Madala regarding Justice Didcott's opinion."[85]

It is submitted that the approach adopted by the late Didcott J is too liberal even for a democratic South Africa. The writer agrees with the view expressed by Mokgoro J that there will be instances where it will be the business of the state to mind what its subjects do, where there will be a need to regulate the kinds of material individuals possess or use. A terrorist group, as an example, cannot be heard to be raising a right to privacy where their e-mails communications have been monitored or/ and intercepted by government officials so as to provide evidence of their criminal acts. Even if they can successfully prove an invasion of privacy, the law still permits such evidence being used in a court of law against such culprits.[86]

Sachs J, in the *Mistry* case[87] held that the terms "search" and "seizure", in s 13 of the Interim Constitution, may be interpreted in a particular case, to the extent that a statute that authorises warrantless entry into private homes and rifling through intimate possessions, would intrude on the "inner sanctum" of the persons in question and the statutory authority would accordingly breach the right to personal privacy as protected by section the Constitution. However Sachs J refrained from answering when, exactly, does an inspection become a search for the purposes of the Constitution and also from deciding what "property" means.

The right to privacy, like other rights in the Bill of Rights, is not absolute and can be limited in terms of s 36 of the Constitution. Even if it is proved that there has been a violation of the right to privacy, that such a violation is not justifiable and reasonable

---

[85] Ibid 65.
[86] See s 35(5) of the Constitution. For a discussion of this, see *S v Naidoo* 1998 (1) BCLR 38 (D); *Tap Wine Trading CC v Cape Classic Wines (Western Cape) CC* 1999 (4) 194 (C); *Protea Technology* (above note 66); *S v Dube* 2000 (6) BCLR 685 (N); 2000 (2) SA 583 (N); 2000 (1) SACR 53 (N) discussed below.
[87] *Mistry v Interim National Medical and Dental Council of South Africa* 1998 (7) BCLR 880 (CC); 1998 (4) SA 1122 (CC),16.

in terms of the Constitution, this however, does not prevent government officials especially the police, from using any evidence obtained in violation of the right to privacy in a court of law as evidence.

In *S v Bierman*[88] the applicant was seeking leave to appeal against a decision of the Supreme Court of Appeals in terms of Rule 20 of the Rules of the Constitutional Court. The applicant had been convicted on a basis of her confession that she made to a certain Reverend Bothma confessing her guilt to a crime of murder.

O'Regan J, for a unanimous Court, examined *Smit v Van Niekerk NO en n' Ander*[89] where the Appellate Division (as it then was), rejected an argument that public policy required that statements made to a clergyman be privileged.

It is submitted that the Constitutional Court's reliance in the *Smit* decision was misplaced considering the fact that this decision was decided almost over 28 years prior to the coming into operation of both the Interim Constitution and the Final Constitution before we had a constitutionally protected right to privacy. However this argument was raised in the lower court in *Bierman* and was rejected by Bosielo J on the basis that it was in the interests of justice to admit the evidence.[90]

Unfortunately the Constitutional Court refused to decide the issue on the basis that some of the constitutional issues were being raised before the Court for the first time without the Constitutional Court having the benefit of the decision and analysis of the Supreme Court of Appeals. The court held that it was not in the interests of justice for it to grant leave to appeal.[91]

In *S v Nkabinde*[92] the court held that the accused's right to privacy was violated in that the police monitored conversations between the accused and his legal representatives. Although authorisation under the Monitoring Act was obtained, the interception of

---

[88] 2002 (5) SA 243 (CC); 2002 (10) BCLR 1078 (CC).
[89] 1976 (4) SA 293 (AD).
[90] See *Bierman* (above note 88) 5 in this regard.
[91] At para 9.
[92] 1998 (8) BCLR 996 (N).

this type of communication was not provided for by the Monitoring Act.[93] In any event, such monitoring invades the attorney-client privilege.

Protea Technology Ltd and Another v Wainer and Others[94] was an application for an interdict based on a restraint of trade agreement. The applicants had attached to their founding affidavit what purported to be transcripts of tape recordings of telephonic conversations in which the first respondent participated. Initially, according to the founding affidavit, a telephone monitoring device had been placed on the telephone in the office occupied by the first respondent in the business premises of the applicants. After it was realised that the first respondent was deliberately making use of a cell-phone to obviate the possibility of telephone-tapping, a different monitoring device was placed in the office of the first respondent which picked up only the voice of the first respondent.

The respondents applied to strike out all evidence in the founding affidavit about the telephone calls. The grounds were twofold: first, that the applicants and those responsible for monitoring the calls and making the recordings on their behalf committed an offence under section 8(1) of the Interception and Monitoring Prohibition Act[95]; second, that the making and use of the recordings in these proceedings would infringe the first respondent's rights of privacy embodied in section 14(d) of the Constitution.

The court, per Heher JA, upon examining the provisions of the Interception and Monitoring Prohibition Act, held that the Act does not define "confidential information" but that the expression must surely mean such information as the communicator does not intend to disclose to any person other than the person to whom he is speaking and any other person to whom the disclosure of such information is necessarily or impliedly intended to be restricted. The court held that there is a distinction between "confidential" information and "private" information.

---

[93] At 1001 I – 1002 B.
[94] *Protea* (above note 66)
[95] Act 27 of 1992. This Act has been repealed by the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (Regulation Act).

Confidentiality can exist even in relation to the communication of information which is in the public domain or is the property of another and, therefore, not private.[96]

The court stressed that, in terms of the Act, the information must be that "concerning any person, body or organisation".[97]

The judge made the following finding regarding the Act:

> "From the above-mentioned statutory prescriptions the following inferences may fairly be drawn:
>
> 1. The legislature regards the conduct of intercepting and monitoring which it prohibits in section 2 as potentially grave offences meriting substantial penalties.
> 2. The criminal consequences of such conduct are to be the lot of any person who engages in it unless he can bring himself within the terms of a direction issued by a judge.
> 3. The potential to obtain such a direction is very strictly controlled. It could, for example, hardly be issued on mere suspicion unsupported by hard facts.
> 4. Having regard to the prescribed content of the application for a direction, such an authorisation if not available to a party who wishes to use it for the purpose of pursuing a civil interest, such as the investigation of a breach of a restraint of trade agreement, no matter how serious the damage which may be threatened. The secrecy provisions in section 7 bear out this conclusion.
> 5. The Act does not authorise interception or monitoring *ex post facto*."

The *Protea Technology* case dealt with the right of an employer to monitor or intercept private communications of an employee. The court said that if the

[96] At 1234 D - F.
[97] Ibid paraG.

communication concerns the employer then the employer had a right to do whatever necessary to get that information. However, it must be remembered that this work is not looking at situations between employer and employees but the government and its 'subjects'.

On the question of the status of evidence placed before a court of law in event that such evidence has been obtained as a result of unconstitutional and unlawful monitoring or interception, the court held that the statute does not expressly or by necessary inference render the production of recordings made in contravention of its terms inadmissible in evidence before a court trying a civil dispute.[98] The court held that courts have discretion whether to accept such evidence.[99]

The writer agrees with this conclusion. From the wording of the Act (the Monitoring Act), there was nothing that could have led to a conclusion that the legislature had the intention to exclude any evidence obtained in violation of this Act. To find otherwise would be to add meaning which was never intended by the legislature.

Later, the learned judge looked at the difference between criminal cases and civil cases in as far as the right against intrusions is concerned. He made the following remarks:

> "This is not a case where the State bears a criminal onus. The accused is not presumed innocent. This is a civil dispute where each party accuses the other of dishonesty and improper motives. It would be quite wrong to allow one party to damage and malign the other while depriving the latter of relevant material at its disposal to disprove such allegations, all for the sake of upholding a right which, in all the circumstances, should not need to be invoked at all unless there is something to hide."[100]

[98] At 1237D.
[99] At 1239A.
[100] At 1243I – 1244A.

This, it is submitted, constitute a distinction without a difference. There is no indication that South African courts are prevented in any way from using improperly obtained evidence be it they are faced with a civil matter or a criminal case.

From the above, it is clear that the right "to be left alone"[101] is not only part of our Constitution, which is the supreme law of the land, but it has also been endorsed by the courts of law, especially the Constitutional Court which is the guardian of the Constitution.

In *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others*[102] the Constitutional Court had to decide on the constitutionality of the National Prosecuting Authority Act[103]. This Act makes provision for the search and seizure of property by an Investigating Director in the office of the National Director of Public Prosecutions, to facilitate the investigation of certain specified offences. The power to search and seize property may be exercised on the authority of a warrant issued by a judicial officer. This case concerned the constitutionality of the provisions that authorise the issuing of warrants of search and seizure for purposes of a "preparatory investigation", one of two investigatory procedures provided for in Chapter 5 of the Act.

The warrant authorises the examination and seizure of any object, the copying of, or the taking of portions from any document or book located on or in the premises, that has or may have a bearing on the inquiry or preparatory investigation, as the case may be. This of course includes electronic communications because of the wide definition of the word 'document' in the *Oxford English Dictionary*.[104]

Langa DP held that the right to privacy, does not however, relate solely to the individual within his or her intimate space. 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

---

[101] As used by Ackerman J in *Bernstein* (above note 20).
[102] *Hyundai* (above note 62).
[103] Act 32 of 1998.
[104] See note 8 above. The word is defined as "Something written, inscribed, etc., which furnishes evidence or information upon any subject, as a manuscript, title-deed, tomb-stone, coin, picture, etc."

unless certain conditions are satisfied. Wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable, the right to privacy will come into play.[105]

In as much as this view adopted by Langa DP makes a lot of sense, from all the cases discussed in this work, the writer has difficulty believing that this is indeed the state of affairs. Allowing for the use of such evidence in the court of law not only prejudices the victim of the invasion of privacy but also gives the law enforcement officers too much room to break the rules which seek to protect or preserve some form of autonomy i.e. protecting privacy.

In *Tap Wine Trading CC v Cape Classic Wines (Western Cape) CC*[106] the court had to decide whether participant surveillance (where one of the participants consenting to surreptitious recording of the conversation) is a breach of:

1. the Interception and Monitoring Prohibition Act; and/or
2. section 14 of the Constitution.
3. also, the court had to decide whether evidence obtained in violation of any of these statutes is admissible in the court of law.

The court per Prisman AJ, held that the provisions of the Interception and Monitoring Prohibition Act[107] and the Constitution s14 were not violated by participant surveillance in civil cases.[108] This was because civil cases involved individual parties and not the state. Applying the Canadian case of *R v Duarte*[109] the learned judge held that the purpose for having legislation that regulates the monitoring or interception of communications was to prevent the State from abusing its power to get information from its citizens. Therefore in a case where the State was not a party the danger of abusing the system did not exist.[110] Reinforcing the principles in the *Protea*

[105] Langa DP in the Hyundai case (above note 62) 16.
[106] *Tape Wine* (above note 86).
[107] Especially s 2 of the Act.
[108] At 197G-H.
[109] (1990) 53 CCC (3d) 1 (SCC).
[110] Prisman AJ 197G – 198H.

Technology case, the court held[111] further that even if the evidence was obtained improperly, illegally or unconstitutionally, the court still had the discretionary right to admit the evidence. The court stated that s 35(5) of the Constitution and the limitation clause, s 36 would permit such admission in civil cases where to do so would further the administration of justice.

S v Dube[112] dealt with participation monitoring. McCall J looked at the decision of *S v Malinga and Others* [113] where Holmes JA defined a trap as a person who, with a view to securing the conviction of another, proposes certain criminal conduct to him, and himself ostensibly takes part therein. In other words, he creates the occasion for someone else to commit the offence.[114]

McCall J noted that there is no defence of entrapment in South African law. However the learned judge stated that evidence of entrapment may, in certain circumstances, be excluded.[115] Endorsing the view expressed by Prisman AJ in the *Tap Wine* case, McCall J held that the Interception and Monitoring Prohibition Act was not applicable to participant monitoring. He looked[116] at the decision by Cameron J in *S v Kidson*[117] where it was held that:

> "The principle of interpretation *in favorem libertatis* obliges the conclusion that the prohibition in s 2(1)(b) of the 1992 statute applies in the first instance only to third party monitoring of conversations. Its primary signification is not to cover participant monitoring, i.e. when one of the parties to the conversation monitors it."[118]

---

[111] At 198G-H. See also Hurt J in *Lenco Holdings Ltd and Others v Eckstein and Others* 1996 (2) SA 693 (N) 704.
[112] Note 86 above.
[113] 1963 (1) SA 692 (A).
[114] *Malinga* 693 F – G.
[115] *Dube* (above note 86) 73 E – F.
[116] Ibid 75 G – H.
[117] 1999 (1) SACR 338 (W).
[118] *Kidson* 348 D – E.

The learned judge than said that the Monitoring Act prohibited the monitoring so as to gather confidential information concerning any person, body or organisation.[119] Therefore, there had to be a legitimate expectation of privacy.[120]

An interesting case dealing with the monitoring of communications is *S v Naidoo.*[121] This case involved the monitoring of cellular phones by police officials after the issuing of a warrant. The warrant had been issued in terms of the Interception and Monitoring Prohibition Act[122] on the furnishing of false or misleading information to the judge by the police to obtain the warrant. This Act provided as follows:

> Section 2. Prohibition on interception and monitoring.—
>
> (1) No person shall—
>
> (a) intentionally and without the knowledge or permission of the dispatcher intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line; or
>
> (b) intentionally monitor any conversation or communication by means of a monitoring device so as to gather confidential information concerning any person, body or organization.
>
> (2) Notwithstanding the provisions of subsection (1) or anything to the contrary in any other law contained, a judge may direct that—
>
> (a) a particular postal article or a particular communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line be intercepted;
>
> (b) all postal articles to or from a person, body or organization or all communications which have been or are being or are intended to be transmitted by telephone

[119] *Dube* (above note 86) 76 B.
[120] Ibid para F –G.
[121] Note 86 above.
[122] Monitoring Act (above note 95).

or in any other manner over a telecommunications line, to or from a person, body or organization be intercepted; or

(c) conversations by or with, or communications to or from, a person, body or organization, whether a telecommunications line is being used in conducting those conversations or transmitting those communications or not, be monitored in any manner by means of a monitoring device.

Section 3. Issue of direction.—

(1) A direction referred to in section 2 (2) may only be issued by a judge—

(a) designated by the Minister of Justice for the division—

(i) from where the postal article or communication referred to in section 2 (2) (a) or (b) has been or will probably be dispatched or transmitted or where that postal article or communication will probably be received; or

(ii) where the proposed monitoring referred to in section 2 (2) (c) will be carried out; and

(b) if the judge concerned is convinced, on the grounds mentioned in a written application that complies with the directives referred to in section 6—

(i) that the offence that has been or is being or will probably be committed, is a serious offence that cannot be properly investigated in any other manner and of which the investigation in terms of this Act is necessary; or

(ii) that the security of the Republic is threatened or that the gathering of information concerning a threat to the security of the Republic is necessary.

The question to be decided in this case, was whether evidence obtained by lawful means i.e. through a warrant issued by a judge which however was obtained through the use of misleading information, could regardless of this fact be admitted in a court of law. There were three grounds for the challenge to the evidence. The first was that the requirements of the Interception and Monitoring Prohibition Act had not been complied with and therefore that the monitoring was illegal in terms of the Act. The second was that certain information had been obtained from Mobile Telephone Network before subpoenas had been obtained in terms of s 205 of the Criminal Procedure Act[123] and that the subpoenas obtained did not, at least initially, comply with the requirements of that section. Thirdly, it was contended that the accuseds' right to privacy had been infringed and that the result of the admission of the evidence of the two telephonic conversations would infringe the accuseds' right to a fair trial.

McCall J after examining s 35(5) of the Constitution, held that even if evidence violated a right in a Bill of Rights, in terms of this section such evidence may still be admissible if such admission will not bring the administration of justice into disrepute.[124]

McCall J examined [125] at *Key v Attorney-General, Cape of Good Hope Provincial Division and Another*[126] where Kriegler J said the following:

> Even if one were to accept that the section was constitutionally invalid, and even if one were further to assume that such invalidity in turn rendered the prior searches and seizures unlawful, it does not follow that the evidence obtained directly or derivatively as a result of such searches and seizures would necessarily be inadmissible in criminal proceedings against the person from whom the documents containing, or pointing to, the evidence were seized.[127]

Later in the *Key v Attorney-General* judgment Kriegler J stated that:

---

[123] Act 51 of 1977.
[124] *Naidoo* (above note 86) 489 F – J.
[125] Ibid 494 E.
[126] 1996 (6) BCLR 788 (CC); 1996 (4) SA 187 (CC).
[127] Ibid 794 G – 795 A.

> "In any democratic criminal justice system there is a tension between, on the one hand, the public interest in bringing criminal to book and, on the other, the equally great public interest in ensuring that justice is manifestly done to all, even those suspected of conduct which would put them beyond the pale. To be sure, a prominent feature of that tension is the universal and unceasing endeavour by international human rights bodies, enlightened legislatures and courts to prevent or curtail excessive zeal by state agencies in the prevention, investigation or prosecution of crime. But none of that means sympathy for crime and its perpetrators. Nor does it mean a predilection for technical niceties and ingenious legal stratagems. What the Constitution demands is that the accused be given a fair trial. Ultimately, as was held in *Ferreira v Levin*, fairness is an issue which has to be decided upon the facts of each case, and the trial Judge is the person best placed to take that decision. At times fairness might require that evidence unconstitutionally obtained be excluded. But there will also be times when fairness will require that evidence, albeit obtained unconstitutionally, nevertheless be admitted."[128]

This view clearly reinforces the decisions that had been discussed in this work which states that even in cases where ones privacy has been infringed, however courts will still accept such evidence. Whether as a new democracy we do require such a principle is a question that needs to be answered. Violating the right to privacy of communications does not only infringe or deprive individuals of their right to privacy but also goes to the core of another very important right in this democracy- freedom of expression. It is submitted that one cannot fully enjoy the right to free speech while knowing very well that what he or she might say or write might be intercepted or monitored. The right to free speech is however, not part of this discussion.

