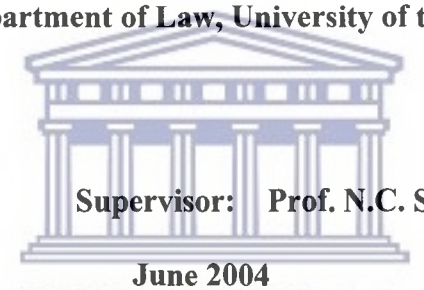
UNIVERSITY OF THE WESTERN CAPE

The Right to Privacy and the Challenge of Modern Cell Phone Technology.

Abraham John Hamman

A minithesis submitted in partial fulfillment of the requirements for the degree of Magister Legum in the Department of Law, University of the Western Cape.



Supervisor: Prof. N.C. Steytler

June 2004

ABSTRACT

The Right to Privacy and the Challenge of Modern Cell Phone Technology.

Abraham John Hamman

Magister Legum –Minithesis, Department of Law, University of the Western Cape.

Privacy has been defined as a state in which one is not observed or disturbed by others and to have freedom from public attention. A person's right to privacy entails that such a person should have control over his or her personal information and should be able to conduct his or her personal affairs relatively free from unwanted intrusions. The right to privacy has been included in the Constitution of the Republic of South Africa, Act 108 of 1996. The inclusion of the right to privacy in the Bill of Rights as a Fundamental right illustrates how important this right is regarded.

By utilizing the latest cell phone technology, non-communicative personal information such as the number that is dialed, the time the call is made, the movement and location of both the caller and the recipient of a call can be obtained.

This type of information is recorded and stored by cell phone companies without the knowledge and consent of users. Technology makes it possible that others can access this information.

This information is not ordinarily available to police and they usually require prior judicial authorization to access this information. The problem is that the cell phone companies, their employees and criminals who want to know the location and movement of other citizens in order to commit crime, can access this information.

On the other hand this type of information, if utilized by the police services can play a crucial part in the solving of crime and the use thereof should be encouraged to solve crimes, provided that the proper legal authorization is obtained. In the case of *S v Petersen* unreported case Cape High Court Case No; SS 95/98, the using of advanced cell phone technology assisted the court to bring out a guilty verdict.

The questions that this research endeavored to address are the following:

(1) Is this type of information protected by the Constitution?

(2) If so, should this intrusion of the right to privacy be regulated?

A number of international instruments such as; the Universal Declaration on Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the UN Convention on Migrant Workers, and the UN Convention on the Protection of the Child contains privacy provisions. This instruments all state that no interference with the right to privacy should be allowed unless provision in domestic laws authorise such interference. Certain decisions of the European Court of Human Rights also confirm this principle and delivered a number of judgments, which dealt with individuals' right to privacy.

In American cases such as *Smith v Maryland* 442 U.S. 735(1979) and *United States v Miller* 425 U.S. 435 (1976) information in possession of third parties do not receive protection if the information is voluntarily conveyed and forms part of commercial records.

Canada on the other hand regards the nature of the information to be important to determine if it is personal and if the information reveals intimate details of a person. If it does the person will have reasonable expectation of privacy in the said information.

However it is submitted that that the nature and extent of non-communicative information and details obtained from the cell phone records such as location and movement of users

is worthy of being protected by the right to privacy. It does disclose details about the personal lifestyle and choices of individuals. Because a reasonable expectation of privacy exists in this type of information, access thereto should be properly regulated. The records should not be trawled in order to form a suspicion. A suspicion should have been present before an application is made to obtain any form of prior judicial authorization.

Date: **June 2004**

DECLARATION

I declare that *The right to privacy: The challenge of modern cell phone technology* is my own work, that it has not been submitted before for any degree or examination in any other university, and that all sources I have used or quoted have been indicated and acknowledged as complete references.

Abraham John Hamman June 2004

Signed_____

CONTENTS

CHAPTER 1 INTRODUCTION

With the introduction of the Constitution, Act 108 of 1996 (hereinafter referred to as "the Constitution") everyone's right to privacy is now constitutionally protected.[1] The right to privacy is now protected in terms of both the common law and the Constitution. The fact that the right to privacy is now a fundamental human right illustrates the importance thereof.

Privacy has been defined as a state in which one is not observed or disturbed by others and to have freedom from public attention.[2] Neethling proposed the following definition of privacy:

> "Privaatheid is 'n individuele lewenstoestand van afsondering van openbaarheid. Hierdie lewenstoestand omsluit al daardie persoonlike feite wat die belanghebbende self bestem om van kennismaking deur buitestaanders uitgesluit te wees en ten opsigte waarvan hy 'n privaat houdingswil het."[3]

This definition of privacy was accepted by the Appellate Division in 1996:

> "Privacy is an individual condition of life of separation from publicity. This condition of life embraces all those personal facts which the person concerned has determined to be excluded from the knowledge of outsiders and in respect of which he has a will that they be kept private."[4]

The Constitutional Court in subsequent matters accepted this definition of privacy.[5]

---

[1] Section 14.
[2] "Privacy" *The Concise Oxford Dictionary*. Ed. Judy Pearsall. Oxford University Press 2001. Oxford Reference Online. Oxford University Press. University of the Western Cape. www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t23.e44535 accessed 19March 2004.
[3] Neethling, *Die Reg op Privaatheid*, Doctoral Thesis Unisa, (1976) 287.
[4] *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 271.
[5] *Bernstein v Bester* 1996 (2) SA 751 (CC) 789.

This right has also been defined as an individual condition of life characterized by seclusion from the public and publicity, which implies an absence of acquaintance with the individual or his personal affairs in this state.[6]

A person's right to privacy includes that such a person should have control over his or her personal information and should be able to conduct his or her personal affairs relatively free from unwanted intrusions.[7] It gives a person the right to control what others know about an individual. It includes the right to walk naked in homes, to enjoy alcohol in the privacy of a home, to read whatever books or magazines one chooses to and to decide what others should know or should not know about you. This right also includes the right to make certain personal choices regarding sexual relations. This right has usually been interpreted to include telecommunications and the contents thereof. The state will only be able to access the content of telecommunications with prior judicial authorization.[8]

It would be assumed that the same rule would apply regarding the content of communications via cell phones. However with the use of modern cell phone technology, other types of personal information are being made available, namely the movement and location of users of cell phones. This information is recorded and stored by cell phone companies and can be accessed and used in future.

Although cell phones are used everyday, it is never realized what details are left in the wake of one call. Personal information such as the number that is dialed, the time the call is made, the location of both the caller and the recipient are obtainable by looking at cell phone records. The different cell phone companies record this information about cell phone calls on computer and they keep a record thereof.

In addition to the abovementioned personal information that is kept by cellphone companies, it is the intention of the legislature to attach an identity to every cell phone

---

[6] Neethling J, Potgieter JM, Visser PJ *Law of Delict* 4th ed, Butterworths (2001) 355.
[7] Neethling J, *Persoonlikheidsreg,* Butterworths 39 and *National Media Ltd v Jooste* 1996 (3) SA 262 at 271 –2.
[8] Section 40 Regulation of Interception of Communications and Provision of Communication Related

user. [9] If this is accomplished a database will be established of all cell phone users and there will be a record of the owners of cell phones and a presumption created that it is the owner who probably used the cell phone.

The problem is that certain information about the movement and location of cell phone users are being kept and stored by third parties, namely cell phone companies. There is always the possibility that this stored information can be accessed and conveyed to others at a later stage, with or without the user's consent. Thus an individual has no control about certain personal information in possession of a third party. In many instances individuals are not even aware that this type of information is being recorded and is in possession of cell phone companies.

It is possible that the information in possession of third parties can be accessed without the consent and knowledge of the users. This information is not ordinarily available to the police and they do not have unlimited and unrestricted access to this information. Prior judicial authorization is required to access this type of information. Authorisation in the form of a subpoena [10] issued by a court is a requirement before the cell phone companies will divulge this information. This would seem to be a justifiable infringement in terms of the Constitution.[11] The cell phone companies itself, their employees, computer hackers and possibly even criminals can have access to this information.