McCall, in the *Naidoo* case concedes that the Interception and Monitoring Prohibition Act was a law of general application in terms of the limitation clause of the Constitution.[129] The judge therefore held that if the monitoring of a conversation was not authorised by a direction properly and lawfully issued by a judge in terms of s 3 of

[128] Ibid 795 F – 796 B.
[129] *Naidoo* (above note 86) 505 A.

the Act, then not only would such monitoring constitute a criminal offence in terms of the Monitoring Act, it would also constitute an infringement of the right to privacy, which includes the right not to be subject to "the violation of private communications".[130]

On the question of the giving of false or misleading information in the motivation for a direction the learned judge stated that:

> "The giving of false or misleading information in the motivation of a direction in terms of subsection 2 and 3 of the Monitoring Act strikes at the very foundation of the exemption contemplated by the Legislature to the declared illegality of, *inter alia*, monitoring conversations in order to gather confidential information."[131]

In *S v Madiba and Another,*[132] the court dealt with evidence obtained without a warrant in terms of s 41 of the Arms and Ammunition Act.[133] The court, per Hurt J, held that the Interim and Final Constitution are drafted in very similar form in so far as the right to privacy is concerned.[134] The court held that that the Constitution must govern the question of whether the evidence must be admitted or excluded.[135] Also, that section 35(5) of the Constitution gives the plainest of indications that the court conducting the trial is vested with a discretion, which it must exercise in order to achieve the object of the section. That object, to paraphrase the section, must be to hold a trial which is fair and not "detrimental to the administration of justice".[136]

The writer agrees with the view expressed by McQuoid-Mason when, after reviewing South African law and referring to the United States, he concludes that foreign jurisprudence suggests that the privacy provisions of the interim Constitution should be interpreted to exclude evidence obtained as a result of the breach of privacy provisions, because *(a)* the courts should not appear to condone lawlessness by law

---

[130] Ibid 507 A.
[131] Ibid 524 G – H.
[132] 1998 (1) BCLR 38 (D).
[133] Act 75 of 1969.
[134] *Madiba* (above note 134) 43D – E.
[135] Ibid 44C.
[136] Ibid 44E – F.

enforcement officials, and *(b)* the exclusionary rule is a necessary requirement in a constitutional democracy.[137]

In *S v Naidoo*[138] McCall J referred to [139] McQuoid-Mason[140] where the learned author suggested that the provisions[141] of the Interception and Monitoring Act may well be open to scrutiny by the Constitutional Court to determine whether or not they are reasonable and justifiable in terms of the limitation clause.

In as much as the Monitoring Act has been repealed, the writer has difficulties believing that the Act or its successor could have or can (with regard to the successor) fail constitutional muster as suggested by McQuoid-Mason. The decisions of the Constitutional Court in *Bernstein; Mistry; Hyndai; Case* and other cases that are discussed in this work, show that the Constitutional Court's jurisprudence is that:

1. Everyone has a right to privacy in terms of the Constitution and the common law;
2. The rights in the Bill of Rights are not absolute and therefore can be limited by law of general application, which limitation must be reasonable and justifiable in a democratic society;[142]
3. Statutes which authorise an invasion into ones privacy, that are regulated by the requirement of a warrant or some authority, are reasonable and justifiable limitations of the right to privacy.[143]

Before examining legislation that limits the right to privacy one need to ascertain whether a potential litigant need to prove any fault on the part of the invader for a constitutional cause of action. The writer is of the opinion that South African courts have not given a ruling on whether or not there is a requirement of fault in order for a defendant to be liable for an invasion of a constitutional right to privacy. It is submitted that there is no requirement of fault in our constitutional jurisprudence of

---

[137] In Chaskalson *et* al (above note 11) 18, 18-13.
[138] Above note 86.
[139] Ibid 504 I – J.
[140] McQuoid-Mason (above note 11).
[141] Section 2(2) and 3 of the Act.
[142] See the discussion on the Limitation Clause Chapter 3 below.
[143] See in this regard Sachs J in *Mistry* (above note 87).

the right to privacy. The constitutional text itself (s 14 to be specific) is silent in this regard. McQuoid-Mason states that fault is not a requirement for a constitutional invasion of privacy.[144] Therefore one can safely conclude that there is strict liability when it comes to invasions of the constitutional right to privacy. This is quite different from the common law right to privacy. The common law right, as discussed above, clearly requires a degree of fault, the so-called *animus injuriandi*. Whether this distinction between the right to privacy at common law and that in terms of the Constitution will call for the development of the common law by the South African courts in terms of s 39(2) of the Constitution, is another issue which thus far, courts have not been called upon to decide.

As will be seen in Chapter 3 below, a different approach is required when a court deals with a constitutional challenge to a rule of the common law. The superior courts are the interpreters and expounders of the common law. They have always had an inherent power to refashion and develop the common law in order to reflect the changing social, moral and economic make-up of society[145]. That power is now constitutionally authorised[146] and must be exercised within the prescript and ethos of the Constitution. In this regard, Kentridge AJ[147] warns that:

> ". . . that judges should not be quick to perpetuate rules whose social foundation has long since disappeared. Nonetheless, there are significant constraints on the power of the judiciary to change the law. In a constitutional democracy such as ours, it is the legislature and not the courts, which have the major responsibility for law reform. The judiciary should confine itself to those incremental changes which are necessary to keep the common law in step with the dynamic and evolving fabric of our society."

---

[144] David McQuoid-Mason (note 55 above) 246.
[145] *Amod v Multilateral Motor Vehicle Accident Fund* 1998 (10) BCLR 1207 (CC); 1998 (4) SA 753 (CC) 22.
[146] Sestions173 and 8(3).
[147] *Du Plessis v De Klerk* 1996 (3) SA 850 (CC); 1996 (5) BCLR 658 (CC), 691-2.

What then is recourse for an aggrieved party whose right to privacy has been violated and such violation is not justifiable in terms of s 36 of the Constitution?[148] Section 172(1) of the Constitution provides the following:

> 172. Powers of courts in constitutional matters.—
> (1) When deciding a constitutional matter within its power, a court—
> (a) must declare that any law or conduct that is inconsistent with the Constitution is invalid to the extent of its inconsistency;
> . . .

The court may also grant 'appropriate relief', including a declaration of rights, to any person who alleges and proves that a right in the Bill of Rights has been infringed or threatened.[149]

Section 38 provides the following:

> 38. Enforcement of rights.—
> Anyone listed in this section has the right to approach a competent court, alleging that a right in the Bill of Rights has been infringed or threatened, and the court may grant appropriate relief, including a declaration of rights.
> . . .

It has been said that there are essentially three broad categories of constitutional remedies:

1. constitutional damages;
2. interdicts; and
3. declarations of invalidity.[150]

What has been discussed in this Chapter shows that in South Africa, individuals have a limited right to privacy like most citizens in other foreign jurisdictions.[151]

---

[148] The limitation clause will be discussed below in Chapter 3.5.
[149] Section 38 of the Constitution.
[150] McQuoid-Mason (above note 55) 256. The learned author points out that these categories of remedies are not closed and the courts have the power to grant any other 'appropriate remedy'.

Therefore, the right to privacy, like most of the rights in the Constitution, can be limited in terms of s36 of the Constitution if such a limitation is reasonable and justifiable in an open and democratic society based on equality and freedom. The right may also be suspended in consequence of the declaration of a state of emergency, but only to the extent that the derogation is strictly required by the emergency and the legislation enacting the state of emergency is consistent with South Africa's obligations under international law applicable to states of emergency.[152]

What is to follow is an examination of various Acts which constitute an invasion of the right to privacy both at common law and in terms of s 14 of the Constitution. Firstly, the writer will examine how these Acts infringe the right to privacy and secondly, whether these Acts constitute a justifiable limitation of the right in terms of the Constitution.[153]

---

[151] See note 3 above.

[152] See s 37 of the Constitution; see also R Buys, *CyberLaw @ SA: The Internet and The Law in South Africa* (2000) 368.

[153] It must be noted that not all South African Acts which purport to limit the right to privacy will be discussed. Only those that the author considers to be of importance to electronic communications will be looked at.

Chapter 3: Legislation authorising invasions of private e-mail communications:

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

One cannot deny the importance of the State's interest in ensuring that the privacy of people's communications is protected and also that law enforcement in South Africa is not compromised. The Regulation of Interception of Communications and Provision of Communication-Related Information Act (Regulation Act) repeals[154] the Interception and Monitoring Prohibition Act.[155] McCall in *Naidoo,* looking at the provisions of the Monitoring Act expressed his views on the importance of such a regulation in the following way:

> "The legislature was at pains, even before the adoption of the interim Constitution, to express its disapproval of the monitoring of conversations, by passing the Monitoring Act, whilst, at the same time, acknowledging the necessity to permit such monitoring for the purpose of investigating serious crimes, under strictly controlled circumstances. Both the interim Constitution and the new Constitution affirm the Legislature's commitment to the concept of protection of private communications against violation or infringement. To countenance the violations in this case would leave the general public with the impression that the courts are prepared to condone serious failures by the police to observe the laid-down standards of investigation so long as a conviction results."[156]

It therefore seem, from this *dictum*, that in as much as there is a need to combat crime, the primary purpose of having legislation that authorise, to a limited degree, invasions of privacy, is to protect privacy as was enshrined in the Interim Constitution and now reiterated in the Final Constitution.

---

[154] See s 69 of the Regulation Act.

[155] See above note 92. At the time this work is written there are no cases interpreting or applying the provisions of the Regulations Act, therefore I will constantly make use of the cases that were decided under the previous Act (the Monitoring Act), for example *Tap Wine; Naidoo; Dube; Protea Technology* and so forth, see note 86 above.

[156] *S v Naidoo* (above note 86) 530 F – H.

The Regulation Act differentiates between direct communication and indirect communication. Section 1 of the Act defines direct communication to mean 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 an utterance by a person who is participating in an indirect-communication, if the utterance is audible to another person who, at the time that the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication. An example of a "direct communication" will be a situation where people present at the same place and time engage in a dialogue. What is however clear is that "direct communication" does not cover e-mail communication.

Indirect-communication, on the other hand, is defined to mean the transfer of information, including a message or any part of a message, whether in a form of speech; music or other sounds; data; text; visual images (whether animated or not); signals or radio frequency spectrum. It also includes the transfer of information 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.[157]

An e-mail communication is defined in the *Oxford English Dictionary* as the system of sending text, pictures, etc to other people by means of computers linked to a network; information sent by this method.[158] Looking at this dictionary definition and the definition of indirect communication found in s 1 of the Regulation Act, it is submitted that it is beyond question that e-mail communication falls within indirect communication in terms of the Act. Therefore, an e-mail communication amounts to an "indirect communication" in terms of the Act.

Unlike its predecessor, the Regulation Act's definition of "a serous offence" is broader than the one that was contained in the Monitoring Act. The Regulations Act defines "serious offence" as follows:

---

[157] See s 1 of the Regulations Act for a definition of "direct and indirect communication".
[158] *Oxford English Dictionary*, Oxford University Press 2003.

"serious offence" means any:

(a) offence mentioned in the Schedule[159]; or

(b) offence that is allegedly being or has been or will probably be committed by a person, group of persons or syndicate:

(i) acting in an organised fashion which includes the planned, ongoing, continuous or repeated participation, involvement or engagement in at least two incidents of criminal or unlawful conduct that has the same or similar intents, results, accomplices . . .

(ii) acting in the execution or furtherance of a common purpose or conspiracy; or

(iii) which could result in substantial financial gain for the person, group of persons or syndicate committing the offence.

Including any conspiracy, incitement or attempt to commit any of the abovementioned offences.[160]

---

[159] The Schedule provides the following: Serious Offences

Section 1: high treason; any offence relating to terrorism; any offence involving sabotage; sedition; any offence which could result in the loss of a person's life or serious risk of loss of a person's life; any offence referred to in Schedule 1 to the Implementation of the Rome Statute of the International Criminal Court Act, 2002 (Act No. 27 of 2002); any specified offence as defined in section 1 of the National Prosecuting Authority Act; any offence referred to in Chapters 2, 3 and 4 of the Prevention of Organised Crime Act; any offence referred to in section 1 3 (f) of the Drugs and Drug Trafficking Act, 1992 (Act No. 140 of 1992); any offence relating to the dealing in or smuggling of ammunition, firearms, explosives or armament and the unlawful possession of such firearms, explosives or armament; any offence under any law relating to the illicit dealing in or possession of precious metals or precious stones; any offence contemplated in section 1 (1) of the Corruption Act, 1992 (Act No. 94 of 1992); dealing in, being in possession of or conveying endangered, scarce and protected game or plants or parts or remains thereof in contravention of any legislation; and any offence the punishment wherefore may be imprisonment for life or a period of imprisonment prescribed by section 51 of the Criminal Law Amendment Act, 1997 (Act No. 105 of 1997), or a period of imprisonment exceeding five years without the option of a fine.

[160] See s 1 of the Regulation Act for the definition of "serious offence". The Monitoring Act defined "serious offence" to mean:

(a) any offence mentioned in Schedule 1 to the Criminal Procedure Act, 1977 (Act No. 51 of 1977), including any conspiracy, incitement or attempt to commit any offence referred to in that Schedule, provided that—

(i) that offence is allegedly being or has allegedly been committed over a lengthy period of time;

(ii) that offence is allegedly being or has allegedly been committed on an organized basis by the persons involved therein;

(iii) that offence is allegedly being or has allegedly been committed on a regular basis by the person or persons involved therein; or

(iv) that offence may allegedly harm the economy of the Republic; or

(b) any offence referred to in sections 13 (f) and 14 (b) of the Drugs and Drug Trafficking Act, 1992;

It is submitted that there are no problems with this broad definition. From the wording of the section, the intention of the legislature seem to have been to discourage syndicates, gangs, people acting in the furtherance of a common purpose which most importantly for financial gain or which will threaten the safety and well being of the Republic.

Chapter 2, Part 1 of the Act prohibits the interception of communications in the course of its occurrence or transmission without a warrant. It is important to note that, in the case of e-mail messages, it is only those messages which are still in transit that the prohibition in terms of s 2 applies, messages which have not yet reached the potential receiver. This is also clear from the definition of "interception" in s 1 of the Act. The section defines "intercept" to mean:

> "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."

Unlike the Monitoring Act, the Regulation Act expressly allows for "party interceptions" i.e. where one of the parties to the communication intercept the communication. This does not require any authorisation be it in a form of a warrant or otherwise.[161] Also, the Act allows for the interception of communication by a third

---

(c) any specified offence as defined in section 1 of the National Prosecuting Authority Act, 1998 (Act No. 32 of 1998).

[161] See s 4 on interception of communication by party to communication.

party in the event that one of the parties consents to such an interception. Like "party interception", there is no requirement of a warrant in this case.[162]

A warrant is not always a requirement in terms of the Act. Section 7[163] provides that any law enforcement officer may intercept a communication without a warrant if he or she is satisfied that there are reasonable grounds to believe that a party to the communication has caused or may cause serious bodily harm and that because of the urgency of the need to intercept the communication, it is not reasonably practicable to make an application for the issuing of a direction to intercept.

Section 49 states that 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. Of course this section does not apply to cases which are exempted from the Act, for example, where a warrant has been issued, one of the parties to the communication consents to the interception by a third party or one of the parties to the communication is intercepting the communication.

It is submitted that the Regulation Act might stand a chance of surviving constitutional muster, if it had to be challenged on its constitutionality. The Act

---

[162] This clearly limits free expression which unfortunately is not within the scope of this work.

[163] Section 7(1) provides:

> **Interception of communication to prevent serious bidily harm**
>
> 7. (1) Any law enforcement officer may, if -
>
> (a) he or she is satisfied that there are reasonable grounds to believe that a party to the communication has-
>
> (i) caused, or may cause, the infliction of serious bodily harm to another person;
>
> (ii) threatens, or has threatened, to cause the infliction of serious bodily harm to another person; or
>
> (iii) threatens, or has threatened, to take his or her own life or to perform an act which would or may endanger his or her own life or would or may cause the infliction of serious bodily harm to himself or herself;
>
> *(b)* he or she is of the opinion that because of the urgency of the need to intercept the communication, it is not reasonably practicable to make an application in terms of section 16(1) or 23(1) for the issuing of an interception direction or an oral interception direction; and
>
> (c) the sole purpose of the interception is to prevent such bodily harm, intercept any communication or may orally request a telecommunication service provider to route duplicate signals of indirect communications specified in that request to the interception centre designated therein.

makes provision for the issuing of a warrant authorising interceptions or monitoring of communications. In as much as there is an exception to the warrant procedure, the writer thinks that the government will not have difficulty arguing that the exception is reasonable and justifiable in an open and democratic society. It is clear that it can never be possible for police officials to always obtain a warrant if they need to intercept or monitor private communications. There will definitely be cases of utmost urgency which, if the procedure of obtaining a warrant had to be followed, might lead to the defeat of the administration of justice.

However, the writer has difficulties accepting the notion of "participant surveillance" without a requirement of a warrant. Not only does it violate other freedoms guaranteed in the Bill of Rights (for example: free speech and association) but there does not seem to be a rational basis in support of this notion. The United States approach, when dealing with participant surveillance, is that authority still needs to be obtained by a party who will be intercepting or monitoring the conversation. Such an approach is needed in a democratic state where values and norm are based on protecting and respecting the autonomy of an individual.

One of the safeguards of the Act is that it allows for officials to apply for a warrant authorising an interception or monitoring of communication. The application for, and issuing of, an interception direction is provided for in terms of s 16 of the Act. The warrant can only be issued by a judge of the High Court.[164] Also, before a judge can issue a direction in terms of this section he or she must be satisfied that a number of factors exists, which includes that there are reasonable grounds for believing that a serious offence has been or will probably be committed, that (depending on the circumstances) other investigative procedures have been applied and have failed to produce the required evidence.[165]

---

[164] See s 1 for the definition of a "designated judge".

[165] Section 16(5)(a)-(c) states that:

An interception direction may only be issued if the designated judge concerned is satisfied, on the facts alleged in the application concerned, that:

a) there are reasonable grounds to believe that –

i) a serious offence has been or is being or will probably be committed;

ii) the gathering of information concerning an actual threat to the public health or safety, national security or compelling national economic interests of the Republic is necessary;

The Act places too many duties on service providers. Firstly they are supposed to provide a telecommunication service which has the capability to be intercepted and store communication-related information.[166] Also, they should provide law enforcement officers with the necessary information that they seek.[167] In terms of s 7(5) a telecommunication service provider who has routed duplicate signals of indirect communications to the designated interception centre must, as soon as practicable thereafter, submit an affidavit to a judge setting forth the steps taken by that telecommunication service provider in giving effect to the request concerned and the results obtained from such steps.[168] In as much as the Act provide for some form of financial relief this is inadequate. Firstly because it is not really clearly what the implications of the Act are and also, many service providers will suffer financial loss because of this Act.

---

iii) the gathering of information concerning a potential threat to the public health or safety or national security of the Republic is necessary;

iv) the making of a request for the provision, or the provision to the competent authorities of a country or territory outside the Republic, of any assistance in connection with, or in the form of, the interception of communications relating to organised crime or any offence relating to terrorism or the gathering of information relating to organised crime or terrorism, is in –

(aa) accordance with an international mutual assistance agreement; or

(bb) the interests of the Republic's international relations or obligations; or

v) the gathering of information concerning property which is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities is necessary;

b) there are reasonable grounds to believe that –

i) the interception of particular communications concerning the relevant ground referred to in paragraph (a) will be obtained by means of such an interception direction; and

ii) subject to subsection (8), the facilities from which, or the place at which, the communications are to be intercepted are being used, or are about to be used, in connection with the relevant ground referred to in paragraph (a) are commonly used by the person or customer in respect of whom the application for the issuing of an interception direction is made; and

c) in respect of the grounds referred to in paragraph (a)(i), (iii), (iv) or (v), other investigative procedures have been applied and have failed to produce the required evidence or reasonably appear to be unlikely to succeed if applied or are likely to be too dangerous to apply in order to obtain the required evidence and that the offence therefore cannot adequately be investigated, or the information therefore cannot adequately be obtained, in another appropriate manner: Provided that this paragraph does not apply to an application for the issuing of a direction in respect of the ground referred to in paragraph (a)(i) or(v) if the –

i) serious offence has been or is being or will probably be committed for the benefit of, at the direction of, or in association with, a person, group of persons or syndicate involved in organised crime; or

ii) property is or could probably be an instrumentality of a serious offence or is or could probably be the proceeds of unlawful activities.

[166] Section 30 of the Act.

[167] For duties of Service Providers see s 28 of the Act.

[168] This can also be found in s 8(5) of the Act.

Section 21 provides for, and issuing of, decryption directions. Section 29 provides for assistance to the law enforcements by the decryption key holder. The section provides that if a decryption direction or a copy thereof is handed to the decryption key holder to whom the decryption direction is addressed by the authorised person who executes that decryption direction or assists with the execution thereof, the decryption key holder concerned must within the period stated in the decryption direction:

a) disclose the decryption key; or
b) provide the decryption assistance, specified in the decryption direction concerned, to the authorised person concerned.

Section 32 of the Act provides for the establishment of interception centres for the interception of communications in terms of this Act.

It is important to note the provisions of s 40, 41 and 55 of the Act. In as much as these provisions do not relate to e-mail communication, the writer submits that it is relevant to look at these provisions so as to demonstrate the sweeping powers given to law enforcement officials in as far as individuals communications are concerned (cellular phone communication). Sections 40 provides that sellers of cellular phones and SIM cards must obtain and keep certain information such as the buyers name; address; identity number including a certified copy of the identity document. A lost or stolen cellular phone and SIM card must be reported in terms of s 41 within a reasonable time after the owner has become aware of the loss, theft or destruction. How one has to ascertain "reasonable time" is another matter which shows a loophole in the Act. The feasibility of the applicability of this section is a cause for concern. The Act has been badly drafted and creates difficulties in logically following its provisions. It is only in s 55 that the Act states that it is an offence not to report a stolen, lost or destroyed SIM card or cellular phone.

As previously stated, the fact that the Act, as a general rule, requires authorisation in a form of a warrant before communications can be intercepted or monitored, is likely to make the Act survive constitutional scrutiny. From the discussion in Chapter 2 of this

work, the trend seems to be that South African courts are more relaxed when it comes to the question of constitutionality of a statute dealing with privacy where there are safeguards or guidelines in the Act.

3.2. The Electronic Communications and Transactions Act No. 25 of 2002.

The Electronic Communications and Transaction Act is applicable to e-mail communications. Section 1 of the Act defines 'electronic communication' to mean communication by means of data messages. E-mail is defined as electronic mails; a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication.

There is no general obligation on service providers to monitor data transmitted or stored. However, s 78(2) of the Act provides that:

> The Minister may, subject to section 14 of the Constitution, prescribe procedures for service providers to
>
> (a) inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service; and
>
> (b) to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

It is submitted that the Regulation Act seem to have already covered the provision for imposing a duty on service providers.[169]

Section 80 provides for the appointment of cyber-inspectors. They have powers to monitor and inspect any web site or activity on an information system[170] in the public domain and report any unlawful activity to the appropriate authority.[171] Cyber

---

[169] See Chapter 3.1 above.
[170] 'Information system' is defined in s 1 of the Act to mean a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet.
[171] Section 81(1)(a).

inspectors may also inspect, search and seize on the authority of a warrant,[172] any premises or information system that has a bearing on an investigation.[173] Section 82(1)(c) states that a cyber inspector may take extracts from, or make copies of any book, document or record that is on or in the premises or in the information system and that has a bearing on the investigation. However this can be done upon authority of a warrant. This obviously affects e-mail communications. The powers vested on the cyber inspectors mean that at any given time, upon the issuing of a warrant, inspectors can monitor and intercept e-mail communications.

It is worth mentioning that, the standard of obtaining a warrant has been lowered to that which was provided by the Monitoring Act. In terms of this Act a warrant may be obtained upon request from a judge or *magistrate*. In terms of the Monitoring Act a warrant could *only* be issued by a judge.[174] Also, the Monitoring Act authorised monitoring and interceptions only with regard to serious offences and the Act defined what amounted to a serious offence.[175]

The Electronic Communications and Transactions Act provides that internet service providers (ISPs) and telephone companies will have to acquire any equipment the government thinks necessary for interception, at their own cost, and establish links to official monitoring stations. The provisions of the Act make it illegal for anyone to provide a telecommunications service, including Internet service, which cannot be monitored. This will have serious financial implications. However, it is submitted that it will be a useless exercise to have legislation in place which allows for the interception and monitoring of information without proper equipment in place or system to see to that the Act is implemented smoothly.

Encryption is not a safe option for people trying to protect their privacy. "Encrypted information" is defined in s 1 of the Regulation Act as electronic data which, without the decryption key to that data:

(a) cannot, or cannot readily, be accessed; or

(b) cannot, or cannot readily, be put into an intelligible form.

---

[172] The procedure for obtaining a warrant is in s 83 of the Act.
[173] Section 82 of the Act.
[174] See s 3 of the Monitoring Act in this regard.
[175] See s 3 for a reference to "serious offence" and s 1 for a definition.

The Electronic Communications and Transactions Act, similarly to the Regulation Act, make provision for an order to be issued which permits the interception and monitoring of information that is encrypted. It can also require anyone holding the keys required for decryption to assist in decoding information.[176] Obviously, in order for this to pass constitutional muster, the government will have to prove that it is reasonable and justifiable limitation of the right to privacy that the communication be decrypted. Where there is suspicion of terrorism or any threat to the well being of the Republic, the safety of the Republic will weigh more than the right of individuals "to be left alone".

In terms of the Act, a person who intentionally accesses data without permission or authority to do so is guilty of an offence and may face imprisonment of up to 12 months or a fine. This basically covers, for example, hackers and police officials who can be proved to have acted *mala fide*.

3.3. Criminal Procedure Act 51 of 1977.

The Criminal Procedure Act was drafted in 1977 without technological advances of the modern age in mind. Things such as SIM cards, cellular phones and e-mails were non existent. However it is necessary to consider whether the provisions of the Act that relate to invasions of privacy can be used by law enforcement officers in the world of technology, to limit the right to privacy of communications.

Chapter 2 of the Act provides for a general power of search and seizure of certain articles by the state. The articles that can be seized are divided in three broad categories:

1. articles concerned with the commission of an offence;
2. articles that may afford evidence of the commission of an offence; and
3. articles intended to be used in the commission of an offence.[177]

---

[176] For a discussion on this, see also Phillip de Wet, *Lock up your SIM cards*, 5 August 2002. (http://www.itweb.co.za).

[177] Section 20. The section provides that:

As a general rule the search and seizure of such articles must be authorised by a warrant.[178] Section 21 provides for some safeguards in the issuing of a warrant by judicial officers. The section states that:

> 21. Article to be seized under search warrant:
>
> (1) Subject to the provisions of sections 22, 24 and 25, an article referred to in section 20 shall be seized only by virtue of a search warrant issued:
>
> (a) by a magistrate or justice, if it appears to such magistrate or justice from information on oath that there are reasonable grounds for believing that any such article is in the possession or under the control of or upon any person or upon or at any premises within his area of jurisdiction; or
>
> (b) by a judge or judicial officer presiding at criminal proceedings, if it appears to such judge or judicial officer that any such article in the possession or under the control of any person or upon or at any premises is required in evidence of such proceedings.

A search may be undertaken without a warrant in cases where a person whose article is to be searched consents to such a search or where a police official believes that a search warrant will be issued if applied for and that the delay in obtaining such a warrant would defeat the object of the search.[179] "Article" is however not defined in

---

> The State may, in accordance with the provisions of this Chapter, seize anything (in this Chapter referred to as an article)—
>
> (a) which is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence whether within the Republic or elsewhere;
>
> (b) which may afford evidence of the commission or suspected commission of an offence whether within the Republic or elsewhere; or
>
> (c) which is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.

See also Buys (above note 152) 370.

[178] Section 21.

[179] Section 22 of the Criminal Procedure Act. The section provides that:

> Circumstances in which article may be seized without search warrant.—A police official may without a search warrant search any person or container or premises for the purpose of seizing any article referred to in section 20—

the Criminal Procedure Act. This creates uncertainty as to whether this Act applies to electronic communications also taking into account the fact that it was enacted when the internet was not known. The *Oxford Dictionary* defines "article" to include the following meanings: the separate members or portions of anything written and a paragraph, section, or distinct item of any document. Whether it will not strain the Act to include e-mail communication in the meaning of the word "article" is another matter. However, it is submitted that the literal meaning of the word article, as defined in the dictionary should surely encompass e-mail communications as these amount to "portions of anything written", "paragraph; section of a document". However, such a reading in is not necessary. The Regulation Act and the Electronic Communications Act seem to provide adequately for e-mail communication.

3.4. Anti-Terrorism Bill B12-2003.

The Anti-Terrorism Bill was drafted to combat terrorism, in response to the September 11 United States disaster. There has been huge debate on whether South Africa needs such a far reaching Bill in its law. Some argue that the Bill does not respect any rights to privacy.

In terms of s 8 of the Bill a police officer may, for the purposes of an investigation of an offence under the Bill, make an *ex parte* application to a judge for an order for the gathering of information. Unlike the Electronic Communications and Transactions Act this order can only be made by a judge and not a magistrate, which means that the application is only made at the High Court. Whether this is a difference with significance is another matter. However, like the Electronic Communications and Transactions Act, the Bill requires that an offence be committed or about to be committed and it is not a requirement that the offence be regarded as a "serious offence" as was the case with the Monitoring Act. It is important to note that before

---

(a) if the person concerned consents to the search for and the seizure of the article in question, or if the person who may consent to the search of the container or premises consents to such search and the seizure of the article in question; or

(b) if he on reasonable grounds believes—

(i) that a search warrant will be issued to him under paragraph (a) of section 21 (1) if he applies for such warrant; and

(ii) that the delay in obtaining such warrant would defeat the object of the search.

the application is made in terms of this section there need to be authorisation from the National Director of Public Prosecutions.[180]

In this regard, the writer is particularly concerned with the powers given to the police and prosecuting authorities to act *ex parte* (on behalf of one party only) against individuals and organisations simply on the basis of unspecified 'reasonable grounds'.

Section 11 obliges people, when called upon in terms of s 8 to answer questions and also to produce things. This, for the purposes of this work, could mean giving out printouts of e-mail communications which in a number of cases might contain confidential information.

This Bill, if passed as it is, will obviously have an impact on the right to privacy in e-mail communication. It is open to abuse and may affect other rights in the Bill of Rights because of the wide definition of a "terrorist act". "Terrorist act" is defined in terms of the Bill to mean an unlawful act, committed in or outside the Republic. Because of this broad definition, a number of people might find themselves subjected to privacy violations because their conduct would, in terms of the Bill, amount to a "terrorist act". It will be better if the Act finally clears up what really amounts to "a terrorist act". This must be done by having a clear, unambiguous and precise definition of what amounts to a "terrorist act". This will be in accordance with the rule of law which requires that law should be made in clear terms.

3.5. South African Constitution- The Limitation Clause.

Privacy is not an absolute right under the Constitution, nor can it be in practice.[181] In the *Hyundai* case, Langa J (as he then was) held that an intrusion into privacy cannot, as was the case in the past, be permissible unless it can be adequately justified on the basis of section 33(1) of the Interim Constitution.[182] It is a notorious fact that the rate

---

[180] See s 8(2) of the Bill.

[181] *Protea Technology* (above note 66) 1242G-H.

[182] Section 33 of the Interim Constitution is the equivalent of s 36 of the Final Constitution (the Constitution). The section provides that:

> (1) "The rights entrenched in this Chapter may be limited by law of general application, provided that such limitation–
>
> (a) shall be permissible only to the extent that it is–

of crime in South Africa is unacceptably high. There are frequent reports of violent crime and incessant disclosures of fraudulent activity. This has a seriously adverse effect not only on the security of citizens and the morale of the community but also on the country's economy. This ultimately affects the government's ability to address the pressing social welfare problems in South Africa. The need to fight crime is thus an important objective in our society.[183]

Langa DP's *dictum* in this case shows that because of difficulties or challenges that the government faces from time to time, each right need to be looked at in the light of other rights, including the state's obligation to combat crime. The limitation clause provides authority for this approach. What is needed is a balancing process where courts have to look at the right to privacy in the light of other competing rights or interests. That weighing then ascertains whether in light of the circumstances of a case such a right can be limited. For example, say a terrorist group which was planning to blow up a university building where students were writing examinations, is convicted for that attempt on the basis that e-mails communications of the group were intercepted by law enforcement officials after obtaining a warrant from a judge (in terms of the law). The members of the group thereafter challenge the admissibility of the evidence of the intercepted e-mails. Also, they sue the government officials and the Minister of Justice vicariously for invasion of privacy. A court, faced with this case, in looking at whether there has been an infringement of privacy, will, upon deciding that there was an invasion, then look at whether there is a justification for such an invasion. In so doing, the court will not only look at the rights of the members of the terrorist group to have the privacy of their communications protected, but also at the government's objective, which in most instances, will be to protect South African citizens by combating crime.

(i) reasonable; and
(ii) justifiable in an open and democratic society based on freedom and equality; and
(b) shall not negate the essential content of the right in question. . ."

Subsection 2 provided the following:

> "(2) Save as provided for in subsection (1) or any other provision of this Constitution, no law, whether a rule of the common law, customary law or legislation, shall limit any right entrenched in this Chapter."
> . . .

[183] Per Langa DP in the *Hyundai* case (above note 62) 53.

The right to privacy of communications is very important in a democratic state, however, what will become of society if because of this right lawlessness is condoned? The following is therefore an examination of the limitation clause and how the courts have applied it with regard to the right to privacy.

Section 36 of the Constitution contains the limitation clause. The section provides the following:

> 36. Limitation of rights.—
>
> (1) The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including—
>
> (a) the nature of the right;
>
> (b) the importance of the purpose of the limitation;
>
> (c) the nature and extent of the limitation;
>
> (d) the relation between the limitation and its purpose; and
>
> (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.

When there is a constitutional challenge to legislation the test for its constitutional validity is divided in two parts. Kriegler J in *Ex parte Walters*[184] delineates the process as follows:

> "First, there is the threshold enquiry aimed at determining whether or not the enactment in question constitutes a limitation on one or other guaranteed right. This entails examining (a) the content and scope of the relevant protected right(s) and (b) the meaning and

[184] *Ex Parte Minister of Safety and Security and Others: In re S v Walters and Another* 2002 (4) SA 613 (CC); 2002 (7) BCLR 663 (CC).

effect of the impugned enactment to see whether there is any limitation of (a) by (b). Subsections (1) and (2) of section 39 of the Constitution give as to the interpretation of both the rights and the enactment, essentially requiring them to be interpreted so as to promote the value system of an open and democratic society based on human dignity, equality and freedom. If upon such analysis no limitation is found, that is the end of the matter. The constitutional challenge is dismissed there and then.

If there is indeed a limitation, however, the second stage ensues. This is ordinarily called the limitations exercise. In essence this requires a weighing-up of the nature and importance of the right(s) that are limited together with the extent of the limitation as against the importance and purpose of the limiting enactment. Section 36(1) of the Constitution spells out these factors that have to be put into the scales in making a proportional evaluation of all the counterpoised rights and interests involved."[185]

Thus, if the impugned legislation indeed limits a guaranteed right, the next question is whether the limitation is reasonable and justifiable regard being had to the considerations stipulated in section 36. If the impugned legislation does not satisfy the justification standard and a remedial option, through reading in, reading down or severance is not competent, it must be declared unconstitutional and invalid. In that event, the court will not, itself, alter, refashion, or develop the enactment to accord with the Constitution. That responsibility resides, not with the courts, but pre-eminently with the legislative authority.[186]

In a constitutional challenge to a common law rule, the court is again required to do a threshold analysis, being whether the rule limits an entrenched right. The court must

---

[185] Ibid 26-7. Also see *S v Makwanyane and Another* 1995 (6) BCLR 665 (CC); 1995 (3) SA 391(CC).

[186] *Abduraghman Thebus and Another v The State* as yet unreported judgment of the Constitutional Court handed down on 28 August 2003; Section 43 of the Constitution. In *Ferreira v Levin NO* 1996 (1) BCLR 1 (CC); 1996 (1) SA 984 (CC); 183, Chaskalson, P reminds us that:

> "...there are functions that are properly the concern of the Courts and others and others that are the properly the concern of the legislature. At times the functions may overlap. But the terrains are in the main separate, and should be kept separate."

give meaning to the affected rights and the impugned rule in the light of the values that underlie an open and democratic society based on human dignity, equality and freedom. If the limitation is not reasonable and justifiable, the court itself is obliged to adapt, or develop the common law in order to harmonise it with the constitutional norm.

What then amounts to a 'law of general application' as required by s 36 of the Constitution? De Waal et al[187] say that all forms of legislation (delegated or original) would qualify as law, as would the common law and customary law. In *President of the Republic of South Africa v Hugo*[188], Mokgoro J[189] in defining the law of general application said:

> "Rules affecting fundamental rights should be accessible, precise and of general application. People should be able to know the law, and should be able to conform their conduct to the law. Law should apply generally and should not target specific individuals."

From the above, there is no doubt therefore, that the South African statutes legalising monitoring and interception of communication amount to "laws of general application". This is because the Acts are: (a) accessible; (b) precise and (c) of general application and does not target specific people.

In *S v Makwanyane*[190], Chaskalson J[191] once it has been established that there is a law of general application, the process calls for the balancing of different interests. In the balancing process, the relevant considerations will include the nature of the right that is limited, and its importance to an open and democratic society based on freedom and equality; the purpose for which the right is limited and the importance of that purpose to such a society, the extent of the limitation, its efficacy, and particularly where the limitation has to be reasonably necessary, whether the desired ends could be achieved through other means less damaging.

---

[187] De Waal (above note 20) 138
[188] 1997 (6) BCLR 708 (CC); 1997 (4) SA 1 (CC)
[189] At 102.
[190] *Makwanyane* (above note 185).
[191] At 104

The right to privacy is not an absolute right in the Constitution[192] and therefore it can be limited under this section but if limited by a law of general application and such law is justifiable and reasonable. This means that the legislature is permitted to enact such laws as may be necessary in trying to discharge its duty by combating crime. Such enactments may of course infringe the privacy of communications. This, in terms of the law is permissible, only if it can pass the s 36 enquiry. Therefore, proof that the relevant law is reasonable and justifiable will lead to it passing constitutional muster regardless of the invasion of privacy rights.