The key issue with regard to cell phones is the use of this non-communicative information such as movement and location. Is the keeping and thereby possibly the divulging of this non- communicative information by cell phone companies an intrusion on an individual's right to privacy? The questions that need to be addressed are the following:

(1) Is this type of information protected by the Constitution?

Information Act. No 70 of 2002 (Hereinafter referred to as the "RICPCRI Act").

[9] Section 40 of Act 70 of 2002 RICPCRI Act, requires that before a cellular phone or sim card is sold to anyone the seller must obtain the full names, identity number, residential and postal address and a certified copy of the person's identity document must be retained by the seller.

[10] Subpoena usually issued in terms of Section 205 Criminal Procedure Act 51 of 1977.

[11] Section 36.

(2) If so, should this intrusion of the right to privacy be regulated?

This situation is, at this stage, not regulated by legislation. The Law Reform Commission of South Africa has released an issue paper (hereinafter referred to as "the LRC issue paper') requesting comments and representations on how privacy and data protection should be regulated by and incorporated in legislation.[12]

In a criminal matter heard in the Cape High Court,[13] the cell phone records of certain individuals were accessed to positively link the accused persons to a crime. Their movements and location were tracked and a route map was compiled by using the information obtained from cell phone records. This type of information can be of great assistance to the crime fighting authorities to not only prevent crime, but also to solve crime. Especially if it is difficult to find certain types of evidence or to disprove an accussed's alibi that he was not at a specific time at a specific place.

In this thesis the aim will be to argue the following:

1. That the nature and extent of non-communicative information and details pertaining to movement and location of users obtained from cell phone records is worthy of being protected by the right to privacy as stipulated in the Constitution.
2. That the access to this type of information should be properly regulated.

To achieve the aforementioned aims, modern cell phone technology will be examined to determine how information about the movement and location of its users is obtained from cell phone records. Privacy issues will be investigated from a South African and international perspective. A study of comparative jurisdictions will also be undertaken to ascertain if any authority exist to ascertain if certain details/information such as the location and movement of cell phone users should warrant protection under the right to privacy.

---

[12]South African Law Reform Commission Issue Paper 24 Project 124 Privacy and Data Protection (LRC Issue Paper).
[13]S v Petersen Unreported case Cape High Court Case no: SS 95/98.

In Chapter Two an analysis will be done of how certain information is obtained from cell phones and cell phone records. The case of *State v Petersen*[14] will be discussed to illustrate how information obtained from cell phone records from certain users assisted the court to deliver a guilty verdict. This case was flagged as the first in South Africa that made use of advanced cell phone technology.

Chapter Three deals with the right to privacy from a South African perspective. Section 14, the privacy provision, in the South African Constitution and a number of Constitutional Court decisions dealing with the right to privacy will be examined.

In Chapter Four a study of international law will be done to ascertain how privacy has been defined internationally and what the extent of the realm of privacy is. International guidelines and conventions will be examined to ascertain what the principles of data protection and collection internationally entails. Certain decisions of the European Court of Human Rights will also be referred to.

Chapter Five contains a comparative study of American and Canadian jurisprudence and an examination will be made under what circumstances information will be protected. It will include an investigation to ascertain whether any authority exist that this type of non-communicative information about the location and movement of cell phone users should warrant protection under the right to privacy.

Chapter Six contains the conclusion whether the nature of the information obtained from cell phone records is such, that protection under the right to privacy is warranted and if so recommendations are made how access to the information should be regulated.

[14] Unreported Case Cape High Court Case No: 95/98.

CHAPTER 2 CELL PHONE TECHNOLOGY AND THE USE OF INFORMATION IT GENERATES

In this chapter an analysis will be done of how certain information is obtained from the cell phone records by using modern cell phone technology. The issue of how cell phone technology which was utilised in the prosecution of a criminal matter in *S v Petersen*[15], will also be discussed. It will be investigated how a cell phone operates, how communication via cell phones takes place and how personal information is collected from cell phones.

2.1. Cell phone technology

Although the attributes of the cell phone can be utilized in the same manner as that of an ordinary landline telephone, it is quite different. A cell phone network consists of the following components:

1. The main component is the cellular phone itself, the handset, commonly referred to as the cell phone;
2. The Sim Card (Subscriber Identification Module) card;
3. Base station/Tower with antennas;
4. A cell;
5. Telecommunications Network; and
6. Computer Network.

2.1.1. The Handset

The handset is the instrument itself, which is used daily by millions of people around the world to communicate with each other. The numbers are dialed from the front side of the handset. A handset can also provide the police with certain clues. Each handset has its specific number and it is possible to ascertain if a handset was used at a certain time. In

[15]Unreported case Cape High Court Case no: SS 95/98.

the case of *S v Mboniswa*[16] information was retrieved from the handset of the accused, which indicated that several calls were made from the specific handset. The sim card of the deceased was slipped into the handset of the accused. The accused was linked to the murder because of evidence, which indicated that the cell phone from which the calls were made belonged to the accused.

2.1.2. The Sim Card

The sim **"Subscriber Identification Module"** card[17] is a small removable disk that slips in and out of cell phones. When a cell phone is purchased, it is a requirement that a starter pack must also be purchased. This starter pack contains the sim card with a specific number, which is allocated to the user, to be inserted into the handset. This number reflects the user's unique cell phone number. It is possible to link the identity of a user to a specific sim card. A user can have more than one handset, but only need to use one specific sim card. In other words, the user can have 10 cell phones, but only have one cell phone number, provided that the sim card can only be used in one specific handset at a time. A cell phone can be switched on without the sim card, but then it can only dial emergency numbers. Subscribers to Vodacom[18] can for example dial the emergency number 112 without a sim card in the handset. It is however not possible to make any other calls without a sim card being inserted in a handset.

2.1.3. Tower/Base Stations

There are a number of towers or base stations[19] situated in a specific area/city. The base station/ tower usually comprise of 3 components (cells) and have three antennas placed in a certain direction. The antennas are usually placed 120 degrees from each other to cover an area of 360 degrees. Each tower has three cells with each cell having its own unique number. The tower itself has a 4-digit code and the specific cell a 5-digit code; this is to identify the geographical area that is covered by each cell. It is possible to statistically ascertain from which tower and antenna a call was made and which tower and antenna

[16] *S v Mboniswa* [2003] JOL 11011 (C).
[17] www.electronics.howstuffworks.com/cell-phone7.htm.
[18] Cell phone company South Africa.
[19] www.electronics.howstuffworks.com/cell-phone1.htm.

received the call. In this manner the precise location of both the caller and the recipient of the call can be determined. These details are stored on computer by the cell phone companies and can be accessed at a later stage.

2.1.4. A Cell

A cell[20] is the geographical area that each cell (antenna) covers in a base station. Each cell in the base station consists of a tower and a compartment containing the radio equipment. The base station is the center of the cell. Cell sizes can vary from as little as 500 (Five Hundred) metres in inner cities and 30 (thirty) kilometers in rural areas depending on terrain and population. A handset can even display in which geographical area (cell) a person is at a specific moment, provided that the cell info display feature is activated on a handset. When a call is made, by dialing a number on a hand set, a signal is transmitted to the tower from the handset from where the call is made and it communicates with the tower at the recipient's location.

2.1.5. Telecommunications Network

This network consists of the different base stations and is linked together via a telecommunications network. All the details of all cell phone users such as the time of the call and the duration of the calls are stored at the central computer network of the various cell phone companies.

2.1.6. Communication via cell phones

Communication takes place via radio signals; - a cell phone is actually a radio – a very sophisticated radio telephone.[21] Before the age of cell phones, people who needed mobile- communications ability, installed radio telephone systems. There was one central tower antenna per city and approximately 25 channels available for users. A powerful transmitter was also required to transmit for about 70 kilometers.[22] Cell phone communication is made possible because of the huge amount of towers in cities. The genius of the cellular system is the division of cities into small cells, which means that a

[20] See note 19.
[21] www.electronicshowstuffworks.com/cell-phone1.htm.
[22] See note 21.

number of people can all use their different cell phones simultaneously. Communications via cell phones take place when the cell phones (handsets) communicates with the radio transmitters known as base stations/ radio towers, which spread a network of signals over the whole country. There are a number of base stations located throughout cities all over the country.