Sachs J in the *Mistry* case, held that the greater the potential hazards to the public, the less invasive the inspection. People involved in such undertakings must be taken to know from the outset that their activities will be monitored.[193] Looking at s 28(1) of the Medicines and Related Substances Control Act[194] that was at issue in that case the learned judge reasoned as follows:

> Had section 28(1) confined itself to authorising periodic inspections of the business premises of health professionals, such inspections would accordingly have entailed only the most minimal and easily justifiable invasions of privacy, if they had qualified as invasions of privacy at all. Indeed, all legitimate health professionals can only welcome such regulatory inspections. It is clear however that section 28(1) does not limit itself to authorising regulatory inspections of the premises of doctors and chemists. It expressly empowers inspectors to enter not only "premises", but also any "place,

---

[192] See Table of Non-Derogable Rights in the Constitution. See also Madala J in *Case* at para 106.
[193] *Mistry*(note 87 above) 20.
[194] Act 101 of 1965. Section 28 (1) provided the following:
28.Powers of inspectors.—(1) An inspector may at all reasonable times—
(a) enter upon any premises, place, vehicle, vessel or aircraft at or in which there is or is on reasonable grounds suspected to be any medicine or Scheduled substance;
(b) inspect any medicine or Scheduled substance, or any book, record or document found in or upon such premises, place, vehicle, vessel or aircraft;
(c) seize any such medicine or Scheduled substance, or any books, records or documents found in or upon such premises, place, vehicle, vessel or aircraft and appearing to afford evidence of a contravention of any provision of this Act;
(d) take so many samples of any such medicine or Scheduled substance as he may consider necessary for the purpose of testing, examination or analysis in terms of the provisions of this Act.

> vehicle, vessel or aircraft". There can be no doubt that the word "place" is meant to have a wider meaning than "premises", otherwise there would have been no need to put it in. The description is accordingly so broad as to authorise the inspectors to enter private homes, whether they be the dwellings of health professionals or of other persons. Similarly, the vehicles, vessels and aircraft that inspectors may search are not limited to ambulances, hospital ships or the planes of flying doctors, nor could they reasonably be confined to such. Although it has become almost a judicial cliché to say that the object is " . . . [to protect] people, not places", that is, to safeguard personal privacy and not to protect private property, there can be no doubt that certain spaces are normally reserved for the most private of activities. The section is so wide and unrestricted in its reach as to authorise any inspector to enter any person's home simply on the basis that aspirins or cough mixture are or are reasonably suspected of being there. *What is more, the section does not require a warrant to be issued in any circumstances at all.*[195] [Emphasis added].

Later,[196] Sachs J held that inspectors, like any other persons exercising power on behalf of the State, are as entitled as the public to know the precise framework within which they can lawfully and effectively carry out their functions. The statute gives hardly any guidance. All is left to the discretion of the inspectors and their superiors.

This demonstrates that there is a level of tolerance for statutes that have some form limitation and/ or guidelines. As an example, statutes requiring the issuing of a warrant before any monitoring or interception will most certainly, if not definitely, be seen as precise, clear and reasonable.

One thing to be noted in these Acts allowing for the interception and/ or monitoring of communications is that, as much as they purport to protect the privacy of individuals against unreasonable invasions, they do not in any of them have a definition of privacy.

---

[195] At 21.
[196] At 22.

The above Acts and/or Bill do affect and invade the privacy of the communications of citizens. The question to be decided is whether such invasions are in accordance with s36 of the Constitution.

From the above case law, invasions of privacy, be it in a form of interceptions, monitoring or searches and seizures[197] in South Africa are lawful and consistent with the Bill of Rights.[198] However, there need to be proof that the following is present:

1. a warrant issued
2. by a judicial officer
3. upon proof that a serious crime is being committed or is about to be committed
4. upon an examination of such proof, the judicial officer must form a reasonable conclusion that it is necessary to allow such monitoring, interception and/ or search and seizure.

If, however, it is proved that a particular law breaches the right to privacy, be it the common law or the constitutional right to privacy, and upon proving that such a violation is not justifiable in terms of either the common law defences or the limitation clause of the Constitution, such legislation or common law rule will be declared unconstitutional and may be struck down completely or saved through constitutional remedies such as severance or reading-in.

Langa DP in the *Hyundai* case reasoned as follows:

> There is no doubt that search and seizure provisions, in the context of a preparatory investigation, serve an important purpose in the fight against crime. That the State has a pressing interest which involves the security and freedom of the community as a whole is beyond question. It is an objective which is sufficiently important to justify the limitation of the right to privacy of an individual in certain circumstances. The right is not meant to shield

[197] As is the case in Canada. There is no separate right to privacy but all is dealt with under the right against unlawful or unreasonable searches and seizures.
[198] See for example *Tap Wine* (above note 86) where the court held that there was no violation of the right to privacy neither was there a violation of the Monitoring Act.

> criminal activity or to conceal evidence of crime from the criminal justice process. On the other hand, state officials are not entitled without good cause to invade the premises of persons for purposes of searching and seizing property; there would otherwise be little content left to the right to privacy. A balance must therefore be struck between the interests of the individual and that of the State, a task that lies at the heart of the inquiry into the limitation of rights.[199]

Unfortunately the courts have adopted the position that, so long as it will not be detrimental to the interest of justice, if such improperly obtained evidence had to be used, then the courts have a discretion favouring the admission of such evidence.

It is however clear from the above discussion that States cannot just "arbitrary record" private communications. The position adopted in South Africa seem to be that, there is a need for a warrant which provides a form of a screening process as to what and who can be monitored or have their private communications intercepted. In very exceptional circumstances will the courts allow any form of interception or monitoring that is done without a warrant issued by a judicial officer. This will obviously be done in extremely urgent situations. This can be done, for example, where the state or its officials might be afraid that seeking a warrant in order to monitor or intercept an e-mail communication might jeopardise the investigation as there might be a risk that the communication might be deleted from the system. At the end of the day, an invasion of the right to privacy affects other rights guaranteed in the Constitution, for example, freedom of expression. It is for this reason that the writer agrees with Sachs J in *Case* where he said:

> ". . . the infringement of privacy becomes harder to countenance when it targets communicative matter. . ."

[199] At 54.

Chapter 4: The right to privacy and legislative authorisation of the monitoring and interception of e-mail communications in other countries:

The right to privacy is recognised and guaranteed explicitly in several human rights instruments such as the Universal Declaration of Human Rights[200], the International Covenant on Civil and Political Rights,[201] the European Convention for the Protection of Human Rights and Fundamental Freedoms[202] and the American Convention on Human Rights[203].

Article 12 of the Universal Declaration of Human Rights states the following:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks

The Universal Declaration of Human Rights sees the right to privacy as part of the right to dignity. It cannot be a coincidence that arbitrary interferences with privacy are prohibited in the same section (article) as the prohibition against attacks upon honour and reputation. Article 12 provides for its own limitation. Interference with privacy is only unlawful if its amounts to an "arbitrary interference".

Artcle 17 of the International Covenant on Civil and Political Rights states the following:

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

---

[200] G.A. res. 217A (III), U.N. Doc A/810 at 71 (1948). Article 12.
[201] 1966, Article 17.
[202] 213 U.N.T.S. 222, *entered into force Sept. 3, 1953, as amended by Protocols Nos 3, 5, and 8* which entered into force on 21 September 1970, 20 December 1971 and 1 January 1990 respectively: Article 8.
[203] O.A.S.Treaty Series No. 36, 1144 U.N.T.S. 123 (1978) Article 11.

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states that:

> Article 8:
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such 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 freedoms of others.

Article 11 of the American Convention on Human Rights states that:

1. Everyone has the right to have his honor respected and his dignity recognised.
2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the right to the protection of the law against such interference or attacks.

It is unfortunate that the African Charter on Human and Peoples' Rights[204] (the African Charter) is silent on the issue of privacy. It makes one wonder whether this is because of the history of African states at the time that resulted in the right to privacy not being regarded as important as freedom and equality which are expressly protected in the African Charter.[205]

---

[204] OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), South Africa is a signatory to the African Charter.

[205] See articles 5 and 6 with regard to freedom and articles 2 and 3 for equality.

Apart from the African Charter, the protection of privacy has been recognised as important in most international instruments. The jurisprudence seems to be that you can limit the right to privacy only if such a limitation is reasonable in terms of the law.

4.1. The United States Position.

The Fourth Amendment to the United States Constitution[206] states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The United States does not have a specific right to privacy. Privacy is part of the right against unreasonable searches and seizures.[207] The Fourth Amendment has two clauses: the unreasonable searches clause and the warrant clause. The Amendment protects people against *unreasonable* searches and seizures.[208] The Amendment requires that the right to privacy may only be violated upon the issuing of a warrant authorising a search or/and seizure. The warrant may only be issued upon proof of probable cause, supported by oath or affirmation. This must describe exactly the place to be searched and the things to be seized. The Supreme Court of the United States has however, carved out a variety of exceptions to the warrant requirement. As an example, a search conducted in the course of a "hot pursuit" does not require a warrant; also a search incident to a lawful arrest.[209] Hogg submits that the criteria of reasonableness in the United States is bound to be somewhat flexible since it is

---

[206] 1789.
[207] United State's Fourth Amendment. See also *Bernstein* (above note 20) and Devenish (above note 1) 138. However, De Waal *et al* (above note 20) claims that like South Africa, United States have general and specific right to privacy. He says the specific right to privacy is contained in the fourth Amendment and the Fourteenth Amendment has been interpreted to provide for a general right to privacy. See in this regard 267.
[208] A position similar to the one adopted in Canada, see discussion below at 4.2.
[209] P. W Hogg, *Constitutional Law of Canada* Vol 2 (1996) 45-3.

necessary to take into account not only an individual's right to privacy and peaceful enjoyment of property but also the practicalities of law enforcement.[210]

From the list or examples of exceptions given by Hogg, it does not seem as if the exception to the requirement of a warrant will apply in the protection of electronic communications in particular, e-mails. Therefore, it might be safe to assume that for an invasion of communication privacy, it will be a requirement or a *must* to have a warrant for any interception or monitoring.[211]

The United States Supreme Court has defined a "search" to mean a "governmental invasion of a person's privacy". Therefore, unlike South Africa where the rights in the Bill of Rights apply both horizontally and vertically, in the United States an infringement of the right to privacy can only be claimed against the government. If therefore, a third party (other then a government official) had to monitor or intercept an individual's e-mail communication, this will not be covered in terms of the Fourth Amendment. There might be recourse, however, in terms of the common law for a tort.[212]

A "seizure" has been defined to mean a "taking of possession" of a thing belonging to a person thus preventing use.[213] Therefore, interception or receiving of telephone messages by a wiretap is a seizure, while the monitoring of a beeper placed on an object moving in public places is not.

A two part "reasonable expectation of privacy" test has been constructed to determine whether an invasion of privacy has occurred. The party alleging a violation of his or her privacy must establish both that he or she has a subjective expectation of privacy and that the society has recognized that expectation as objectively reasonable.[214] In determining whether the individual has lost his/her legitimate expectation of privacy,

---

[210] Ibid at 45-4.
[211] See for example *Katz v United States* (1967) 384 US 347.
[212] Although the elements for this cause of action may vary between states, a plaintiff must generally show that (1) the conduct was highly offensive to a reasonable person, and (2) the plaintiff had a reasonable expectation of privacy.
[213] John Wesley Hall *Search and Seizure* 3rd Ed. Vol. 1 (2000) 23 (definition modified).
[214] Devenish (above note 1) 144. See also Ackerman in *Bernstein* (above note 20) 75.

the court will consider such factors as whether the item was exposed to the public, abandoned, or obtained by consent.[215]

Warrantless searches are presumed unreasonable and the burden is on the government to prove they are valid.[216] The source of the development of the doctrine of Fourth Amendment "reasonableness" is *Camara v Municipal Court of San Francisco.*[217] *Camara* involved the City of San Francisco's warrantless housing inspection program. Camara was charged with violating the City housing code. Camara argued that the inspection violated the Fourth Amendment, but the city argued that a warrantless entry was reasonable under the Fourth Amendment even when conducted without probable cause. The court held that a warrant would not be constitutionally required when the "burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search".[218] The court concluded that such housing inspections satisfy the "reasonableness" requirement of the Fourth Amendment because of the purpose of the search and the relatively limited nature of the intrusion.[219]

Defining the right of privacy, Brandeis J in a dissenting judgment in *Olmstead v United States*[220] held that:

> "The makers of our Constitution undertook to secure conditions favourable to the pursuit of happiness. They recognised the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the

---

[215] See *Katz* (above note 211) at 361.
[216] John Wesley Hall (above note 213) 17 (2000).
[217] (1967) 387 US 523.
[218] Ibid 533.
[219] Ibid 536-537.
[220] (1928) 277 US 438, 478. This was the first time in which the Supreme Court considered a wiretapping case.

> government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[221]

Earlier on in the judgment the learned judge had said the following:

> "Moreover, 'in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be'. The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions."[222]

Evidence of a conspiracy to violate the National Prohibition Act[223] was obtained by government officials by secretly tapping the lines of a telephone company connected with the chief office and some of the residences of the conspirators, and thus clandestinely overhearing and recording their telephonic conversations concerning the conspiracy and in aid of its execution. The tapping connections were made in the basement of a large office building and on public defendants.

The majority in *Olmstead* was of the view that the wiretapping did not violate the Fourth Amendment because no actual searching, nor seizing, took place as those terms were traditionally defined by the court. Since there was no tangible, physical trespass, the court declined to find constitutional grounds for overturning the conviction.[224] It was held that the reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment.[225] The court held that Congress could pass a law making evidence obtained through the interception of

---

[221] Ibid.
[222] Ibid 474.
[223] Act of 1919. Also know as the Volstead Act.
[224] Ibid 464-465.
[225] Ibid 466.

telephone conversations inadmissible in court, but the courts could not adopt such a stance by "attributing an enlarged and unusual meaning to the 4th Amendment".[226] Under the common law, the admissibility of evidence is not affected by the fact of its having been obtained illegally.[227]

It took nearly forty years for the United States Supreme court to reject the view adopted in the *Olmstead* case.[228] In *Katz v United States*[229] overruled *Olmstead.* In this case police had placed an electronic bug (listening device) on the outside of a public telephone booth and had listened to and recorded the accused's end of a telephone conversation that he made from the telephone booth. The question was whether the recording of the accused's conversation had been obtained in breach of the Fourth Amendment which prohibits unreasonable searches and seizures. The court held that the right to privacy in the Fourth Amendment protects people and not places.[230] The government's eavesdropping activities violated the privacy upon which petitioner justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment.[231] Looking at *Silverman v United States*[232], the court held that the Fourth Amendment governs not only the seizure of tangible items but extends as well to the recording of oral statements. The court held that "[o]ne who occupies it (a telephone booth, shuts the door behind him and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world".[233] That which remains private, even when exposed to public view, is

---

[226] Ibid 465.
[227] Ibid 467.
[228] In a line of telecommunications privacy cases following *Olmstead*, the court had always required a physical trespass or penetration in order for the Fourth Amendment to be implicated. See for example *Goldman v United States* (1942) 316 U.S. 129, 134-5 (holding that use of detectaphone placed against wall to hear conversations next door did not violate Fourth Amendment because there was no trespass); On *Lee v United States* (1952) 343 U.S. 747, 751-54 (holding that use of microphone and transmitter by informer inside home of defendant did not implicate Fourth Amendment because there was no trespass); *Silverman v United States* (1961) 365 U.S. 505, 509-512 (holding that placement of footlong microphone against heating duct violated Fourth Amendment because it intruded into constitutionally protected area). The writer is indebted to Scott A Sundstrom 'You've Got E-mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-mail Monitoring' (1998) 73 *New York University Law Review* 2079, FN 77.
[229] *Katz* (above note 211)
[230] Ibid 351.
[231] Ibid 350-353.
[232] (1961) 365 U.S 505, 511.
[233] *Katz* 352.

protected.[234] Because the Fourth Amendment protects people rather than places, its reach cannot turn on the presence or absence of a physical intrusion into any given enclosure. The 'trespass' doctrine of *Olmstead* is no longer controlling.[235]

Justice Harlan held that the "reasonable expectation of privacy" test has two parts: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognise as "reasonable".[236]

Although the surveillance in this case may have been so narrowly circumscribed that it could constitutionally have been authorised in advance, it was not in fact conducted pursuant to the warrant procedure which is a constitutional precondition of such electronic surveillance.[237]

In *Wigmore on Evidence*[238] the author said:

> "Wiretapping – unconsented-to wiretapping – is in this day and age essential to effective police work . . . A statute which proscribes wiretapping altogether is seriously defective."[239]

Therefore, as is the case with many jurisdictions, the United States recognises and protects the right to privacy (in particular the privacy of communications), however, it is also realised that this right or protection of the right cannot be absolute. Therefore, in circumstances where there need to be effective administration of justice, the right to privacy will be limited. The government's objective in the enforcement of law and combating crime outweighs the individuals' right to privacy.

In *United States v White*[240] the court held that participant surveillance is not a search and seizure within the meaning of the Fourth Amendment. This is because the other

---

[234] Ibid 351-352.
[235] Ibid 351, 353.
[236] Ibid 361.
[237] Ibid 354-359.
[238] § 218b (McNaughton rev 191) (1961) 58.
[239] McCall J in *S v Naidoo* (above note 86) 500.
[240] 401 US 745 (1971), see also *Lopes v United States* 373 US 427 (1963).

party to the surveillance is a consenting and willing party. However, Douglas J dissenting held that electronic surveillance is the greatest leveller of human privacy ever known.[241]

The Omnibus Crime Control and Safe Streets Act[242] make it a crime for a person to intercept any wire or oral communication. It also provides that whenever such communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceedings. Similar to the interception and monitoring statutes in South Africa, this Act provides that a government official may apply to a federal judge for an order authorising interception of wire or oral communications by federal officers. Evidence that is intercepted under a valid court order is admissible.

With the advent of cellular telephones, computer-to-computer transmissions and electronic e-mail systems, technology outpaced the Omnibus Act. The problem with the Omnibus Act is that it only dealt with wire or oral communications and was not applicable to electronic communications such as e-mails. The Electronic Communications Privacy Act[243] (ECPA) was therefore enacted. This Act amends the Omnibus Act. Sidbury[244] submits that the Act has been held to apply to the interception of e-mail. This is also clear from the wording of s 101(3)(b)[245] and 101(6)(c) of the Act.[246] The ECPA includes two main categories of protection: Title 1 prohibits interception of messages in transit, while Title 2 prohibits access to and disclosure of stored information. The statute prohibits the intentional interception of any electronic communication or intentionally using or disclosing the contents of any electronic communication, knowing or having reason to know that the information was obtained in violation of the Act. The Act provides for some general exceptions to

---

[241] Ibid at 756.
[242] Act of 1968, 42 U.S.C (18 USC §§ 2510-2520).
[243] 8 U. S. C. (1986).
[244] Benjamin F. Sidbury 'You've Got Mail. . . And Your Boss Knows It: Rethinking the Scope of the Employer – E-mail Monitoring Exceptions to the Electronic Communications Privacy Act' [2001] 5 UCLA Journal of Law and Technology.
http://www.lawtechjournal.com/articles/2001/05_010912_sidbury.php
[245] Section 101(3)(b) states that s 2510(4) of title 18, United States Code is amended by inserting "electronic" after "wire".
[246] Section 101(6)(c) adds and defines electronic communication to mean:

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical . . .

liability.[247] It provides that internet service providers shall not disclose the content of electronic communications (e-mails) without permission or legal process[248] except where it appears the information pertains to a crime.[249] Warrants and subpoenas are permissible methods of access to stored electronic communications. When notified that process is being sought, the keeper of the electronic communications must preserve the information.[250] John Hall states that most e-mail providers are quite helpful to the government.[251] The Act provides civil remedies for violations.[252] What is important to note, is that, this Act, unlike the Fourth Amendment provides for the protection of privacy against both the government and private individuals.