2.1.7. Information obtained from cell phone records

When a cell phone company furnishes an account to its users, it only contains information that is required for billing purposes. Details such as the time the call was made, the duration of the call, the number that has been dialed and the costs of the call are furnished to the users. Subscribers to cell phone companies only receive this information. Users making use of prepaid cell phones do not receive accounts from cell phone companies. If requested, the cell phone company can furnish the following additional information. The details indicating from which cell the call was made (location of caller), to which cell the call was made (the location of the recipient), the specific handset that was used, and if the sequence of the calls are mapped out, the route that the user took on a specific day can also be ascertained.

Millions of people around the world use cellular phones on a daily basis and with this type of information, the location of almost any cell phone user on the planet can be determined by looking at the cell phone records.

2.1.8. A Handover

It is possible to continue with a conversation via a cell phone even if the user is moving around. Although a cell is only one area covered by one antenna in a base station, cells can indeed overlap from one base station to another and are laid out to overlap at the edges. This ensures that a call is not interrupted, as the user move around whilst driving or moving whilst talking over the cell phone. As the user approach the edge of a cell, the network calculates where the best signals are and transfer the call accordingly to the next best selected cell; this is called "a handover".[23]

[23] www.nashuamobile.co.za/nm_portal.asp?=101_howwork&siteid=nmportal.

A handover ensures that a conversation can be continued with, without the call being interrupted. When a user is moving, the strongest cell is selected via which the call is to be made and to be continued. The importance of this technology is that if user is busy with a call and drives through a certain area, it will automatically select the strongest signal as the user moves and passes different towers. Technology at this stage has not advanced to such an extent that a record is kept of all the towers that were passed during the movement of the user. It only records the details of the cell from where the call initially was made.

2.1.9. The tracking of the movement and location of users

Presently the movements of users cannot be traced if a person is continuously busy on the phone with one specific call. It only records from where the call was made. Only if a user makes another call, the movements will be tracked. The cell phone records will only reflect the movement when the user actually made use of the phone. Even if the cell phone is switched on and no calls are made this will not reflect on the cell phone records. But who knows with the technological developments it could in future be possible to track the movements of a user even if the cell phone is not in use.

The movements of a user can be traced if the cell phone was used a number of times and the user traveled on a specific day. This is done by looking at a print out of the cell phone records of users. This occurs if a number of calls were made during a certain period. Cell phone records reflect the following information

1. The telephone, the handset (cell phone numbers) that has been used;
2. The time of the call/s;
3. The length (duration) of the call/s;
4. The location of the caller (sending point of the call /the cell the call was made from);
5. The location of the recipient (reception point of the call /the cell where the

call was made to)

It is possible to compile a map to indicate the route that a user took by linking the cell phone calls to the different base stations that were passed. It can be precisely pinpointed where the user and the recipients was when the call was made. Both the location of the caller and the recipients can be determined in this manner. The compiling of a route map is usually done with the assistance of a GIS specialist[24]. A GIS specialist is a geographical information systems specialist who obtained a degree in science, specifically geography. With the information obtained from the cell phone records the specialist will be able to compile a map of a city to indicate the movements of an individual.

This specialist will be able to plot and place Vodacom, MTN and Cell C[25] towers/base stations on a map anywhere in the country. With the assistance of computer software programs, spacial data such as cell phone towers, houses and areas such as farms and soil types can be plotted on maps. Points can be plotted on maps and can be described in detail, for example a tower, a dam, a house or anything else.

This type of software would enable a GIS specialist, if approached by the police, to plot and place the towers of cell phone companies on a map anywhere in the country. Any sector or area of a town or city can be taken and be enlarged on a computer so that one can actually see the streets and even the street names.

The map will indicate the direction or movement of a cell phone user if that person made a number of calls from a specific handset. The correct location of the cell phone tower can be ascertained by zooming into a specific area. Obviously the records must first be obtained from the cell phone companies.

The three sections of the tower and the coverage area of each section (cell) can be plotted

[24] Information for this section obtained from Mr. Peter Smitz GIS specialist employed by the CSIR.
[25] Vodacom, MTN and Cell C the three cell phone companies currently operating in Southern Africa.

with precision. The sector (cell) from which the call was made, the details of the reception area (tower to where the call was made) can in a similar manner be plotted. It will indicate if a call was made from or to a Vodacom reception area, a MTN reception area or a Cell C reception area. If the sequence of the calls can be ascertained, it is possible to plot the route that the user took during the period that the cell phone was used. This is done by numbering the calls in sequence of their occurrence and plotting them on a map.

If required, this information can be used in a court of law and it can be of great assistance to the crime fighting authorities, not only to prevent crime but can also solve crimes. It can place an accused on the scene or in the vicinity of a crime with almost absolute accuracy and it can disprove an accused's alibi if his whereabouts can be pinpointed on a specific day, hour, minute and even a second[26].

2.2. State v Petersen and Another: The cell phone case

In the unreported case of *S v Petersen*[27], heard in the High Court of the Cape of Good Hope Provincial Division, advanced cell phone technology was utilised by the prosecution. The detailed billing records were obtained from the cell phone companies and the information obtained from the cell phone records assisted the court in reaching a verdict. This case was flagged as the first in South Africa that made use of advanced cell phone technology.

2.2.1. The facts

Marilese Holmes and Eddie Keim were murdered in the early hours of Monday 5th January 1998. They drove up to Signal Hill, Cape Town to view the city lights. Unbeknown to the couple, as they drove up Signal Hill, they were being followed. Their bodies were found murdered in the region of Monwabisi beach, near Strandfontein

[26] Cell phone technology used in *Petersen* case.
[27] Cape High Court Case No: SS 95/98
Other information obtained *Sunday Times* 26 September 1999.
available at www.suntimes.co.za/1999/09/26/insight/in01.htm and
www.mnet.co.za/CarteBlanche/Display/Display.asp?Id=1637.

approximately 30 kilometers from Signal Hill.

The Murder and Robbery Unit of the police received information that the bodies of a male and a female had been found in the Khayelitsha area. On the scene, the body of a white male with one single bullet in the back of his head was discovered which indicated that he had been shot execution style. It seemed that his head was forced to the ground to stop him from screaming. His mouth was also full of sand. On the scene a few bottles and a dagga pipe were found and one of the sandals of the deceased was missing.

Around ten to fifteen kilometers from where the white male's body was lying, the body of a white female was discovered. The body was lying five meters from the road with a gunshot wound under the chin and another next to the left eye. Three spent cartridges and one live round were also found on this scene. After a post mortem was performed on the body, it was discovered that the deceased was assaulted and raped twice. In the area between the bodies the police found the burnt out shell of Holmes' metallic green BMW motor vehicle.

No one knew what exactly happened during the long journey of 30 kilometers from Signal Hill down to Khayelitsha. The huge media coverage given to the murders resulted in the police making a breakthrough. A person had telephoned crime stop with information that they know the suspects in the killings. As a result of the information the two bodies of the Knotts were found.

Close to the scene where Keim's body had been dumped, police found the bodies of Mike and Maggie Knott, a Somerset West couple who were hijacked outside their home on the 2nd of January 1998. Their bodies had been lying in the area for four days. They had been severely assaulted and shot several times. All the other victims, apart from Maggie Knott, who had been strangled and shot, had been shot execution style. Spent cartridges found at this scene would later link the same murder weapon to the murders of Holmes and Keim. The police realized as they gathered more evidence that they were looking for a gang of killers.

On the same weekend, a Stellenbosch pastor, Andries Manders, and his 10-year old son, also named Andries, were hijacked, but managed to sweet talk their way out of danger by asking their attackers: "Do you know that you are in the presence of a child of God?" Fortunately for them they escaped with their lives. The hijackers took them to a plantation, tied them to a tree and went off with the Manders' white bakkie. One of the perpetrators allegedly said to the victims:"You can be lucky we never killed you because we usually do".

On the 7th January 1998, the police had enough evidence to arrest four suspects that were linked to the crimes. They received the names of the four from different informers, people who did not know each other. Rashaad Petersen and Marshal Andrews respectively 28 and 24 years old, were arrested for the murders. A shoot out occurred outside Paarl when an attempt was made by the police to arrest the other two suspects, namely Dawood Dastigir and Charles Marcus. The said Dastigir and Marcus were fatally injured during the shootout with the police. DNA samples later positively link Dastigir and Marcus to the rape of Marlese Holmes. Petersen and Andrews' bail hearing was held in Mitchell's Plain Magistrates' Court, but an administrative blunder on the part of the prosecution saw the Magistrate struck the case off the court roll. Because of pressure from various sectors including Deryck Holmes, Marilese's father, the media and the widespread attention and the public's outrage, Petersen and Andrews gave themselves over to the police, as they were scared that they would be murdered.

Rashaad Petersen and Marshall Andrews were charged in the High Court of Cape Town, Cape of Good Hope Provincial Division, with four counts of murder, six counts of assault and three counts of theft:

2.2.2. The prosecution

There were no direct evidenced against the accused and no state witnesses who saw the murders. Only after the bodies were found, informers told the police whom they think it could possibly be. Both the accused pleaded not guilty to all the charges and it was left to the prosecution to build a solid case against them. But apart from a fingerprint found on

the BMW's CD shuttle in the vehicle of Holmes, most of the evidence was circumstantial. There was indeed a feeling that it was almost pointless to prosecute a case like this, as the evidence was extremely thin against the accused.[28]

The police together with the prosecution had an idea that was to make legal history. Holmes' cell phone was missing. They subpoenaed the records from the cell phone companies Vodacom and MTN and obtained the detailed billing records of Holmes's cell phone and the one that Dastigir allegedly used. The details of the location from where all the calls were made were put on a map within certain areas of the Cape Peninsula.[29]
What the suspects did not realize was that every time a call was made on a cell phone, the number which is dialed, the time of the call, the date and the location of both the caller and the recipient of the call was recorded on computer. These computer records proved that a number of calls were made from Holmes' cell phone to one belonging to a relative of Dawood Dastigir, one of the dead suspects.[30] The killers left an electronic trace.

Dastigir was linked to a cell phone with the number 083 7652 778. The evidence of the state witness, Adullah Davids was crucial for the state. She testified that during December 1998, Charles Marcus, who was the boyfriend of her daughter, Rahana Galant came twice to her home in Mitchell's Plain, with a golden Mercedes Benz. During January 1999 he came to her home in Hanover Park with a cream Mercedes.[31]

She also testified that Petersen, Andrews and Dastigir always accompanied Marcus when he came to her. She also testified that in and during January 1999, the four of them came to her home in Mitchell's Plain and Charles wanted her to look at a dark green or dark navy BMW motor vehicle and a cell phone, a Nokia 8110.

The four asked her if she was interested in buying the motor vehicle and the cell phone from them. She said that she switched the cell phone on and testified in court that she

[28] Information obtained from State Advocate Kevin Rossouw who prosecuted case in High Court, Cape Town. Interviewed 21 May 2003.
[29] www.suntimes.co.za/1999/09/26/insight/in01.htm.
[30] Evidence of statewitness D R Oosthuizen Vodacom.

identified all four suspects in a green BMW and she specifically remembered the cell phone.

A section 205[32] subpoena was obtained to compel the cell phone companies to hand over the cell phone records of the two cell phones. The police got the different times that these calls were made to each of the phones. It was then decided to put it all onto a detailed map of Cape Town and its surrounds.

It was left to a geographical information specialist (GIS)[33] to build a visual image out of the data received from the cell phone companies by using maps. Although it was the first in this country the specialist was confident that the movement of the killers could be tracked. By looking at the cell phone records the following could be ascertained because Holmes' cell phone was used:

After the vehicle was hijacked on Signal Hill the gang must have split up into two groups. The one then used Holmes' cell phone to phone the other to arrange rendezvous points. Holmes' cell phone had a Vodacom cell number 082 5699 139 and the other cell number was a MTN number 083 7652 778, a cell phone which belonged to a Rashied Sathar, the brother in law of Dawood Dastigir. The said Sathar[34] testified in court that during the period of 30 December 1998 to 6 January 1999 he borrowed his cell phone, which could only receive calls, to Dawood Dastigir.

The following details of the records from Vodacom[35] were obtained and handed in as an exhibit in court:

MSISDN	IMEI	TRAN	CALL DATE	CALL TIME	DURATION	OTHER PARTY	CELL NAME
27825699139	490137100223180	MOC	5 –JAN- 1998	01:20:23	01:19	083 7652 778	GARDENS
27825699139	490137100223180	MOC	5 –JAN- 1998	01:31:29	00:58	083 7652 778	VALKENBERG
27825699139	490137100223180	MOC	5 –JAN- 1998	01:33:35	01:06	083 7652 778	ATHLONE

[31] Evidence statewitness Adullah Davids.
[32] Section 205 of the Criminal Procedure Act 51 of 1977.
[33] Evidence of P Smitz statewitness GIS expert.
[34] Evidence of Rashied Sathar.
[35] Extract from Exhibit SS of court record - data received from Vodacom.

27825699139	490137100223180	MOC	5 –JAN- 1998	01:50:20	00:40	083 7652 778	KHAYELITSHA
27825699139	490137100223180	MOC	5 –JAN- 1998	01:51:27	01:03	083 7652 778	STRANDFONTN
27825699139	490137100223180	MOC	5 –JAN- 1998	01:52:56	00:18	083 7652 778	STRANDFONTN
27825699139	490137100223180	MOC	5 –JAN- 1998	01:53:30	00:37	083 7652 778	MITCH PLAIN
27825699139	490137100223180	MOC	5 –JAN- 1998	01:58:28	00:22	083 7652 778	STRANDFONTN
27825699139	490137100223180	MOC	5 –JAN- 1998	01:59:06	00:26	083 7652 778	STRANDFONTN
27825699139	490137100223180	MOC	5 –JAN- 1998	02:06:43	00:45	083 7652 778	MITCH PLAIN
27825699139	490137100223180	MOC	5 –JAN- 1998	02:08:02	00:31	083 7652 778	MITCH PLAIN
27825699139	490137100223180	MOC	5 –JAN- 1998	02:12:59	00:52	083 7652 778	MITCH PLAIN

The following details of the records from MTN[36] were obtained and also handed in as an exhibit in court:

CALL DATE	CALL TIME	CALLING NO.	CALLED NO.	DURATION	IMEI	IN/OUT	SITE
980105	012020	0825699139	0837652778	1.19	450058010687750	I	CAPE SWISS HOTEL, GARDENS
980105	013125	0825699139	0837652778	0.58	450058010687750	I	LEDGER HOUSE, ATHLONE
980105	013327	0825699139	0837652778	1.06	450058010687750	I	NICO MALAN, HEIDEVLED
980105	025012	0825699139	0837652778	0.4	450058010687750	I	GARDENPOTCENTER, RYLANDS
980105	015120	0825699139	0837652778	1.03	450058010687750	I	NICO MALAN, HEIDEVELD
980105	015248	0825699139	0837652778	0.18	450058010687750	I	NICO MALAN HEIDEVELD
980105	015323	0825699139	0837652778	0.36	450058010687750	I	HANOVER PAR K TELKOM
980105	015820	0825699139	0837652778	0.22	450058010687750	I	VGK CHURCH , LANDSDOWN
980105	015828	0825699139	0837652778	0.25	450058010687750	I	NEUMAN FARM CAPE TOWN
980105	020635	0825699139	0837652778	0.45	450058010687750	I	PHILIPI COD STRRAGE PHILIPI INDUSTRIAL
980105	020754	0825699139	0837652778	0.3	450058010687750	I	MANDALAY PRIMARY SCHOOL, MANDALAY
980105	021252	0825699139	0837652778	0.51	450058010687750	I	MANDALAY PRIMARY SCHOOL MANDALAY

The detailed billing records contained the following; the telephone; the handsets (cell phone numbers) that has been used; the time of the call/s; the length (duration) of the call/s; the location of the caller (sending point of the call /the cell the call was made from); the location of the recipient (reception point of the call /the cell where the call was made to).