In the *Steve Jackson Games, Inc*[253] case the Secret Service executed a search warrant at the offices of a games publisher whose computer served both a development system and a public broadcaster. Pursuant to its investigation, the Secret Service seized the computer thereby also seizing the e-mail of some 300 customers. Steve Jackson Games and its customers, none of whom were targets of the Secret Service probe, filed a civil suit claiming that the government's action violated the Electronic Communications Privacy Act (ECPA); Privacy Protection Act[254] and the Wire and Electronic Communications Interception and Interception of Oral Communications Act[255]. The reason for this claim was because the Secret Service has taken none of the preliminary steps required by the above statutes. Evidence established that the Secret Service personnel or its delegates did read all electronic communications seized and did delete certain information and communications.

The Privacy Protection Act states that:

> "Notwithstanding and other law, it shall be unlawful for a government officer or employee, in connection with the investigation . . . of a criminal offence to search for or seize any work product materials possessed by a person

[247] See Burchell (above note 17) 411.
[248] 18 USCS s2511(a)(2), 2517, 2702, 2703.
[249] 18 USCS s 2702(b)(6)(A)(ii).
[250] 18 USCS s 2703(f).
[251] John Wesley Hall 598.
[252] 18 USCS s 2707.
[253] Steve Jackson Games, Inc. v United States Secret Service 816 F- Supp. 432 W.D Texas, [1993].
[254] 42 U.S.C 2000 aa.
[255] 18 U.S.C. 2510.

reasonably believed to have a purpose to disseminate to the public a newspaper, broadcast, or other similar form of public communication . . ."[256]

The court held that since Steven Jackson Games was involved in a business of disseminating to the public publications and broadcast, the Privacy Protection Act had been violated.[257]

The court further held that unread e-mail was a "stored communication" rather than a "transmission" which entitled it to lesser protections under the ECPA.[258]

In *Smith v Maryland*[259] the Supreme Court held that there was no reasonable expectation of privacy in the numbers dialled on a telephone which were recorded by a pen register.[260] In *Smith*, the victim of a robbery complained to the police that she was being harassed on the telephone by a man who claimed to be the one who robbed her. He called her and told her to go outside, where she saw his car. She told the police, they got its license number, and discovered it was registered to Smith. Then, they decided to put a pen register on Smith's telephone to see if he indeed called his victim. It turned out that he actually did. A search warrant was obtained for his house, and incriminating evidence was found. He was identified in a line-up and indicted. The court held that no telephone user has a reasonable expectation of privacy in the numbers he or she dials, because the user has to know that the telephone company has the capability of and often does record the telephone numbers dialled from a telephone.[261] The fact that the telephone company has the capability of recording local telephone numbers but hardly ever did made no constitutional difference.[262]

---

[256] See 42 U.S.C. s 2000 aa(a).
[257] *Steve Jackson Games* (above note 253) 440.
[258] Anna Beeson 'Privacy in Cyberspace: Is Your E-mail Safe From the Boss, the SysOp, the Hackers, and the Cops?' http://www.aclu.org/issues/cyber/priv/privpap.html.
[259] (1979) 442 US 735.
[260] A 'pen register' is defined in the Electronic Communications Privacy Act as a device which records or decodes electronic or other impulses which identify the numbers dialled or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.
[261] *Smith* (above note 259) 742-745.
[262] Ibid 745.

John Hall states that the *Smith* case has been rejected under several state constitutions.[263] Congress enacted The Electronic Communications Privacy Act.[264] This Act requires judicial approval of pen registers, traps, and tracing devices and permits compelling cooperation from third parties to install them.[265]

John Hall states that:

> "The four walls of the home are by no means a limit on the Fourth Amendment. It applies to the cartilage of the home and to businesses as well.
>
> Protection of private papers is also a core value. As with searches of the home, seizure of papers was one of the reasons the Fourth Amendment was adopted. Papers include books.
>
> The Fourth Amendment also protects "effects". The definition of what is a Fourth Amendment "effect" has been the subject of relatively little discussion by the Supreme Court, but the common law gave great respect to "effects". The Court has held that "intangibles" and "information" are "effects". Only recently did the Supreme Court define "effects" as "other personal property" and not real property.[266],[267]

From the above passage, "effects" clearly include electronic communications, therefore e-mails.

It is important to note that the United States also has what is called "Carnivore".[268] This system uses specialised software on a computer that can be attached to an internet service provider network and programmed to scan large volumes of e-mail

---

[263] John Wesley Hall (above note 213) 339.
[264] 18 U. S. C. (1986).
[265] See in this regard 18 USCS section 3121-27.
[266] *Oliver v United States* (1984) 466 US 170, 177.
[267] John Hall (above note 213) 34-35.
[268] See Peter J Young: 'The Case Against Carnivore: Preventing Law Enforcement From Devouring Privacy' 35 (2001) Indiana Law Review 303; see also 'Outrage as FBI unleashes Carnivore on the Net- http://www.iol.co.za/general/newsprint.

messages. It gives law enforcement officers access to all traffic sent through an Internet service provider's network. Despite its presence in the Internet Service Providers (ISP) facilities and attachment to their computers, ISPs are not given access to the system, making the FBI exclusively knowledgeable of Carnivore's capabilities.[269] This clearly has potential for abuse. Also, the US runs "Echelon", a spy system of satellites and listening posts which can intercept millions of telephone, fax and e-mail messages.[270] William Webster, a US judge was quoted as having said privacy must yield in some areas to the rights of others to be protected. He said:

> "Unless law-enforcement is given tools, they will not succeed in getting there before the bomb goes off. This ironic considering that this statement was made before the September 11 disaster."[271]

The Patriot Act came into effect 2001. Title II of the Act is titled "Enhanced Surveillance Procedures". In terms of s 212, the Act allows ISPs to voluntarily hand over all "on-content" information to law enforcement without the need for any court order or subpoena. Sections 210 and 211 expands the records that the government may seek with a simple subpoena (no court review required) to include records of session times and durations, temporarily assigned network, addresses, means and sources of payments, including credit card or bank account numbers. They can also see where people venture in cyberspace. These "clickstreams" can reveal what people are reading, downloading and even purchasing. The Act allows law enforcers to bypass Internet providers to capture e-mail addresses or even to read and wiretap conversations in real time. Any federal judge, regardless of jurisdiction, can now approve such warrants.[272]

Section 201 provides for the interception of authority to intercept wire, oral, and electronic communications relating to terrorism and s 202 for the authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offences.

---

[269] Ibid.
[270] Richard Meares 'Digital Surveillance? You'll get used to it. http://www.iol.co.za/general/newsprint. 2000.
[271] Ibid.
[272] Matthew Fordahl 'Requests for subscriber information concern privacy advocates' 2002 http://www.nando.net/nation/v-text/story.

The Communications Assistance for Law Enforcement Act of 1994[273] (CALEA) was enacted to preserve the government's ability to intercept communications involving advanced technologies while protecting the privacy of communications and without impeding the introduction of new technologies, features and services. The Act requires telecommunication carriers, by 1998, to design systems to isolate and intercept communications requested by the government under court order.[274] Unlike the ECPA, Congress intended this Act to only facilitate government interceptions and clearly define the role of the telecommunication carriers in the process. It does not address any privacy expectations of the telecommunication carriers' subscribers.[275]

CALEA is about access, not authority. CALEA does not expand the law enforcement authority's fundamental statutory authority to conduct electronic surveillance. It simply seeks to ensure that after the law enforcement authority obtains the appropriate legal authority, telecommunications carriers will have the necessary capability, and sufficient capacity, to assist the law enforcement authority regardless of their specific systems or services.

Devenish submits that American citizens have a "legitimate expectation" that their conversations will remain private and that a violation of this expectation requires the demonstration of a probable cause necessary to obtain a search warrant. The right to privacy may be infringed if a compelling state interest necessitates such an infringement. However, he submits that, the restricting statute must be shown to be necessary and not only rationally connected to the attainment of a permissible state policy. Strict scrutiny is therefore applicable in these circumstances. Devenish labels the American experience as complex, paradoxical, confusing and controversial.[276]

The protection of the right to privacy has developed to such a degree that it now embraces not merely the right to seclusion but the right to individual autonomy or free

---

[273] Pub. L. No. 103-414, 108 Stat. 4279. Sometimes referred to as the "Digital Telephony Act"
[274] See s 103.
[275] See for this discussion, Michelle Skatoff-Gee 'Changing Technologies and the Expectation of Privacy: A Modern Dilemma.' 28 (1996) Loyola University of Chicago Law Journal 189, 204.
[276] Devenish (above note 1) 144.

choice- the right to make certain personal decisions relating to marriage, procreation, contraception, family relationships, child-rearing, education and even death.[277]

4.2. The Canadian Position.

Canada, similarly to the United States[278], does not specifically provide for the protection of personal privacy. As is the case with the United States, the issue arise in connection with the protection of persons against unreasonable search and seizure. This is found in section 8 of the Canadian Charter of Rights and Freedoms.[279]

The section provides that:

> *Everyone has the right to be secure against unreasonable search or seizure.*

Individuals are secure against only those searches and seizures that are regarded as unreasonable. Section 8 of the Charter therefore imposes a requirement of reasonableness on the techniques available to the police (or other agents of the state) for the looking of and obtaining of evidence of crime (or other legal wrong).[280] This position is similar to the one adopted in the United States where they protect individuals against *unreasonable* searches and seizures. However, unlike the United States Fourth Amendment, the Canadian Charter does not have explicit requirements of judicial authorisation for each search and seizure, a standard of "probable cause", and particularly in the description of the place to be searched and the things to be seized.

Unlike in South Africa where the Constitution provides for vertical and horizontal application, but similarly to the United States, the Canadian Charter of Rights only applies to governments. Therefore individuals are protected against searches and seizures only by government officials.

---

[277] Jonathan Burchell, *Personality Rights and Freedom of Expression*, (The modern *Actio Injuriarum*). Juta 1998.
[278] See Chapter 4.1 immediately above for a discussion on the position in the United States.
[279] 1982.
[280] Hogg (above note 209) 45-2.

A "search" has been defined to mean an examination, by the agents of the state, of a person's person or property in order to look for evidence. A "seizure" is the actual taking away, by the agents of the state, of things that could be used as evidence.[281] It is clear that the word "search" extends to searches of persons as well as those of property.[282] Therefore from this definition offered by Hogg, it is submitted that things that are capable of being seized include even electronic communication, for example e-mail print out. What should be noted is that the word "seizure" within s 8 refers to the seizure of property for investigatory or evidentiary purposes. Hogg warns that this section is not a general guarantee of property rights, for example it does not include protection against the taking of property for expropriation. The same could be said of the South African Constitution. As had been mentioned, South Africa has a general right to privacy and specific rights which includes a right against infringement of private communications, rights against searches and seizures. It is even clearer from the South African Constitution that this section was not intended to be a protection of property rights, because, firstly it clear states that individuals have a right to privacy, secondly there is a distinct and separate right to property in the Bill of Rights.[283]

In *Hunter et al v Southam Inc*[284] Dickson J held that an assessment of the constitutionality of a search and seizure, or of a statute authorizing a search or seizure, must focus on its "reasonable" or "unreasonable" impact on the subject of the search or the seizure, and not simply on its rationality in furthering some valid government objective.[285] The court endorsing the United States position in *Katz v United States*, held that:

---

[281] Ibid 45-4.
[282] Ibid.
[283] See section 25 of the South African Constitution.
[284] (1984) 11 DLR (4th) 641 (SCC) at 652-3. On April 13, 1982, in the course of an inquiry under the Act, the appellant Lawson A.W. Hunter, Director of Investigation and Research of the Combines Investigation Branch, authorized the other appellants, all combines investigation officers, to exercise his authority under s. 10 of the Act to enter and examine documents and other things at the business premises of the Edmonton Journal, a division of the respondent corporation, Southam Inc. On April 20th the officers commenced the search. They said they wished to search every file of Southam Inc. at 10006-101 St., Edmonton, except files in the news-room but including all files of J. Patrick O'Callaghan, publisher of the Edmonton Journal. They declined to give the name of any person whose complaint had initiated the inquiry, or to say under which section of the Act the inquiry had been begun. They also declined to give more specific information as to the subject-matter of the inquiry than that contained in the authorization to search. The issue, therefore, was the constitutional validity of a statute authorising a search and seizure.
[285] Ibid 650.

> "Construing this provision (prohibition against unreasonable searches and seizures) in *Katz v. United States* . . . Stewart J., delivering the majority opinion of the United States Supreme Court, declared at p. 351 that "the Fourth Amendment protects people, not places". Justice Stewart rejected any necessary connection between that Amendment and the notion of trespass. With respect, I believe this approach is equally appropriate in construing the protections in s. 8 of the Canadian Charter of Rights and Freedoms." [Emphasis added][286]

The court held that the guarantee of security from unreasonable search and seizure only protects a reasonable expectation.[287] This limitation on the right guaranteed by section 8, whether it is expressed negatively as freedom from 'unreasonable' search or seizure, or positively as an entitlement to a 'reasonable' expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public's interest to be left alone by government must give way to government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.[288]

The court, dealing with the provisions of the Combines Investigation Act[289], unanimously held that a search and seizure is reasonable only if it was authorised by statute, and three conditions were to be stipulated by the authorising statute:

1. a requirement of a search warrant or other authorisation, to be obtained in advance of the search;
2. a requirement that the warrant be issued by a person who must be "capable of acting judicially", that is, who must not be involved in the investigation; and

---

[286] Ibid 652.
[287] Ibid.
[288] Ibid 652-653.
[289] R.S.C. 1970, c. C-23, s. 10. The Act authorised the Director of the Combines Investigation Branch, or his representative, "to enter any premises on which the Director believes there may be evidence relevant to an inquiry under the Act", to search for evidence on the premises and to seize evidence found there. The Act qualified this power by requiring the Director, before exercising the power, to obtain an authorisation from a member of the Restrictive Trade Practices Commission.

3. a requirement that the warrant be issued only after it has been established upon oath that "reasonable and probable grounds" exist to believe that an offence has been committed and that evidence is to be found in the place to be searched.[290]

Dickson J realising the impossibility of always requiring a warrant or some form of prior authorisation before a search and seizure held that:

> "I recognise that it may not be reasonable in every instance to insist on prior authorisation in order to validate governmental intrusions upon individual's expectations of privacy. Nevertheless, where it is feasible to obtain prior authorisation, I would hold that such authorisation is a precondition for a valid search and seizure."[291]

The court in this case assumed without discussing that a corporation possessed the same constitutionally protected expectation of privacy as is the case with an individual. This position is clearly in line with that adopted in South Africa. The Bill of Rights protects not only natural persons but also juristic persons. The South African jurisprudence shows however that individuals possess a higher degree of privacy than juristic (or legal) persons. This is based on the fact that South African courts recognise the right to privacy as part of the right to dignity.[292] The courts have therefore said, since a company does not have any claims to dignity, the right to privacy that it possess is lesser than that guaranteed to natural persons.[293]

The view expressed in *Hunter et al* has been endorsed by Wilson J in the case of *Mickinley Transport Ltd et al v The Queen*.[294] Wilson J pointed out that one of the purposes underlying the s 8 right is the 'protection of the individual's reasonable expectation of privacy'.[295] Since an enquiry into privacy constitutes an important

---

[290] *Hunter* 654-658.
[291] At 653.
[292] The right to dignity is protected by section 10 of the South African Constitution.
[293] See for example *Bernstein v Bester* (above note 20); *Financial Mail v Sage Holdings* (above note 22) and also a discussion in Chapter 2.2.
[294] (1990) 68 DLR (4th) 568 578.
[295] Note 117 578A-C.

component in determining the scope of an unreasonable search and seizure, the Courts have had to develop a test to determine the scope and content of the right to privacy.

In *R v Grant*[296] the Supreme Court of Canada dealt with the validity of a provision of the Federal Narcotic Control Act that authorised a warrantless search of "any place other than a dwelling house" in which a peace officer believed on reasonable grounds that illegal drugs were present. The court followed the decision of *Hunter v Southam,*[297]holding that the absence of any requirement of a warrant issued by a judge made the statutory authorisation unconstitutional in its unqualified form. However, the court did not strike down the statutory provision. Instead they "read down" the statute to limit the provision "to situations in which exigent circumstances render obtaining a warrant impracticable".[298] The court held that exigent circumstances would be present "where there exists an imminent danger of loss, removal, destruction or disappearance of the evidence sought in a narcotics investigation if the search or seizure is delayed in order to obtain a warrant.[299]

Another issue in this case was whether a search and seizure conducted in terms of an authorised warrant which however was issued by a judge through a breach of s 8 was an unreasonable search and seizure in terms of the Charter, the court per Sopinka J held that the test for the validity of a warrant obtained with unconstitutional evidence was whether the judge would have been justified in issuing the warrant "had the improperly obtained facts been excised from the information sworn to obtain the warrant".[300]

One of the purposes underlying the section 8 right in the Canadian Charter is the "protection of the individual's reasonable expectation of privacy." The "reasonable expectation of privacy" test comprises two questions. Firstly there must at least be a subjective expectation of privacy and, secondly, the expectation must be recognized as reasonable by society.

---

[296] (1993) 3 S.C.R. 223.
[297] See note 284 above.
[298] Ibid at 233, 241.
[299] Ibid at 241-242.
[300] At 251. For the South African experience on unlawfully obtained warrants see *S v Naidoo* (above note 86).

In *R v Plant*[301] the Calgary police, who suspected the accused of cultivating marijuana in the basement of his home, looked up the records of the City of Calgary's electricity utility. They found that the accused's consumption of electricity was four times higher than that of comparable homeowners. The electricity records were stored in the City's computer to which the police had access through a terminal located at the police station. The City had agreed to give the police access to its computerised records. The accused had not given permission for the viewing of or access to such records. At his trial for a charge of possessing marijuana, the accused argued that the police inspection of the computerised records amounted to an unreasonable search under s 8 of the Charter. What need to be noted is that the police had not entered the accused premises and did not inspect the accused's own personal records.[302]

The issue was whether the conduct of the police violated s 8 of the Charter.