[36] Extract from Exhibit TT of court record- data received from MTN.

The GIS expert[37] and the police spent approximately three full days in front of computer screens to prepare evidence for court. First a street map of Cape Town was installed on computer. Then the towers that transmitted the calls were entered. The calls that had been made in the early hours of Monday 5 January 1998 were then logged onto the computer. From this picture it was accurately and simply indicated to the court where the two vehicles must have been and at what time. A total of twelve calls were made from Holmes's cell phone – 082 5699 139 all to the same MTN number - 083 7652 778.

The records indicted that at 01:50 the area was reached where Keim's body was found later that day. The expert drafted a map of the whole route that the users of the cell phones took, by looking at the cell phone records. It proved that the user of number 082 5699 139 was at Gardens at 1:20 and talking to user of cell phone 083 7652 778 who was at Cape Swiss Gardens. Calls 10 –12 also confirmed that the users of the cell phones were in the vicinity of Mitchells Plain, which confirmed the version of witness Adullah Davids that they were at her home in the early hours of that Monday morning.

During the incident, five calls were made from the area where Holmes' body was found. Between 02:06 and 02:12 three calls were made to the other vehicle. The map showed the gang had moved towards Mitchells Plain. They then drove to the house of Adullah Davids where they allegedly tried to sell her Holmes's BMW and cell phone. During the trial, Adullah, who turned state witness, confirmed this.

.

Derryck Holmes, the father of Holmes, testified that he had put a message on Holmes's cell phone, when switched on it read" Hello Marilese". This is what Adulah Davids told the court that she saw on the face of the cell phone that the four tried to sell her in the early hours of 5 January 1998. Under cross-examination, she said it could have been in the region of 3am in the morning that the four came to her

[37] Evidence of witness P Smitz.

2.2.3. The defence.

Both Petersen and Andrews testified in their own defence. The basis of their defence were that they were somewhere else and even had witnesses to substantiate their alibis. Petersen testified that he went with family to a funeral on the Sunday and that he could not took part in the hijacking of Manders.[38] The court also rejected the evidence of the defence witnesses as false and contradictory.[39] The accused who throughout the trial maintained their innocence would through cell phone tracking have their alibi shattered and placed in the vicinity of the bodies of the victims.

2.2.4. The verdict and sentence

The court[40] made the following finding. That it was common knowledge that Holmes' vehicle was hijacked on Signal Hill in the early hours of Monday 5 January 1998. The state had proven with the extracts of the cell phone records from Vodacom that a Vodacom cell phone with sim card 082 569 9139, Holmes's cell phone, made 12 calls to a MTN cell phone, 083 7652 778, which was in possession of Dawood Dastigir. These calls were made between 01:20 and 2: 12 during a period of 52 minutes.

The court found that the only inference it could make was that the calls that were made from Holmes' cell phone to the cell phone of Sathar, which was in the possession of Dastigir. It was also found that the calls were made according to the route that was mapped out by using the cell phone records.

The court found that the movement of the suspects could be ascertained from Signal Hill to Mitchell's Plain near the house of Adullah Davids. The court made the deduction that the hijackers must have traveled with Holmes and Keim in the BMW from Signal Hill and that there was another vehicle, which probably had Sathar's cell phone in it. The 12 calls were made on route to where the body of Holmes was found and that they went from there to the home of Adullah Davids in Mitchell's Plain.

[38] Judgment page 27.
[39] Judgment page 28.
[40] Judgment delivered by Lategan J.

A ballistic expert[41] also testified that the 9mm hand weapon was the same that was used in the murders of Holmes, Keim and the Knots. It was also found that the CD shuttle, which Petersen testified that he received from someone else, came out of Holmes' BMW motor vehicle. The defense also made the admission that the pubic hair that was found on the leg of Holmes was that of Dastigir and that the semen extracted from a vaginal smear was that of Charles Marcus.[42] The court rejected the evidence of Petersen and Andrews that they had alibis and found, that even the witnesses that they called to substantiate their alibis, contradicted each other and their evidence was very poor.

Adullah Davids' testimony, combined with the irrefutable evidence of the mapped cell phone records destroyed the alibis ventured by the accused. The court found both accused guilty on all thirteen charges.

On the 23rd September 1999, Petersen and Andrews were sentenced to life imprisonment. Declared dangerous criminals, their sentences will only be reviewed when they next appear in court again in September 2029. It was with the assistance of modern cell phone technology that the prosecution was able to obtain a guilty verdict, although there was no direct evidence against the accused.

2.3. Conclusion

Cell phone records can indicate precisely where a user was on a specific day, by using the records of the cell phone companies. The precise geographical area from where the call was made and the location where the recipient was can be ascertained. This can be determined by looking at which tower was used in making the call, the time of the call, the duration and which tower received the call. All this information is obtainable from the printouts of cell phone records from cell phone companies.

An expert if required will be able to plot all the detail on a map to indicate with precision where a user was when a call was made. A user who used a cell phone on a specific day

[41] Evidence of Inspector C Pieterse.
[42] Judgment page 26.

and makes a number of calls whilst moving around can have the movements plotted on a map and it can then be traced by making use of cell phone records.

The latest cell phone technology was utilized in the case of *S v Petersen & Another* to ensure a conviction. Without the cell phone records there were no direct evidence against the accused, as there were no eyewitnesses. The two accused would through cell phone technology be linked to the crime. Their movements were tracked from Signal Hill in Cape Town to where the bodies were found and to the place where they wanted to sell the vehicle and the cell phone. By compiling a route map by using the cell phone records to pinpoint the locations of base stations towers, it was almost accurately done to illustrate to the court the movements of the individual whilst they were moving and using their cell phones during a 52 minute period. The one cell phone belonged to the deceased Marilese Holmes and the other to a Sathar who borrowed it to Dastigir, one of the suspects.

As a result of cell phone technology the court could bring out a guilty verdict. The irrefutable evidence of the mapped cell phone records destroyed the alibis ventured by the two accused.

Although the police obtained authorization to obtain the cell phone records, the question is whether the accused was entitled to the protection of the information regarding their movements. Put differently, could the police have obtained the information from the cell phone companies when there was not enough evidence to obtain a section 205 warrant? For example if the police establish the time of death at a particular place- could they trawl through cell phone records for persons who may have been there at a certain place and at a certain time to establish a suspicion? The constitutional right of privacy will be examined to ascertain if this information should receive constitutional protection.

CHAPTER 3 THE RIGHT TO PRIVACY- A SOUTH AFRICAN PERSPECTIVE

The right to privacy has been included in the Constitution as a fundamental right. This right is now protected under the common law as well as the Constitution. Is there any authority in South African law that the right to privacy protects the type of personal information obtained from cell phone records, which would reveal the movements and location of a user? In this chapter an attempt will be made to answer this question by examining the common law and how the Constitutional Court dealt with other incidents where it had to deal with infringements of the right to privacy.

3.1. Common Law

The common law recognizes the right to privacy as an independent personality right, which the courts consider to be part of the concept of a person's 'dignitas'. [43] An iniuria occurs when there is an unlawful intrusion on someone's personal privacy (a breach of a person's privacy or an unlawful disclosure of private facts about a person).

The following examples are breaches of privacy recognized by the common law:
Entry into a private residence, the reading of private documents, the disclosure of private documents, listening in to private conversations, the shadowing of a person, the disclosure of private facts which have been acquired by a wrongful intrusion, and the disclosure of private facts in breach of a relationship of confidentiality.[44]

The common law right to privacy has also been regarded to be invaded where a person's photograph is published as part of an advertisement without the consent of the person;[45] by a doctor informing third parties that his patient had HIV;[46] by the wire-tapping or 'bugging' of private premises;[47] and by peeping at a woman while she is undressing.[48]

---

[43] De Waal J, Currie I, Erasmus G *The Bill of Rights Handbook* Juta (2001) 268.
[44] Mentioned by Ackerman J in *Bernstein v Bester* 1996 (4) BCLR 449 (CC) para 69.
[45] *O'Keefe v Argus Printing and Publishing Co Ltd* 1954 (3) S A 244 (C).
[46] *Jansen Van Vuuren v Kruger* 1993 (4) SA 842 (A).
[47] *S v A* 1971 (2) SA 293 (T).
[48] *R v Holiday* 1927 CPD 395.