The majority of the court, per Sopinka J, held that the purpose of s 8 is to protect against intrusion of the state on an individual's privacy. The limits of such state action are determined by balancing the right of citizens to have respected a reasonable expectation of privacy as against the state interest in law enforcement.[303] Like the United States in the *Katz* case, the court held that s 8 protects people and not property and because of this, it is not necessary to establish a proprietary interest in the thing seized.[304] In balancing the reasonable expectation of privacy of the individual with the interests of the state in law enforcement, Sopinka J held that the Canadian courts have determined that electronic taping of private communication by state authorities violates the personal sphere protected by s. 8.[305] In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. The computer records investigated in the case at bar while revealing the pattern of electricity consumption in the residence

[301] (1993) 3 S.C.R. 281.
[302] Ibid.
[303] Ibid 16.
[304] Ibid.
[305] Ibid 17.

cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence.[306]

McLachlin J held the opposite. She held that the question in each case is whether the evidence discloses a reasonable expectation that the information will be kept in confidence and restricted to the purposes for which it is given.[307] The records disclosed enough information about the lifestyle of the occupant that the occupant had a reasonable expectation that the records would be used solely for the purposes of supplying and billing electricity.[308]

R v Dersch,[309] like *Hunter v Santam,* dealt with information voluntarily provided by third parties. In this case the police requested from a hospital the results of a blood alcohol test that had been done, for medical purposes, on the victim of a road accident. The report was given to the police who thereafter charged the victim with impaired driving. The accused had not agreed to the release of this report by the doctor to the police. He therefore claimed a breached of s 8 of the Charter.

The Supreme Court of Canada, per Major J held that the accused had a reasonable expectation of privacy with respect to his hospital records, including the blood alcohol test results, which he was justified in assuming that it would be kept confidential by the hospital.[310] Therefore, the obtaining of the information by the police was an unreasonable search within the meaning of s 8.[311] The court also excluded the evidence in terms of s 24(2) of the Charter on the basis that the admission of the evidence against the accused would have had the effect of bringing the administration of justice into disrepute.[312]

The Canadian Criminal Code defines "private communication" to mean any oral communication, or any telecommunication, that is made by an originator who is in

---

[306] Ibid 20.
[307] Ibid 41.
[308] Ibid 41-42.
[309] (1993) 3 S.C.R. 768.
[310] Major J 25.
[311] Ibid 26.
[312] Ibid 29.

Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.[313]

Section 183.1 states:

> Where a private communication is originated by more than one person or is intended by the originator thereof to be received by more than one person, a consent to the interception thereof by any one of those persons is sufficient consent for the purposes of any provision of this Part.

Section 184. (1) provides that every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

Section 184.2 (3) states that an authorization may be given under this section if the judge to whom the application is made is satisfied that

> (*a*) there are reasonable grounds to believe that an offence against this or any other Act of Parliament has been or will be committed;
>
> (*b*) either the originator of the private communication or the person intended by the originator to receive it has consented to the interception; and
>
> (*c*) there are reasonable grounds to believe that information concerning the offence referred to in paragraph (*a*) will be obtained through the interception sought.

[313] R.S.C. 1985, c. C-46 Part VI, Invasion of Privacy, section 183.

From the provisions of the Criminal Code, it seems to me that provision is made for interceptions by a state agent[314] who has however received consent from one of the parties to the communication. However what is clear is that a state agent regardless of the consent must, also apply for a warrant authorising the interception of that private communication.

Section 184.4 makes provision for interceptions in exceptional circumstances. The section provides that:

184.4 A peace officer may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication where

> (*a*) the peace officer believes on reasonable grounds that the urgency of the situation is such that an authorization could not, with reasonable diligence, be obtained under any other provision of this Part;
>
> (*b*) the peace officer believes on reasonable grounds that such an interception is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property; and
>
> (*c*) either the originator of the private communication or the person intended by the originator to receive it is the person who would perform the act that is likely to cause the harm or is the victim, or intended victim, of the harm.

In the South African case of *S v Naidoo* McCall J[315] dealing with the applicability of the Interception and Monitoring Act in cellular phones conversations looked at the Canadian case of *R v Solomon* in the Quebec Municipal Court reported in the Digest.[316] The case concerned the admissibility of evidence of certain cellular telephone conversations that had been intercepted by the police. The Crown submitted that the provisions of Part VI of the Code (Invasion of Privacy) were not applicable because a cellular telephone conversation was not a 'telecommunication' or a 'private communication' within the meaning of s 183 of the Code. The report notes that it was held that:

---

[314] A state agent is defined in s 184.1 (4) as a peace officer and a person acting under the authority of, or in cooperation with, a peace officer.
[315] (Above note 86) 525 E – G.
[316] Canadian Digest (1993) 11 CRR (2d) D-5.

> "The cellular phone conversations were telecommunications, but not private communications within the meaning of s 183 of the Criminal Code. Accordingly, Part VI of the Code was not applicable. A person who used a cellular telephone was broadcasting, and anyone could listen."

The court in this case however accepted that an aggrieved party can challenge the interception in terms of s 8 of the Canadian Charter as an unreasonable search and seizure.[317] The writer has difficulty accepting the view that a cellular phone conversation is not a private conversation. In the 21st century where almost everyone owns a cellular phone, where business deals are made through this medium and clients consult lawyers, it will be very unfortunate if such reasoning had to be followed. Surely cellular phone users have a legitimate expectation of privacy in the communications they make over the cellular phone.

The writer agrees with the following words said by La Forest J in *R v Duarte*[318] stating that:

> "The rationale for regulating the power of the State to record communications that their originator expects will not be intercepted by anyone other than the person intended by the originator to receive it. . . has nothing to do with protecting individuals from the threat that their interlocutors will divulge communications that are meant to be private. No set of laws could immunise us from that risk. Rather, the regulation of electronic surveillance protects us from a risk of a different order, i.e. not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the State, in its unfettered discretion, to record and transmit our words.
>
> The reason for this protection is the realisation that if the State were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any

[317] McCall in *Naidoo* (above note 86) 525 G – H.
[318] (1990) 53 CCC (3d) 1 (SCC) ([1990] 1 SCR 30.

expectation that our communications will remain private. A society which exposed us, at the whim of the State, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J, dissenting in *United States v White*[319] put it:

> "Electronic surveillance is the greatest leveller of human privacy ever known."

If the State may arbitrarily record and transmit our private communications it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime. This is not to deny that it is of vital importance that law enforcement agencies be able to employ electronic surveillance in their investigation of crime. Electronic surveillance plays an indispensable role in the detection of sophisticated criminal enterprises. Its utility in the investigation of drug related crimes, for example, has been proven time and again. But, for the reasons I have touched on, it is unacceptable in a free society that the agencies of the State be free to use this technology at their sole discretion. The threat this would pose to privacy is wholly unacceptable."[320]

Duarte was concerned with the protection accorded by s. 8 of the Canadian Charter of Rights and Freedoms against electronic recording of the conversations of individuals with the police and informers in the absence of judicial authorization.

R v Wiggins[321], like *Duarte*, also dealt with participant surveillance. The appellant was the owner of a vessel alleged to have been used by him to carry out a scheme to import narcotics into Canada. He contacted a person who, unknown to him, was a police informer, and asked him if he would like to invest in the scheme. The informer

---

[319] Above note 240, 756.
[320] *Duarte* 21-23.
[321] (1990) 1 S.C.R. 62.

had further conversations with the appellant while wearing a "body pack" which transmitted the conversations to the police who simultaneously recorded them. In one taped conversation, the appellant told the informer how the narcotics were obtained, transported and hidden upon his reaching British Columbia. The police conducted searches of the appellant's vessel but found no narcotics and no evidence to support the appellant's detailed account of the scheme. Appellant was convicted of conspiring to import a narcotic contrary to s 423(1)(d) of the Criminal Code. The British Columbia Court of Appeal dismissed appellant's appeal.

This appeal was primarily concerned with the protection accorded by s 8 of the Canadian Charter of Rights and Freedoms against electronic recording of the conversations of individuals with the police and informers in the absence of judicial authorisation.

These were the first questions that La Forest dealt with:

1. Does s. 178.11(2)(a) of the Criminal Code, legalizing the interception of private communications with the consent of the originator or intended recipient thereof, without the need for judicial authorization, infringe or deny the rights and freedoms guaranteed by s. 8 of the Canadian Charter of Rights and Freedoms?

2. If s. 178.11(2)(a) of the Criminal Code does infringe or deny the rights and freedoms guaranteed by s. 8 of the Canadian Charter of Rights and Freedoms, is it justified by s. 1 of the Charter and therefore not inconsistent with the Constitution Act, 1982?

3. Does s. 178.16(1)(b) of the Criminal Code, making admissible as evidence an intercepted private communication, where the interception was not lawfully made, with the express consent to the admission thereof of the originator or intended recipient thereof, infringe or deny the rights and freedoms guaranteed by s. 8 of the Canadian Charter of Rights and Freedoms?

4. If s. 178.16(1)(b) of the Criminal Code does infringe or deny the rights and freedoms guaranteed by s. 8 of the Canadian Charter of Rights and Freedoms, is it

justified by s. 1 of the Charter and therefore not inconsistent with the Constitution Act, 1982?

The court, per La Forest J, endorsing the reasons given by the court in *Duarte*, held that the participant electronic surveillance conducted by the police and an informer in this case infringes the right to be secure against unreasonable searches and seizure guaranteed by s. 8 of the Charter and is not saved by s. 1 of the Charter. However, the appellant had not discharged the onus of establishing that the admission of the recordings of the intercepted communications in the present case would bring the administration of justice into disrepute.[322] The court held that this evidence should not, therefore, be excluded.[323]

In answering the questions that had been stated earlier (numbered 1 to 4) the court reasoned thus:

On the first question the court held that:

> Section 178.11(2)(a) of the Code does not infringe or deny the rights and freedoms guaranteed by s. 8 of the Charter, but the interception of private communications by an instrumentality of the state with the consent of the originator or intended recipient thereof, without prior judicial authorization, does infringe the rights and freedoms guaranteed by s. 8.

On the second and fourth questions the court held that it was not necessary to answer these questions.

On the third question, the court held that Section 178.16(1)(b) of the Code does not infringe or deny the rights and freedoms guaranteed by s. 8 of the Charter.[324]

Lamer J held, also endorsing the reasons given in *Duarte*, that Section 178.11(2)(a) of the Code does not infringe or deny the rights and freedoms guaranteed by s. 8 of the Charter, but the interception of private communications by an instrumentality of the

---

[322] *Wiggins* 9.
[323] Ibid.
[324] Ibid 12.

state with the consent of the originator or intended recipient thereof, without prior judicial authorization, does infringe the rights and freedoms guaranteed by s. 8. Section 178.16(1)(b) of the Code does not infringe or deny the rights and freedoms guaranteed by s. 8 of the Charter.

Hogg's reasoning for such a finding is that in any conversation, no matter how confidential its subject matter, each participant runs the risk that his interlocutor will betray the confidence by repeating the conversation to someone else. If a participant is charged with a crime, and the conversation is relevant to the charge, then his interlocutor is free to talk to the police, and to testify in court about the conversation; indeed, the interlocutor can be compelled to testify about the conversation in court. Since the disclosure of a private conversation is admissible in a court of law, then surely the recording of a conversation by a participant ought to be admissible too.[325]

Duarte[326] dealt with participant surveillance.

Hogg[327] submits that the Canadian Criminal Code make provision for the electronic interception of private telephone conversations under a warrant issued by a superior court judge based on reasonable and probable grounds. When the Criminal Code's regime of judicial authorisation is complied with, the tapping, although obviously still a search and seizure, is not only lawful but is not unreasonable under s 8.

This view seems to be in line with that adopted in South Africa. In the *Hyundai*[328] case Langa DP clearly endorsed the view that where there is some form of control, the right to privacy can be justifiably limited. Sachs J in *Mistry*[329] also expressed the same view. In that case the section authorising searches and seizures was struck down on the very basis that the process was not regulated. There was no requirement of a warrant. The process was therefore open to abuse and could not on the s 36[330] analysis be justified.

---

[325] Hogg at 45-12.
[326] Ibid.
[327] At 45-11.
[328] See note 62 above.
[329] See note 87 above.
[330] The limitation clause.

Hogg[331] makes an interesting point about privacy law in Canada. He states that in Canada a tapping or surveillance is a search and seizure within the meaning of s 8. Evidence obtained in violation of the s 8 might not be admissible in a court of law. However participant surveillance is allowed and evidence obtained from such surveillance is admissible in a court of law. His view is as follows:

> "The police informers in *Duarte* and *Wiggins* are free to testify in court about their conversations with the accused, where their memory and credibility will no doubt be challenged by the accused; but the electronic records of the conversations, which would set all doubts at rest, are inadmissible!"

It is this reasoning that leads him to conclude that Canada has an extravagant notion of privacy.[332] From looking at some of the Canadian cases on the issue, the writer is convinced that this view is correct. Take for example *R v Wong*,[333] this case was an appeal concerning the protection afforded by s. 8 of the Canadian Charter of Rights and Freedoms against the surreptitious video recording of hotel rooms by the police in the absence of judicial authorization. In this case the police had concealed a video camera in a hotel room that was used for illegal gaming. The hotel consented to the installation of the camera.

The court held that:

> "When the intrusion takes the form of unauthorized and surreptitious electronic audio surveillance, *R. v. Duarte* makes it clear that to sanction such an intrusion would see our privacy diminished in just such an unacceptable manner. While there are societies in which persons have learned, to their cost, to expect that a microphone may be hidden in every wall, it is the hallmark of a society such as ours that its members hold to the belief that they are free to go about their daily business without running the risk that their words will be recorded at the sole discretion of agents of the state."[334]

---

[331] Hogg (above note 209).
[332] Ibid.
[333] (1990) 3 S.C.R. 36.
[334] *Wong* 13 [Emphasis added].

The court held that the tape of an illegal gambling session was obtained in breach of s 8. The court held that the participants in the illegal gambling had a reasonable expectation of privacy in the hotel room that was infringed by the concealed camera.[335] Criticising the decision of the Court of Appeal which had held that since the appellants were engaged in an illegal activity (illegal gambling) they cannot seek protection of the Charter, the court held that:

> "Moreover, it is clear from the excerpt cited above that the Court of Appeal, in assessing the constitutionality of the search, has allowed itself to be influenced by the fact that the appellant was carrying on illegal activities. By way of expansion on my earlier references to *Duarte,* I would note that that decision places considerable emphasis on the fact that the answer to the question whether persons who were the object of an electronic search had a reasonable expectation of privacy cannot be made to depend on whether or not those persons were engaged in illegal activities . . . If reliance were to be placed on such *ex post facto* reasoning, and the courts to conclude that persons who were the subject of an electronic search could not have had a reasonable expectation of privacy because the search revealed that they were in fact performing a criminal act, the result would inevitably be to adopt a system of subsequent validation for searches. Yet it was precisely to guard against this possibility that this Court in *Hunter v. Southam Inc* . . . at p. 160, stressed that prior authorization, wherever feasible, was a necessary pre-condition for a valid search and seizure."[336]

When a breach of s 8 occurs, any evidence so discovered by the unreasonable search or seizure will have been obtained in breach of the Charter of Rights. However as Hogg points out[337], this does not necessarily render the evidence inadmissible. Section 24(2)[338] of the Charter provides that evidence obtained in breach of the

---

[335] Ibid 24.
[336] *Wong* 19 [Emphasis added].
[337] Hogg 45-2.
[338] Section 24(2) states the following:

> (2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the *proceedings would bring the administration of justice into disrepute.* [emphasis added].

Charter of Rights shall be excluded only if its admission would bring the administration of justice into disrepute. Hogg[339] states that if the police show that they acted in good faith and were unaware that they were acting in violation of the Charter, courts will sometimes admit evidence obtained in breach of s 8. However a deliberate violation of the Charter and any violation of settled law (which the police are assumed to be aware of), will nearly always lead to exclusion. Section 24(4) does not therefore operate to licence searches and seizures that are unreasonable according to settled law.[340]

The learned author further states that no law can override s 8. However a law can introduce safeguards, perhaps in the form of requirement of a warrant to be issued by a court on the basis of reasonable and probable grounds.

In *R v Collins*[341] Lamer J in considering the concept of "disrepute' said that:

> "The concept of disrepute necessarily involves some element of community views, and the determination of disrepute thus requires the Judge to refer to what he conceives to be the views of the community at large."

At 136 the learned judge held further that:

> "The approach I adopt may be put figuratively in terms of the reasonable person test proposed by Professor Yves-Marie Morissette . . . In applying s 24(2), he suggested that the relevant question is: "Would the admission of the evidence bring the administration of justice into disrepute in the eyes of the reasonable man, dispassionate and fully apprised of the circumstances of the case?" The reasonable person is usually the average person in the community, but only when that community's current mood is reasonable.
> The decision is therefore not left to the untrammelled discretion of the judge."

---

[339] See above note 209.
[340] Ibid.
[341] [1987] 28 CRR 122; 1 SCR 265, 135.

A law that provides for an unreasonable search and seizure could still be upheld as a reasonable limit under s 1 of the Charter. This section provides that:

> 1. The *Canadian Charter of Rights and Freedoms* guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

Hogg argues that there is a possibility that while a law might not pass the reasonable test in s 8 of the Charter, it can however be saved or pass the reasonable test provided for in s 1 of the Charter.[342]

It is submitted that the South African system is, to a great extent, similar to that adopted in Canada. The South African Constitution grants a general right to privacy and also has a specific right against searches and seizures. Also, the Constitution provides that the rights in the Bill of Rights are not absolute, they may be limited by law of general application in terms of s 36 of the Constitution.[343] This is almost similar to the provisions of s 1 of the Charter which requires that rights may only be limited in a reasonable way by law.

Another similarity between the South African system and the Canadian is that in the event that a court finds that the evidence was obtained in breach of a right/s in the Charter, this will not necessarily mean that such evidence cannot be admissible in court. Section 24(2) of the Canadian Charter is therefore similar or equivalent to the South African s 35(5). This section (s 35) provides that evidence improperly obtained may still be admissible if such an admission will not bring the administration of justice into disrepute or render the trial unfair.[344]

The common law rule in Canada is that a police officer or government official has no authority to enter private property for the purpose of searching for evidence, and no authority to seize private property for use as evidence, unless authorised by law. The common law authorises searches for, and seizures of, evidence without a warrant as

---

[342] Ibid.
[343] See Chapter 3.5 for a discussion of the limitation clause.
[344] See in this regard the *Protea Technology* case discussed above note 66; *Tape Wine* note 86, *S v Dube* note 86; *S v Naidoo* note 86 above.

an incident of a lawful arrest, and it authorises searches for, and seizures of, stolen goods upon a warrant issued by a justice upon sworn evidence that there was strong cause to believe that the goods were concealed in the place to be searched.