The examples are all closely related to what should be regarded as private and confidential namely aspects of a person's autobiographical details. There is no indication that the common law principles will be extended to include personal information, which is obtained from cell phone records. The Common Law does not provide an answer on the question whether personal information such as the location and movement of cell phone users should receive protection by the right to privacy. Although the shadowing of a person[49] was regarded to be an infringement on the right to privacy.

3.2. Constitutional right to privacy

Section 14 of the Constitution[50] reads as follows:

> Everyone has the right to privacy, which shall include 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.

This section dealing with the right to privacy consists of two parts.[51] The first part guarantees a general right to privacy and the second part protects against specific infringements of privacy, mainly searches of home and property and seizures and infringements of communications. A right to privacy in information in possession of a third party revealing detail about an individual's movement and location would probably fall under the first part, which guarantees a general right to privacy. As a fundamental right it can be limited in accordance with the limitation clause that is by a law of general application which includes other fundamental rights.[52]

An invasion of privacy in terms of the Constitution must be assessed differently to an invasion under Common Law principles. Ackerman J in *Bernstein*[53] held that the

---

[49] *Epstein v Epstein* 1906 TH 87.
[50] Act 108 of 1996.
[51] De Waal J, Currie I, Erasmus G *The Bill of Rights Handbook* Juta (2001) 267.
[52] Neethling J, Potgieter JM, Visser PJ *Law of Delict* 4th ed, Butterworths (2001) 19.

[53] *Bernstein* para 71.

Constitutional Court should guard against applying the common-law principles, in the determination of whether an invasion of the common law right to privacy has taken place, in a single enquiry. In terms of the Constitution it is not a single enquiry but a two- stage analysis:

1. The party who seeks that certain evidence should be excluded should establish that he/she has a subjective expectation of privacy.
2. That society has recognized that expectation as reasonable.

The limitation of a right to privacy is a separate inquiry. If an infringement of a right took place, it must be determined whether such infringement was justifiable in terms of the Constitution.[54] Section 36 (1) of the Constitution provides:

> "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 limitation
> (c) the nature and extent of the limitation
> (d) the relation between the limitation and its purpose; and
> less restrictive means to achieve the purpose"

If the infringement was not justifiable the aggrieved party must have certain remedies against those who infringed the right. In determining whether a person indeed has a right to privacy in certain information or in information revealing certain details about an individual, a number of Constitutional Court decisions dealing with infringements of the right to privacy have to be examined.

Matters that came before the Constitutional Court can be classified as privacy matters dealing with the inner core, business and court proceedings. No matters concerning informational privacy were at this stage heard by the Constitutional Court.

[54] Act 108 of 1996.

3.2.1. The inner core/ inner sanctum

The strongest protection will be afforded to what constitutes the "inner core" or what takes place in the "inner sanctum" of an individual. The "inner core" of privacy was referred to as what is done in the privacy of an individual's home and what type of erotic material is kept in the privacy of a home. A person's family life, sexual preferences and home environment form part of this inner core, which will receive protection from the right to privacy. It was held in *Case v Minister of Safety and Security*[55] that it is nobody's business what is done in the privacy of one's home. Part of this inner core is the right to make decisions concerning sexual relationships. It is regarded as an aspect of the right to be left alone that was considered in the *National Coalition for the Gay and Lesbian Equality v the Minster of Justice.*[56] What an individual decides regarding his family life, sexual preference and sexual relationships is regarded, as being personal and that he/she must be left alone regarding the decision.

Privacy in the abovementioned examples 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 protected personal space shrinks accordingly.[57] The rights to privacy will be accordingly reduced the further the individual move away from this inner core. As soon as social interaction takes place, for example in business dealings, there will be a differentiation in protection of privacy.

3.2.2. Business

In the decision of *Investigating Directorate: Serious Economic Offences and Others v Hyundai Motor Distributors Pty Ltd and Others; in re Hyundai Motor Distributors Pty*

---

[55] *Case v Minister of Safety and Security* 1996 93) SA 165 (CC), the offence of possession of obscene photographic matter, in contravention of section 2(1) of the Indecent and Obscene Photographic Matter Act was declared inconsistent with the Constitution and declared invalid. The court held that the offence Infringed the right to privacy of individuals and that there was no justification for this infringement. Didcot J held:

> "what erotic material I may choose to keep within the privacy of my home, and only for personal use there, is nobody's business, but mine. It certainly is 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..."

[56] *National Coalition for the Gay and Lesbian Equality v the Minster of Justice*1999 (1) SA 6 (CC).

[57] *Bernstein* para 67.

Ltd and Other v Smit No and others, [58] the Constitutional Court qualified the "inner core" principle. In this case search warrants were authorized, which empowered the respondents to conduct a search and seizure at the place of business of certain individuals. As a result of the operation a large quantity of documents, records and data were seized. The Court held per Langa DP, when the court referred to a previous decision, that it should not be construed to mean that persons no longer retain a right to privacy in their social capacities. The Court stated that:

> "the right, however, does not relate solely to the individual within his or her space. Ackerman J did not state in the above passage that when we move beyond this established "intimate core", we no longer retain a right to privacy in the social capacities in which we act. Thus, when people are in their offices, in their cars or on mobile telephones, they still retain a right to be left alone by the state unless certain conditions are satisfied. Wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such decision will be respected as reasonable the right to privacy will come into play"[59]

Even if there is a move away from the inner core, protection will still be afforded to an individual. When a person is at his place of business or even whilst travelling on an open road, the right to privacy will still be applicable. The more public the undertaking and the more closely regulated, the more attenuated would the right to privacy be and the less intense any possible invasion.[60] Although privacy rights can exist in business, the more public the manner in which a business is being regulated the lesser the invasion of privacy will be. In *Mistry*[61] it was held that the right to privacy protects the invasion of certain places. The entering, searching and seizing of premises in terms of the Medicines and Related Substances Control Act was held to be an unjustifiable breach of the right to privacy. It is and indication that protected personal spaces will also be extended to places of employment and business.

[58] 2000 (10) BCLR 1079 (CC).
[59] *Hyundai* para 16.
[60] *Hyundai* para 27.
[61] *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127(CC).

3.2.3. Information and communications

In classifying privacy rights it seemed that the inner core arguments relates only to space from home to office and from there to the public domain. The question that needs to be addressed is if the protection of privacy will stretch to all sorts of information such as movement and location. The inner core argument does not at all deal with personal information.

In *Simons v P4 Radio,*[62] a matter before the Broadcasting Tribunal, a presenter of the respondent conveyed a listener's cell phone number to other listeners, inviting them to call the said person and debate an issue with him. The presenter did not obtain the listener's permission to convey the number to the public. It was held that the conveying of a person's cell phone number to listeners without that person's consent amounted to an invasion of the listener's right to privacy, which was protected by the broadcasting code and also section 14 of the Constitution.

It was held that the listener did not say anything on air, which necessitated the serious invasion of his privacy. The Tribunal held that it is hard to imagine a set of facts (short of an emergency), which would allow the divulging of the cell phone number without the permission of the person involved.[63] It is clear from this case that although being heard by the Broadcasting Tribunal, that information such as the cell phone number of a user should be regarded as information that is protected. The furnishing of a cell phone number without the consent of the user was regarded as a very serious invasion of privacy.

In a number of decisions the admissibility of intercepted telephone/cell phone conversations came under scrutiny. In *Protea Technology v Wainer*[64] it was held that where an employee make and receive calls that have nothing to do with his or her employer's business, a legitimate expectation of privacy exist in respect of the content

[62] *Simons v P4 Radio* [2003] JOL 10745 BCCSA.
[63] *Simons* para 11.
[64] *Protea Technology v Wainer* 1997 (9) BCLR 1225 (W).

such calls.[65] Conversations by the employee, involving the employer's affairs are not private and not protected by the constitutional right to privacy. The employer is entitled to demand and obtain a full account of the content of such calls.

False and misleading information furnished by the police to obtain a direction to tap cell phones in *S v Naidoo*[66], resulted that the direction was declared invalid. Because the direction issued by the judge was not lawful, the monitoring of the cell phone conversations was an unjustifiable violation of the right to privacy. In *S v Nkabinde*[67] the monitored conversations between an accused and his legal representative was also held to be an invasion of the right to privacy of an accused. It however only relate to the content of telecommunications. It does not address the issue if the protection of privacy will stretch to all sorts of information such as movement and location obtained from cell phone records.

Is there any legislation apart from the Constitution in South Africa that the right to privacy protects the type of non-communicative personal information such as the movement and location of cell phone users?

3.3. The Regulation of Interception of Communications and Provision of Communication- Related Information Act (RICPCRI) No 70 OF 2002.

The privacy of communications receives protection by section 14 (1) d

> "Everyone has the right to privacy, which include the right not to have the privacy of their communications infringed."

Communications are not only protected by the Constitution. The Regulation of Interception of Communications and Provision of Communication- Related Information Act (RICPCRI)[68] also give protection to communications which states that a court order

---

[65] *Protea Technology v Wainer* para 1240.
[66] *S v Naidoo* 1998 (1) BCLR 46 (D).
[67] *S v Nkabinde* 1998 (8) BCLR 996 (N).
[68] Section 62 (1) Act 70 of 2002 repealed with certain provisos the Interception and Monitoring Act No 27 of 1992.

must be obtained to get access to the content of conversations.[69]

Although the content of communications are protected by legislation and the constitution, the problem is that many third parties hold information about persons (clients) and the question that needs to be addressed is if the right to privacy protects this information? Does information about the movement and location of cell phone users form part of this protected information?

In addition to other non-communicative information being kept by cell phone companies, the RICPRCRI Act was enacted to regulate the interception of certain communications and replaced previous legislation dealing with the interception of communications. This Act places a lot more responsibilities on cell phone owners and cell phone companies. It stipulates that much more information about the owners and sellers of cell phones must be kept on record. Information in respect of cell phones and SIM-cards must be obtained, kept and in the event of it being sold, details of the purchaser must be obtained and retained by the seller.[70] There is also a duty on cell phone owners to report the loss, theft or destruction of cell phones[71] and the police must provide written proof that a report to this effect was made.

It is understandable that the legislature intended to eradicate the theft of and trade in stolen cell phones. It is now also an offence to be found in possession of any cell phone or SIM- card where there is a reasonable suspicion that it has been stolen and the possessor is unable to give a satisfactory account of the possession.[72] It is also an offence to acquire or receive a stolen cell phone. The Act creates a reverse onus provision where the onus is placed on the person acquiring the cell phone to prove reasonable cause that a belief that the person from whom it was acquired, was either the owner or had the

[69] S 16 Act 70 of 2003 an application for an interception direction must be made to a designated judge.
[70] S 40 Act 70 of 2002 full names, identity number, residential and business addresses or postal address, a certified photo Copy of the identity document on which a photo appears.
[71] Section 41 Act 70 of 2002.
See also the criticism by S Camerer www.pmg.org.za Justice Portfolio Committee 4 September 2001 " police would think people are 'nuts' for reporting broken cell phones "and her opinion "that police will never comply with the Act to open dockets in this regard".
[72] Section 52.

authority to dispose of the cell phone.[73]

Although it can be appreciated that the reason for enacting the provisions is to compile a data base of the identity of all cell phone users, it will take years to have a detailed record of all cell phone users. Cell phone companies have all these information of persons who have contract phones, but it is highly problematic where the pre-paid customers are concerned. It is estimated that cell phone companies had a pre-paid user base (October 2001) of over five million people for whom they had no identity information.[74] It is presumed that this figure had increased dramatically. Because the identity of pre-paid users cannot at this stage be ascertained from the records of cell phone companies, other investigatory techniques will have to be employed to determine the identity of users.

Once the data base has been compiled and there is a record of the identity of most of the users, it will have the effect that the movements and location of almost every cell phone user will be traceable. It will also be possible to locate a person using a cell phone down to a range of a few metres. A person will be identified and located to almost exactly where he finds himself at a specific time, if the cell phone is used.

Although, subject to certain provisions, it is an offence to provide real-time or archived information to any person other than the customer[75], nothing is mentioned in this Act that the right to privacy protects information regarding the non-communicative information of movement and location of cell phone users. In fact this Act stipulates that more information regarding cell phone users should be kept on data bases by cell phone companies. The fact that the details of movement and location of users can be ascertained by looking at the records, has the possibility that rights of individuals will be infringed, without them even realizing that these details can be accessed by looking at the cell phone records in possession of cell phone companies.

[73] Section 52 (2) "in the absence of evidence to the contrary, which raises reasonable doubt, proof of such possession is sufficient evidence of the absence of reasonable cause'.
[74] www.pmg.org.za Justice and Constitutional Development Portfolio Committee 5 October 2001.
[75] Section 50(1), 50 (2).

3.4. Conclusion

After examining the common law, certain Constitutional Court decisions, decisions of other courts and legislation, it does not satisfactorily answer the questions if information obtained from cell phone records in possession of third parties can rely on protection from the right to privacy.

There is an indication that the right to privacy could be extended to include personal information, which are obtained from cell phone records. It was held that a person when at his place of business or even whilst travelling on an open road can still receive protection under the right to privacy[76] and that the right to privacy is retained even if a move occur beyond the intimate core. Although not expressly stated by the Court, an argument can be raised that movement will take place if a user is talking on a cell phone while driving a vehicle.

The Constitutional Court mainly dealt with privacy matter regarding pornographic material, the right to privacy in a home, but not with privacy to information revealing details about individuals. The content of conversations between accused and legal representative also receives protection under the right to privacy and if false and misleading information is furnished to obtain an order to tap the content of conversation sit was held to be an unjustifiable infringement on the right to privacy. The *Simons* case is an indication that information such as cell phone numbers should be protected, but the question remains unanswered.

It is at this stage not clear that details such as the location and movement of cell phone users should also receive protection. Although to divulge information about the movement and location of a cell phone user is much more serious than giving details of the cell phone number without the consent of the user.

No authority exists in South African law that the right to privacy protects the type of non-communicative personal information, such as the movement and location of cell phone

[76] *Hyundai case.*

users. The enactment of recent legislation namely the RICPCRI Act has the result that even more information in respect of cell phone users will be in possessions of third parties.

It is submitted that the type of information such as the movement and location of cell phone users should be protect by the right to privacy. Because such a lot of information is in possession of third parties the intrusion of the right of privacy of cell phone users should be properly regulated. A study will be made of International Law and other jurisdictions in order to seek authority for this argument. The Constitution prescribes that International Law must be considered when a court, tribunal or forum interprets the Bill of Rights.[77]

[77] Sec 39 (1) of Act 108 of 1996.
When interpreting the Bill of Rights, a court, tribunal or forum
(a) must promote the values that underlie an open and democratic society based on human dignity, equality and freedom;
(b) must consider international law; and
(c) may consider foreign law.

CHAPTER 4 INTERNATIONAL LAW

In this chapter International Law will be referred to in order to ascertain how privacy has been defined internationally and what the extent and scope of the realm of privacy is.

4.1. International Instruments

A number of international instruments dealing with privacy and privacy in personal data evolved over a long period. The fact that vast quantities of information can be transmitted within seconds between countries necessitated the consideration to have privacy protection guidelines in relation to personal data. Some of the instruments will be referred to and the principles contained therein will be discussed. The instruments are:

1. Universal Declaration of Human Rights[78] (UDHR)
2. International Covenant on Civil and Political Rights[79] (ICCPR);
3. United Nations Convention on Migrant Workers[80]
4. United Nations Convention on Protection of the Child[81]

4.1.1. Universal Declaration of Human Rights

The privacy benchmark at international level can be found in the 1948 Universal Declaration of Human Rights. This declaration specifically protects the privacy of territory and communications. Article 12 states:

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

It is evident from this article, which was adopted as far back as 1948 that a need existed that the privacy of individuals should be protected. This declaration stipulates that there

---

[78] Available at www.hrweb.org/legal/udhr.html.
[79] Adopted by General Assembly United Nations Resolution 2200 A (XXI) of 16 December 1966 copy available at http://www.sahr.org.za/civil_and_political_rights.PDF.
[80] Adopted by the general assembly at its 45th session on 18 December 1990 (A/RES/45/158). Availble at www.migrantrsrights.org/Int_Conv_Prot_Rights_Migworkers_Fam_1999_En.html.
[81] Adopted by the General Assembly Resolution 44/25 of 20 November 1989 available at www.unicef.org/crc/fulltext.htm.

should not be any unlawful interference with the privacy of individuals. Numerous other international human rights instruments were adopted in almost the same language, which specifically recognized the right to privacy.