The Canadian experience demonstrates that as much as authorisation is required before a search and seizure, this is however not feasible in every situation. In some situations therefore, a warrantless search could be upheld as reasonable depending on the circumstances of each particular case. Hogg[345] states that where there is a diminished expectation of privacy, the standard of reasonableness of the search and seizure will be lowered. He also points out that where there is no reasonable expectation of privacy, then in that case there will be no search and seizure within s 8 and the question of reasonableness does not arise. This is because s 8 protects individuals against searches and seizures where there is a legitimate expectation of privacy.[346]

A person who engages in a regulated activity has a diminished expectation of privacy with respect to that activity. In the case of a regulated business, the proprietor's expectation of privacy with respect to the commercial premises, equipment and records is attenuated by the obligation to comply with the regulations and to tolerate the administrative inspections that are an inseparable part of an effective regime of regulation.[347]

4.3. The United Kingdom Position.

Article 8(1) of the European Convention on Human Rights[348] provides that "everyone has the right to respect for his private and family life, his home and his correspondence". This right is limited by article 8(2) on the basis that interference may only occur in accordance with the law, and must be necessary in a democratic society, in the interests of national security, safety or the economic well-being of the

---

[345] Hogg 45-25.
[346] See for example the reasoning in of McLachlin J in *R v Plant* (above note 301).
[347] Ibid at 45-27. For the South African position, see Sachs J's decision in the *Mistry* (above note 87) case at chapter 3.4.
[348] 1953.

country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.[349]

In terms of a resolution of the Consultative Assembly of the Council of Europe the right to privacy has been defined as follows:

> The right to privacy consists essentially in the right to live one's own life with a minimum of interference. It concerns private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection from disclosure of information given or received by the individual confidentially.[350]

In the final conclusions of the Nordic Conference on the Right to Respect for Privacy of 1967 the following additional elements of the right to privacy were listed: the prohibition to use a person's name, identity or photograph without his/her consent, the prohibition to spy on a person, respect for correspondence and the prohibition to disclose official information. The Commission connected the right to privacy of Article 8 also with the right to freedom of expression of Article 10 by stating that "the concept of privacy in Article 8 also includes, to a certain extent, the right to establish and maintain relations with other human beings for the fulfilment of one's personality.[351]

---

[349] The section states the following:
Article 8:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such 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 freedoms of others.

[350] See *Bernstein* (above note 20).
[351] Van Dijk and Van Hoof *Theory and Practice of the European Convention on Human Rights*, 2nd Ed (1990) 369.

The United Kingdom's Regulation of Investigatory Powers Act (RIPA)[352] regulates the interception and monitoring of electronic communications (and other forms of communications). The Act provides for, and regulates the use of, a range of investigative powers, by a variety of public authorities. It updates the law on the interception of communications to take account of technological change such as the growth of the Internet. It provides new powers to help combat the threat posed by rising criminal use of strong encryption; and ensures that there is independent judicial oversight of the powers in the Act.[353]

The Act allows police, the intelligence services, customs and the Inland Revenue to demand access without a warrant or court order to any data held by communications providers for a much broader range of purposes. Access to this information by law-enforcement agencies is only on the grounds of national security or for investigating crime related directly or indirectly to national security.[354]

Part I relates to the interception of communications and the acquisition and disclosure of communications data. Part II relates to the use of covert surveillance, agents, informants and undercover officers. Part III covers the investigation of electronic data protected by encryption. Part IV provides for independent judicial oversight of the powers in the Act. Part V covers miscellaneous and supplemental matters such as consequential amendments, repeals and interpretation.

Section one of the RIPA makes it unlawful to intercept a communication in the course of its transmission. The section states that:

> Unlawful interception.
>
> 1. (1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of-
>
> (a) a public postal service; or
>
> (b) a public telecommunication system.

[352] Act of 2000 c 23.
[353] Privacy and Human Rights 2003: UK and Northern Ireland, "*United Kingdom of Great Britain and Northern Ireland*" http://pi.greennet.org.uk/survey/phr2003/countries/unitedkingdom.htm.
[354] Ibid.

(2) It shall be an offence for a person-

(a) intentionally and without lawful authority, and

(b) otherwise than in circumstances in which his conduct is excluded by subsection (6) from criminal liability under this subsection, to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system.

"Telecommunication system" means any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy. Therefore, the prohibition in s 1 includes electronic communications.

Section 3 of the Act provides for interception with a warrant and s 7 provides for the issuing of a warrant. It is submitted that there is a strict test for the issuing of a warrant to intercept in terms of the Act. Section 7 only provides that an interception warrant shall not be issued except under the hand of the Secretary of State, in urgent cases in which the Secretary of State has herself/ himself expressly authorised the issue of the warrant; or in a case in which the warrant is for the purposes of a request for assistance made under an international mutual agreement by the competent authorities of a country or territory outside the United Kingdom. Apart from this, the Act does not seem to have any "screening" process i.e. the Act does not have any requirement, for example, that there need to be probable cause or a reasonable suspicion that certain offences are being committed or about to be committed.[355]

In *National Panasonic (U.K) Ltd v E.C. Commission*[356] the court dismissed an action brought against the Commission by an English company after Commission investigators had presented themselves at the company's premises armed with a search warrant, the company not having previously received either an informal request for access to its premises or notice of the imminence of the warrant and so it

[355] Compare this to the Regulation Act in South Africa with it requirement of a "serious offence" and judicial authorisation after a judge is satisfied on reasonable grounds that certain factors exist.
[356] [1980] 3 E.H.R.R. 50.

had no opportunity either to influence the content of the warrant before the decision was taken or to dispute its validity before submitting to the search.

One of the grounds of which the company's action was based, was the violation of article 8 of the Convention.[357] The court held that Article 8(2) of the European Convention, in so far as it applies to legal persons, whilst stating that public authorities should not interfere with the exercise of the rights referred to in article 8(1), acknowledges that such interference is permissible to the extent to which it '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 freedoms of others.[358]

The court's decision in this case is in accordance with other jurisdictions. Looking at South Africa as an example, the law in South Africa recognises a right to privacy of legal persons. Also, in as much the right to privacy is guaranteed, this is however not absolute. Like article 8(2), the limitation clause[359] limits the rights guaranteed in the Bill of Rights if such a limitation is reasonable and justifiable in an open and democratic society. Therefore, while United Kingdom law acknowledges the right to private communication, such a right is not absolute, with legislation like RIPA, such communications can be, in terms of the law, monitored or intercepted.

In *R v Preston's*[360] facts are as follows: following a surveillance operation mounted by the police, during which a telephone interception warrant had been issued pursuant to section 2(2)(b) of the Interception of Communications Act 1985,[361] the defendants were charged, *inter alia*, with conspiracy to evade the prohibition in force in respect of the importation of cannabis. In addition to evidence of personal contact between the defendants, the prosecution relied on the frequency of calls made on the defendants' telephones. The case was concerned with the question whether there was an obligation on the prosecutor to disclose to the defence material which had been

[357] The right respect for private and family life, home and correspondence; See article 8 of the Convention.
[358] Ibid 19.
[359] Section 36 of the South African Constitution, discussed in Chapter 3.5.
[360] [1994] 2 A.C. 130.
[361] This Act was repealed by the RIPA.

obtained as a result of the interception of a telephone under a warrant issued by the Secretary of State under section 2 of the Interception of Communications Act 1985.

Lord Mustill held that:

> ". . . for many years the interests of national security have required the interception by public authorities of messages passing through public systems of communication. Thus, although the principle that the mail is inviolable has always been accorded great importance the executive has habitually encroached upon it, in the special interest of protecting the revenues drawn from Customs and Excise duties, and more generally of preserving national security and forestalling serious crime. Latterly, rapid improvements in technology have enlarged both the volume and the methods of communication, and have at the same time prompted the development of new means of exercising surveillance over messages passed by these new means. Thus, the harm done by the telephonic transmission of subversive or criminal messages by telephone is countered by new methods of interception: telephone-tapping as it is often called.[362]

This is view is correct. With technological advancement, not only are we advancing the modes of communication but also criminals are finding new ways of committing crime. Take the ABSA hacker for example.[363] While we are finding much easier ways of doing banking (internet banking) on the other hand we are running a risk of being violated by criminals. ABSA clients have lost a lot of money through becoming victims of technology. It therefore becomes inevitable for law enforcement agencies to expand on their methods of combating crime. Thus it cannot be denied that there are instances when it is of necessity to monitor or intercept private communications. Law enforcements need to keep up with the ever growing world of technology.

The learned judge held further that:

---

[362] *Preston* (above note 340) 144-145.

[363] This story appeared in the *Sunday Times* 20 July 2003, Edwin Lombard.: 'Hacker cleans out bank accounts Hundreds of thousands of rands stolen via Internet from Absa clients'.

> "To these general prohibitions section 1(2) (of the Interception of Communications Act – now repealed by RIPA) creates exceptions in the case of (a) an interception made in obedience to a warrant issued by the Secretary of State, and (b) an interception made by someone who has reasonable grounds for believing that the person to or by whom the communication is sent has consented to the interception. Subsection (3) creates further exceptions, not here material."[364]

He went on to hold the following:

> "In the end, however, I consider that the very real apprehensions voiced by counsel for the defendants cannot prevail over the plain intent and wording of the Act. The need for surveillance and the need to keep it secret are undeniable. So also is the need to protect to the feasible maximum the privacy of those whose conversations are overheard without their consent. Hence sections 2 and 6. These policies are in flat contradiction to current opinions on the 'transparency' of the trial process. Something has to give way, and the history, structure and terms of the statute leave me in little doubt that this must be the duty to give complete disclosure of unused materials. The result is a vulnerable compromise, but it may be the best that can be achieved. At all events I conclude that it is the one which the statute does achieve, and I therefore accept the argument for the prosecutor on the principal issue in the appeal."[365]

Morgans v Director of Public Prosecutions[366] dealt with telephone interception. Printouts from logging device placed on defendant's telephone line resulted in the defendant being charged with using public telecommunication system to obtain unauthorised access to computer systems. The issues were whether the printouts were containing "communications" and whether such printouts were admissible in evidence. In allowing the appeal, the court held that the electrical impulse or signal

---

[364] *Preston* (above note 340) 149.
[365] Ibid 168-169.
[366] [2001] 1 AC 315.

transmitted by a telephone call was in itself a communication and any intentional interception of that signal in the course of its transmission through a public telecommunication system was subject to the provisions of the Interception of Communications Act 1985; and that, accordingly, the information relied on in the defendant's trial was the product of a communication within the meaning of section 1(1) of that Act.[367]

The court held further that the 1985 Act had been enacted to protect the integrity of public communications, subject to limited exceptions necessitated by national security and the prevention of serious crime and with the intention that any material thus intercepted would not be passed to the prosecutor or used in court proceedings, save where the interception had been for one of the purposes set out in section 1(3)of the Act. It was further held that section 9(1) of the Act was to be construed as prohibiting the adducing in evidence in any court or tribunal of material obtained as a result of an interception, whether by a warrant or otherwise, by an officer of the Crown, or other person or body specified in section 9(2), of a communication made by means of a public telecommunications system, with the exception of interceptions falling within section 1(3) or where the proceedings were for an offence specified in section 9(4) or were before the tribunal established under section 7of the Act. Finally, that accordingly, the evidence resulting from the interception of the telephone calls on which the defendant's conviction had been based ought not to have been admitted.[368]

Of relevance also to this issue in the United Kingdom, is the Data Protection Act[369]. The Data Protection Act gives effect to the requirements of the EU Data Protection Directive. The three main intentions of the Directive are to:

- harmonise data protection legislation throughout the EU;
- protect individuals' rights and freedoms, especially the right to privacy regarding the processing of personal data; and
- facilitate the free flow of personal data within the EU in the interests of improving the operation of the single market.[370]

---

[367] See *Morgans* 333.
[368] Ibid 318 C-D; 320 F-G; 338 B-C and 339 D-F.
[369] Act of 1998 c 29.
[370] Directive 95/46/EC.

The 1998 Act repeals and replaces the Data Protection Act[371] in its entirety although in many areas it follows a similar scheme and structure. The 1998 Act give data subjects the following rights:

1. to be provided with:
    - information as to whether or not their personal data are being processed;
    - details about the data (i.e. a description of the data, the purpose(s) of processing and the likely or actual recipients of the data); and
    - a copy of all personal data of which he or she is the subject (s 7 and 8);
2. to prevent processing likely to cause damage or distress (s 10);
3. to prevent direct marketing (s 11);
4. to require a data controller not to make a decision based solely on automated means which significantly affects him or her (s 12);
5. to receive compensation from a data controller for its breach of the 1998 Act (provided, in most cases, that the data subject can demonstrate that the breach has caused the data subject financial loss) (s 13); and
6. to have inaccurate personal data blocked, erased, or destroyed (s 14).[372]

It is submitted that the Data Protection Act's main focus is to protect data that has been voluntary given by an individual for a particular purpose, not to be utilised for something else. For example, if one had to bank with Standard Bank and make a loan application which will inevitably require a disclosure of private, and in most cases confidential facts, if that information had to be used by the Bank for something other than to process the loan application, then within the jurisdiction of the EU, the Data Protection Act will come into play. This Act can also be relevant if an individual makes transactions over the internet and the information, like credit card numbers, addresses, are used for something else, without the consent of the owner of that information.

The United Kingdom, therefore, recognises the right to privacy of communication in terms of article 8(1) of the European Convention. This article provides for its very

[371] Act of 1984 c 35.
[372] James Mullock and Piers Leigh-Pollitt *The 1998 Data Protection Act* 2nd Ed. (2000), 8.

own limitation in terms of article 8(2). Therefore, like most jurisdictions, the right to privacy in the United Kingdom is not absolute and can be limited. The Regulation of Investigatory Powers Act (RIPA) forms such a limitation to the right to privacy of communications.

4.4. The European Commission:

The European Commission has ruled on a number of decisions on the right to privacy as guaranteed by the European Convention's article 8.

In *Malone v United Kingdom,*[373] the applicant, an antique dealer, was prosecuted for offences relating to the dishonest handling of stolen goods. During the trial it emerged that the applicant's telephone had been tapped by the police acting on the authority of a warrant issued by the Home Secretary. Following his acquittal on the criminal charges, the applicant brought civil proceedings seeking to establish that the tapping of his telephone had been unlawful. Before the Commission, the applicant alleged violations of Articles 8 and 13[374] of the Convention.

The court held that:

> "The court would reiterate its opinion that the phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention. The phrase thus implies--and this follows from the object and purpose of article 8--that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1. Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident. Undoubtedly, as the [United Kingdom] Government rightly suggested, the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where

[373] (1985) 7 E.H.R.R. 14.
[374] This Article will not be discussed in this work and therefore the applicant's argument on this basis will not be discussed.

> the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence."[375]

The court therefore held that there had been a breach of article 8 because English law did not satisfy the qualitative test necessary to meet the requirement that any interference with the right of privacy must be "in accordance with the law".[376]

The court looked at the process known as "metering". This process involved the use of a device (a meter check printer) which registered the numbers dialled on a particular telephone and the time and duration of each call. The release of metering information to the police without the consent of the subscriber amounted to an interference with Article 8 of the Convention.[377]

In *Chappell v United Kingdom*[378] the applicant's complaint concerned the execution of an Anton Piller order made by the High Court against him for breach of copyright, requiring him to permit the plaintiffs to search his business premises (which were also his home) for and remove specified films and documents. The order was executed simultaneously with a police search warrant. The court unanimously held that there had been no breach of Article 8 of the Convention.

The court held that there had been interference with the exercise of the applicant's right to respect for his 'private life' and his 'home', which had the legitimate aim of protecting 'the rights of others'. These points had not been contested by the parties.[379]

---

[375] *Malone* 67.
[376] Ibid 80 and 87.
[377] Ibid 84.
[378] 12 E. H. R. R. 1.
[379] *Chappell* 51.

There had been a sufficient legal basis for the interference, since 'law' under Article 8(2) included unwritten or common law.[380] It had not been established that the grant and the exercise of the order did not comply with English law. The court's power of review in this respect was limited, it being in the first place for the national courts to interpret and apply that law.[381]

The grant of the order, was undoubtedly necessary, having regard to the nature and scope of the applicant's business.[382] Moreover, the order itself incorporated significant limitations on its scope, the plaintiffs had given a series of undertakings and a series of remedies for improper exercise were available to the applicant. The court did not find any problem in the fact that the implementation of the order was left to the plaintiffs solicitors.[383]

In *Amann v Swirtzerland*[384], the European Court of Human Rights stated that "tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.

In this case, the police had intercepted a telephone call between the applicant and a woman from the former Soviet embassy. The applicant was a business man who imported depilatory appliances into Switzerland. The woman wanted to order a "Perma Tweez" depilatory appliance. This telephone call was intercepted in terms of the Federal Criminal Procedure Act[385] which empowered the police service to intercept and monitor communications in order to prevent acts liable to endanger the Confederation's internal or external security. The reason for the monitoring was that as he had contacts with an employee of the Soviet embassy and it was not immediately clear that the "Perma Tweez" appliance which he had sold was a

[380] Ibid 52.
[381] Ibid 54.
[382] Ibid 59.
[383] Ibid 60-61.
[384] (2000) 30 E.H.R.R. 843.
[385] Act of 1934 (RS 312.0).

harmless depilatory instrument, the authorities had to investigate his identity, his circumstances and the "Perma Tweez" appliance in question and the record the result.

There were two issues to be decided by the European Commission:

(a) whether there has been a violation of Article 8 of the Convention;

(b) whether there has been a violation of Article 13 of the Convention.[386]

The Commission concluded, by nine votes to eight, that there had been a violation of Article 8.[387] The Commission held that that the monitoring of the applicant's telephone conversation and the storage of the information obtained therefrom violated his right to respect for his private life, and that he had no domestic remedy at his disposal to complain thereof.[388] It was held that the existence of an interference cannot depend upon the applicant having suffered any identifiable damage, as such a requirement would render the Convention guarantees in Article 8 of the Convention theoretical and illusory, whereas they are intended to be practical and effective.[389] After deciding that there was a violation of the right to privacy in terms of the Convention, the Commission held that it then had to establish whether this violation was justifiable in terms of article 8(2) of the Convention.[390] It was held that the expression "in accordance with the law" in paragraph 2 of Article 8 of the Convention requires that the interferences must have some basis in domestic law. Moreover, the law in question must be accessible to the individual concerned and its consequences for him must also be foreseeable. In the context of secret measures of surveillance or interception of communications by public authorities, the expression "in accordance with the law" not only necessitates compliance with the law, but also relates to the quality of that law, requiring it to be compatible with the rule of law. Thus, the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances and conditions on which public authorities are empowered to resort to any such secret measures.[391] At paragraph 69, it was held that "the storing by a public authority of data relating to the private life of an individual

---

[386] This section deals with administrative action and is therefore not relevant for the purposes of this work.
[387] *Amann* 40.
[388] Ibid 44.
[389] Ibid 55.
[390] Ibid 56.
[391] Ibid 57-58.

amounts to an interference within the meaning of article 8. The subsequent use of the stored information has no bearing on that finding . . ."

Chapter 5: Recommendations for legislative change.

The government's ability to intercept and monitor communications plays a central role in fighting crime. Government agents use interception and monitoring devices to infiltrate drug trafficking organisations and organised crime circles, and to fight white collar crimes and terrorism. The intrusive nature of government's interceptions and monitoring, however, necessitates restrictions on governmental 'eavesdropping' to preserve individual privacy interests. Therefore, as stated by Sachs J in *Mistry* (above note 58), there must be guidelines regulating the nature of the power, the circumstance under which and when it should be exercised. A requirement of a warrant is one such guideline. The South African statutes seem to accord with this notion. Of course, like most statutes there is provision for exceptions to the "warrant" or "prior authorisation" requirement. This however cannot be said to be unreasonable and or unjustifiable. The very nature of law enforcement sometimes requires that rules requiring a warrant in order to monitor or intercept private e-mail communication, be dispensed with. However, this discretion should be exercised sparingly and under very urgent, sensitive or serious cases with due regard to the rights of individuals embodied in the Bill of Rights.

Cavavos and Morin once said that with cryptographic technology, individuals seeking absolute privacy no longer need to depend on the legal system for their protection. Rather, the technology itself provides all the protection needed.[392] This is however not possible in terms of South African law. The Regulation Act and the Electronic Communication and Transactions Act make it clear that no one may possess or sell cryptography without proper authorisation.[393]

The Regulations Act and other acts discussed in chapter 3 above provide that anyone using cryptography may be called to provide the keys to decrypt any information.[394] In fact, the Acts prohibits service providers from dealing or selling services that are not capable of being monitored or intercepted. Therefore it will not be true to say that

---

[392] Quote from Cavavos and Morin *Cyber-space and the Law*, in Burchell (above note 30) 411.
[393] See Chapter 5 of the Regulation Act.
[394] See chapter 3 above.

we can find protection against unlawful invasions to privacy by the government by making use of cryptography.

The writer has difficulty with South African law on participant surveillance. Allowing such a method of infringement of privacy not only is it regarded by the writer as immoral (contra bones mores) but, it is submitted, is not in accordance with the values that underlie the Constitution. It promotes a lack of trust (while the Constitution promotes free association), it restricts the exercise of free speech not to mention the invasion of privacy.

The writer agrees with the view that statutory protections can be reduced or negated through private agreement. However, in the South African context, I disagree with the submission that private agreements can also be used to increase user privacy.[395] This could have been possible 3 years ago but not with the existence of the Regulation Act and the Electronic Communication and Transaction Act. These Acts make it mandatory for service providers to assist law enforcement agencies in their duties to combat crime by providing systems that can be monitored and allow for interception, by requiring encrypted messages to be decrypted, by making it an offence not to abide by the provisions of the Acts. Service providers stand the chance of losing everything if they do not abide by the book. On the other hand consumers of their (the service providers') services cannot in today's world survive without the technology that is being offered.

[395] Ann Beeson 'Privacy in Cyberspace: Is Your E-mail Safe From the Boss, the SysOp, the Hackers, and the Cops?' http://www.aclu.org/issues/cyber/priv/privpop.html.

Chapter 6: Conclusion.

The right to privacy is protected by both the common law and the Constitution. A litigant bringing a delictual action in terms of the common law need to prove that there has been an unlawful and intentional infringement of the right. Common law defences will however, suffice in negating liability for a common law delictual action. On this basis therefore, in a delictual action for an invasion of privacy, if the government can show that one of the defences available in a common law action for privacy, is present, the plaintiff will not be successful.

The Constitution guarantees everyone a right to privacy.[396] However, from the preceding chapters, it is clear that this right is not absolute and therefore can be limited in terms of s 36 of the Constitution. It can be limited if the limitation is reasonable and justifiable in an open and democratic society. It is for South African courts to decide whether legislation allowing for invasions of privacy is consistent with the requirements of s 36.

The right may also be suspended in consequence of the declaration of a state of emergency, but only to the extent that the derogation is strictly required by the emergency and the legislation enacting the state of emergency is consistent with South Africa's obligations under international law applicable to states of emergency.

It is important to note that the fact that a violation of a right to privacy is proved will not automatically render any evidence obtained in a manner that violates the Constitution inadmissible. The Constitution states that, evidence will only be inadmissible if it is proved that admitting such evidence will result into an unfair trial or bring the administration of justice into disrepute.[397]

International jurisprudence is in line with South Africa. In the United States, the Fourth Amendment prohibits unreasonable infringement of privacy.[398] What is therefore required, is that any monitoring or interception of electronic

[396] Section 14 of the Constitution.
[397] Section 35(5) of the Constitution.
[398] The United States and Canada do not have an express right to privacy. The right is part of the protection against unreasonable searches and seizures.

communications should be done in a reasonable manner. This can be achieved by applying for a warrant authorising the invasion unless it is in a situation where it would have defeated the ends of justice to allow for the application for a warrant. Therefore the United States does not have an absolute right against privacy violations.

In Canada there is also a protection against unreasonable searches and seizure. The Canadian experience demonstrates that as much as authorisation is required before a search and seizure, this is however not feasible in every situation. Therefore, like South Africa, there are instances where an interception or monitoring can take place without a warrant. These cases will have to be very exceptional.

Like most jurisdictions, the right to privacy in the United Kingdom is not absolute and can be limited. The Regulation of Investigatory Powers Act (RIPA) forms such a limitation to the right to privacy of communications. The European Commission has also recognised and upheld protection of privacy in terms of the European Convention. As with South Africa, it is clear that the Commission follow a two stage process. That is, whether there has been a violation of the right to privacy in terms of the European Convention and if the answer is positive, whether such a violation can be justified in terms of s 8(2) of the Convention.

Given the examples of unreasonable invasion of privacy under pre-1994 laws in South Africa country, privacy is an important right in the Constitution. From the above discussion on the right to privacy and the jurisprudence in other jurisdictions, it is clear that privacy law in the sphere of electronic communications is still being developed.

In as much as the writer is in favour of the protection of privacy, it is clear that a degree of invasion to the privacy of individual's communications cannot be avoided. There are instances where it will legitimate for government officials to invade the sphere of privacy of the South African citizens. However, this process should not be left unregulated. Provision for a requirement of a warrant must always be found in laws that authorise invasions into the private sphere of individuals. The realities of law enforcement make it impossible to always obtain a warrant before an invasion. There will always be cases where it is impossible to obtain a warrant or if it is to be

obtained, will render the administration of justice into disrepute. These cases should, however, be very limited and extremely exceptional.

It is the above stated reasons that the writer agrees with Langa J[399] (as he then was) in *Case* where he said that:

> The emphasis with which Didcott J[400] expresses himself with regard to the individual's right to privacy has to be seen against the backdrop of our history and the fact that constitutional protection of this right is new in this country. It is a right which, in common with others, was violated often with impunity by the legislature and the executive. Such emphasis is therefore necessary particularly in this period when South African society is still grappling with the process of purging itself of those laws and practices from our past which do not fit in with the values which underpin the Constitution – if only to remind both authority and citizen that the rules of the game have changed.

The writer agrees with the view expressed by Devenish[401] that in the light of South Africa's history of human rights abuses, the protection of human dignity must of necessity enjoy priority, and therefore privacy which is so intimately related to human dignity must be boldly and unequivocally protected by means of a liberal and benevolent interpretation of section 14.

---

[399] *Case* (above note 79) 100.
[400] Didcott J in *Case* 91.
[401] Devenish (above note 1) 152.

References:

1. Statutes:

1. The International Covenant on Civil and Political Rights (1966).
2. The African Charter on Human and Peoples' Rights OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982).
3. The Universal Declaration of Human Rights 1948.

South Africa

1. Anti-Terrorism Bill B12-2003.
2. The Constitution of the Republic of South Africa 200 of 1993.
3. The Constitution of the Republic of South Africa Act 108 of 1996.
4. Electronic Communication and Transactions Act 25 of 2002.
5. Interception and Monitoring Prohibition Act 27 of 1992.
6. Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

United States

1. The American Convention on Human Rights 1978.
2. Communications Assistance for Law Enforcement Act Pub. L. No. 103-414, 108 Stat. 4279 (1994).
3. Electronic Communications Privacy Act 18 U. S. C. (1986).
4. The Fourth Amendment to the United States Constitution 1789.
5. Omnibus Crime Control and Safe Streets Act of 1968 42 U.S.C (18 USC §§ 2510-2520.
6. The Patriot Act of 2001 H.R 2975.

United Kingdom

1. Data Protection Act of 1998 c 29.
2. The European Convention on Fundamental Rights and Freedoms 1953.
3. Interception of Communications Act of 1985 c 56.
4. Regulation of Investigatory Powers Act (RIPA) 2000 c23.

Canada

1. The Canadian Charter of Rights and Freedoms 1982.
2. Canadian Criminal Code R.S. 1985, c. C-46 Part VI.

2. Cases:

South Africa:

1. *Abduraghman Thebus and Another v The State* As yet unreported judgment of the Constitution handed on the 28th of August 2003.
2. *Amod v Multilateral Motor Vehicle Accident Fund* 1998 (10) BCLR 1207 (CC); 1998 (4) SA 753 (CC).
3. *Bernstein and Others v Bester and Others NNO* 1996 (4) BCLR 449 (CC); 1996 (2) SA 751 (CC).
4. *Carmichele v Minister of Safety and Security and Another* 2001 (10) BCLR 995 (CC); 2001 (4) SA 938 (CC).
5. *Case and Another v Minister of Safety and Security and Others; Curtis v Minister of Safety and Security and Others* 1996 (5) BCLR 609 (CC); 1996 (3) SA 617 (CC).
6. *De Fourd v Town Council of Cape Town* 1898 S.C 399.
7. *Du Plessis v De Klerk* 1996 (3) SA 850 (CC); 1996 (5) BCLR 658 (CC).
8. *Ex Parte Minister of Safety and Security and Others: In re S v Walters and Another* 2002 (4) SA 613 (CC); 2002 (7) BCLR 663 (CC).
9. *Ferreira v Levin NO* 1996 (1) BCLR 1 (CC); 1996 (1) SA 984 (CC).
10. *Fedics Group (Pty) Ltd and Another v Matus and Others* 1997 (9) BCLR 1199 (C); 1998 (2) SA 617 (C).
11. *Financial Mail (Pty) Ltd and Others v Sage Holdings Ltd and Another* 1993 (2) SA 451 (A).
12. *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors (Pty) Ltd and Others: In re: Hyundai Motor Distributors (Pty) Ltd and Others v Smit NO and Others* 2000 (10) BCLR 1079 (CC); 2001 (1) SA 545.
13. *Jansen Van Vuuren and Another NNO v Kruger* 1993 (4) SA 842 (A).
14. *Key v Attorney-General, Cape of Good Hope Provincial Division and Another* 1996 (6) BCLR 788 (CC); 1996 (4) SA 187 (CC).
15. *Kidson v S.A Associated Newspapers* 1957 (3) SA 461 (W).
16. *Lenco Holdings Ltd and Others v Eckstein and Others* 1996 (2) SA 693 (N).

17. *Mistry v Interim National Medical and Dental Council of SA* 1998 (7) BCLR 880 (CC); 1998 (4) SA 1127 (CC).
18. *National Coalition for Gay and Lesbian Equality v Min of Justice* 1998 (12) BCLR 1517 (CC); 1999 (1) SA 6) (CC).
19. *National Media Ltd and Another v Jooste* 1996 (3) SA 262 (A).
20. *Pharmaceuticals Manufacturers of SA: In ex parte Application of the President RSA* 2000 (2) SA 674 (CC); 2000 (3) BCLR 241 (CC).
21. *President of the Republic of South Africa v Hugo* 1997 (6) BCLR 708 (CC); 1997 (4) SA 1 (CC.
22. *Protea Technology Ltd and Another v Wainer and Others* 1997 (9) BCLR 1225 (W).
23. *R v Umfaan* 1908 T.S 62.
24. *S v A and Another* 1971 (2) SA 293 (T) 297.
25. *S v Bierman* 2002 (5) SA 243 (CC); 2002 (10) BCLR 1078 (CC).
26. *S v Dube* 2000 (6) BCLR 685 (N); 2000 (2) SA 583 (N); 2000 (1) SACR 53 (N).
27. *S v Kidson* 1999 (1) SACR 338 (W).
28. *S v Madiba and Another* 1998 (1) BCLR 38 (D).
29. *S v Makwanyane and Another* 1995 (6) BCLR 665 (CC); 1995 (3) SA 391(CC).
30. *S v Naidoo and Another* 1998 (1) SACR 479 (N).
31. *S v Nkabinde* 1998 (8) BCLR (N).
32. *Smit v Van Niekerk NO en n' Ander* 1976 (4) SA 293 (AD).
33. *Tap Wine Trading CC v Cape Classic Wines (Western Cape) CC* 1999 (4) 194 (C).

United States:

1. *Bowers, Attorney General of Geargia v Hardwick et al* 478 US 186 (1985).
2. *Camara v Municipal Court of San Francisco.* (1967) 387 US 523.
3. *Katz v United States* (1967) 389 U. S 347.
4. *Lopes v United States* (1963) 373 US 427.
5. *Olmstead v United States* (1928) 277 US 438; 72 L Ed 944; 48 S CT 564.
6. *Smith v Maryland* (1979) 442 U.S 735.
7. *Steve Jackson Games Incorporated v United States Secret Services, United States of America* 1993 U. S Dist. Lexis 3378.
8. *United States v Maxwell* 42 M.J 568 1995.

9. *United States v White* 401 US 745 (1971).

Canada:

1. *Hunter v Southam Incorporated* 1984 (2) S. C. R 145
2. *Mickinley Transport Ltd et al v The Queen* 1990 (68) D.L.R. 568.
3. *R v Collins* 1987 (28) C.R.R. 122; 1987 (1) S.C.R 265.
4. *R v Dersch* 1993 (3) S. C. R 768.
5. *R v Duarte* 1990 (1) S. C. R 30.
6. *R v Grant* 1993 (3) S.C.R. 223.
7. *R v Plant* 1993 (3) S.C.R. 281.
8. *R v Solomon* Digest 1993 (11) C. R. R. (2d).
9. *R v Wiggins* 1990 (1) S.C.R. 62.
10. *R v Wong* 1990 (3) S.C.R. 36.

United Kingdom:

1. *Morgans v DPP* [2001] 1 AC 315.
2. *National Panasonic (U.K) Ltd v E.C Commission* [1980] 3 E.H.R.R. 50.
3. *R v P* [2001] 2 58 HL.
4. *R v Preston* [1994] 2 A.C. 130.

European Human Rights Commission:

1. *Amann v Swirtzerland* (2000) 30 E.H.R.R. 843.
2. *Chappell v United Kingdom* 1989 (12) EHRR 1.
3. *Malone v United Kingdom* 1984 (7) EHRR 14.
4. *National Panasonic v Commission* 1980 (3) CMLR 169.

3. Articles:

South Africa

1. David McQuoid-Mason, "*Invasion of Privacy: common law v constitutional delict – does it make a difference?" Acta Juridicta* (2001), 227.
2. E. Lombard, 'Hacker cleans out bank accounts: Hundreds of thousands of rands stolen via Internet from Absa clients, 20 July 2003 *Sunday Times.*
3. C Mischke, 'The monitoring and interception of electronic communications' *Contemporary Labour Law* (2001) No.10, 91-8.

4. S Temkin 'Electronic Communication and Transactions Bill will allow government and business to move to paperless society-Experts say bill offers exciting opportunities.' *Business Day* 5 March 2002 2.
5. Phillip de Wet, 'Lock up your SIM cards.' 5 August 2002. http://www.itweb.co.za.

USA

1. Anna Beeson 'Privacy in Cyberspace: Is Your E-mail Safe from the Boss, the SysOp, the Hackers, and the Cops?' http://www.aclu.org/issues/cyber/priv/privpap.html.
2. Matthew Fordahl 'Requests for subscriber information concern privacy advocates' 2002 http://www.nando.net/nation/v-text/story.
3. Richard Meares 'Digital Surveillance? You'll get used to it. http://www.iol.co.za/general/newsprint. 2000.
4. Benjamin F. Sidbury 'You've Got Mail. . . And Your Boss Knows It: Rethinking the Scope of the Employer – E-mail Monitoring Exceptions to the Electronic Communications Privacy Act' (2001) *UCLA Journal of Law and Technology* 5. http://www.lawtechjournal.com/articles/2001/05_010912_sidbury.php.
5. , Michelle Skatoff-Gee 'Changing Technologies and the Expectation of Privacy: A modern Dilemma.' (1996) 28 *Loyola University of Chicago Law Journal* 189.
6. Scott A Sundstrom 'You've Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-mail Monitoring' 73 (1998) *New York University Law Review* 2064.
7. Warren and Brandeis 'The Right to Privacy' 4 (1890) *Havard Law Review* 193.
8. *Wigmore on Evidence* § 218b (McNaughton rev 191) (1961).
9. Peter J Young 'The Case Against Carnivore: Preventing Law Enforcement From Devouring Privacy' (2001) 35 *Indiana Law Review* 303.
10. Privacy and Human Rights 2003: UK and Northern Ireland, "*United Kingdom of Great Britain and Northern Ireland*". http://pi.greennet.org.uk/survey/phr2003/countries/unitedkingdom.htm.

UK

1. Y Akdeniz, N Taylor and C Walker, 'BigBrother.gov.uk: State Surveillance in the age of information and rights' (2001) Criminal Law Review (February) 73.
2. S Millar, 'Blankett security laws may be illegal' The Guardian July 31 2002.

4. Books:

South Africa

1. R Buys, *CyberLaw @ SA: The Internet and The Law in South Africa* (2000).
2. M. Chaskalson, Kentridge, J. Klaaren, G. Marcus, D. Spitz and S. Woolman (eds): *Constitutional Law of South Africa* 5th ed (1999) Kenwyn: Juta.
3. J. De Waal, I. Currie and G. Erasmus (eds): *The Bill of Rights Handbook* 4th ed (2001) Cape Town: Juta.
4. G. E. Devenish *A Commentary on the South African Bill of Rights* (1999) Durban: Butterworths.
5. D. J. McQuoid-Mason, *The Law of Privacy in South Africa* (1978) Kenywn: Juta.
6. J. Neethling, J. M. Potgieter and P. J. Visser (eds): *Law of Delict* 4th ed (2001) Durban: Butterworth.
7. J Neethling, J Potgieter and P Visser *Deliktereg* 5th Ed (2002).
8. J Neethling, J Potgieter, P Visser, *Neethling's Law of Personality* (1996) Butterworths.

USA

1. J. W. Hall, *Search and Seizure* 3rd Ed. Vol. 1 and 2 (2000).

UK

1. J Mullock and P Leigh-Pollitt, *The Point of Law: The 1998 Data Protection Act,* 2nd Ed (1999).
2. Van Dijk and Hoof, *Theory and Practice of the European Convention on Human Rights,* 2nd Ed (1990).

Canada

1. P. W. Hogg: *Constitutional Law of Canada* vol II 3 Ed (1992).