4.1.2. The International Covenant on Civil and Political Rights (ICCPR)

The International Covenant on Civil and Political Rights (ICCPR) adopted in 1966 protects privacy in Article 17.1. It reads as follows:

> "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."

Article 17 is similarly worded to art 12 of UDHR but the word "unlawful" is added. Although the protection of privacy is in this instrument confined to the home, family and the secrecy of correspondence, the UN Human Rights committee commented that article 17 should be given a broad interpretation to include 'the place where a person resides or carries out his usual occupation.'[82] It is thus evident that the right to privacy will receive protection not only at home, but also at the place of an individual's employment.

4.1.3. United Nations Convention on Migrant Workers

The United Nations Convention on Migrant Workers adopted in 1990 contains a privacy provision in similar language in article 14, which reads as follows:

> "No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interferences with his or her privacy, family, home, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference."

It is interesting to note that the content of this convention is also similar to the preceding

[82] Steytler op cit 79.

ones, with both the words "unlawful' and "arbitrary" include when referring to interferences.

4.1.4. United Nations Convention on Protection of the Child

In similar vein the privacy rights of a child is protected in Article 16 of the United Nations Convention on Protection of the Child. It reads as follows:

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

This international instrument includes children specifically to receive protection under the right to privacy. It is quite clear from these instruments that the protection of the right to privacy is essential to human nature. The wording in the instruments is almost identical when the privacy rights of migrant workers and children are referred to. Should interferences take place it must be lawful in terms of domestic laws and not arbitrary. The interference should in any event be reasonable in the circumstances. If legislation is enacted which allows interference it must specify in detail the precise circumstances in which such interferences will be permitted.[83]

4.1.5. United Nations Guidelines Concerning Computerized data files

The United Nations guidelines regarding computerized data files[84] are intended to encourage those UN member states without data protection legislation in place to take steps to enact legislation based on the guidelines. The guidelines are also aimed at encouraging governmental and non-governmental international organisations to process personal data in a responsible, fair and privacy-friendly manner. It contains the following principles:

1. Principle of lawfulness and fairness

---

[83] Steytler op cit 80.
[84] Adopted by the General Assembly of the United Nations on 14 December 1990. Available at www.datenschutz-berlin.de/gesetze/internat/aen.htm.

2. Principle of accuracy
3. Principle of the purpose –specification
4. Principle of interested-person access
5. Principle of non discrimination
6. Power to make exceptions
7. Principle of security
8. Supervision and excess
9. Transborder data flows
10. Field of application

The basic content of these guidelines is that the information must be collected or processed fairly and lawfully. The compilation and keeping of data recorded information must be accurate and only for a specific purpose. People should have the right to know of information is stored about the individual.

4.2. Regional instruments

4.2.1. The Conventions for the Protection of Human Rights and Fundamental Freedoms

This Convention created the European Commission of Human Rights and the European Court of Human Rights to oversee the enforcement of the rights as stipulated in article 8. Article 8 of the Convention[85] which reads as follows:

"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."

[85] Conventions for the Protection of Human Rights and Fundamental Freedoms Rome, signed at Rome on 4

The privacy rights in article 8 refer to respect for family life, home and correspondence. No public authority may interfere with the exercise of this right, unless certain requirements are met. What instances may be covered by notions of "private life" and "correspondence", and under what circumstances individuals have a reasonable expectation of privacy will be investigated.

4.2.2. Decisions of the European Court of Human Rights

The European Court of Human Rights regard article 8 as reflecting a general right to privacy.[86] In *Klass v Germany*[87] the court held the telephone conversations are included in the notions of "private life" and "correspondence." This protection was extended in *Kruslin v France*[88] to not only protect the subscriber to a telephone service, but any user of a telephone.

The record and details of the telephone numbers dialed on a particular phone, the time and the duration of certain calls received protection under article 8 in *Malone v United Kingdom.*[89] It was held that the "metering" of a telephone[90] is a violation of the privacy rights, guaranteed under Article 8.

The process of "metering' (telephone tapping) involved the use of a device (a meter check printer). From the result of this metering, information about the details of the numbers that was dialed on a particular phone and also the time and the duration of the calls could be ascertained.[91]

It was held that the records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the

November 1950, entered into force on 3 September 1953. Available at www.coe.fr/eng/legaltxt/5e.htm.
[86] Steytler op cit 80.
[87] *Klass v Germany* 6 September Series A no 28 at 41.
[88] *Kruslin v France* 24 April 1990 Series A no 176-a.
[89] *Malone v United Kingdom* 2 August 1984 Series A no 82.
[90] *Malone v United Kingdom* para 62.

subscriber also amounted to, in the opinion of the court, to an interference with a right as guaranteed by article 8.[92] Information regarding the telephone numbers dialed from a specific telephone is being regarded as private and important enough to be protected as notions of private life and correspondence under article 8.

In *Niemitz v Germany*[93] a broad interpretation was given to private life and the home. It was held that the office of a lawyer fell within the protected sphere of privacy

Information conveyed to a third party, although private, will not automatically receive protection under article 8. In *M.s v Sweden* [94] it was held that it would depend on the manner in which the information was conveyed to the third party. If the information had been disclosed to another public authority and therefore to a wider circle of public servants, the disclosure of the information could be justified. This will be the case even if the information conveyed was of a confidential nature.

There had been an interference with the applicant's right to respect for private life under paragraph 1 of article 8, but that the interference had been justified under paragraph 2. Although the medical records contained personal information that was indeed of a very personal and of a sensitive nature, it was conveyed to a wide circle of public servants that had access to the information.

It thus seems that the manner in which information is conveyed to a third party and the number of people who will have access to the information plays an important part in the right to receive protection in the information.

4.2.3. American Convention of Human Rights[95]

Article 11 of the American convention on human rights sets out the right to privacy in

---

[91] *Malone v United Kingdom* Para 83.
[92] *Malone v United Kingdom* Para 84. This is a contrary view to what was held in the United States case of *Smith v Maryland* where it was held that no reasonable expectation of privacy exist in telephone numbers recorded by pen registers.
[93] *Niemits v Germany* 16 December 1992 Series A no 251 B.
[94] *M.S. v Sweden* (74/1996/693/885) 27 August 1997.

terms similar to the Universal Declaration on Human Rights. It states:

"1. Everyone has the right to have his honor respected and his dignity recognized.

2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or 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 attack."

It is interesting to note that that the African Charter on Human and Peoples' Rights [96]does not make any reference to privacy rights.

A study of the principles of data protection contained in various instruments will now be made. The non-communicative information such as the movement and location of cell phone users is an example of data being captured by cell phone companies. This analysis is done in order to ascertain if the right to privacy should protect information such as the non-communicative information/data obtained from the usage of cell phones.

4.2.4. Instruments dealing with data protection:

During the last twenty years technology developed at an alarming pace. It resulted in the automatic processing, collection and storage of personal information of individuals. A need developed to have certain regulations to safeguard the rights of individuals.

The Basic Principles for Data Protection is contained in various regional instruments. The principles are very similar to the United Nations guidelines concerning computerized persona data files. Some of them are:

1. The Council of Europe: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CoE Convention);[97]
2. Organisation for Economic Cooperation and Development Guidelines on the

[95] Pact of San Jose. Costa Rica 22 November 1969 entered into force on 18 July 1978.
[96] Adopted by the 18th Assembly of the Heads of State and Government of the OAU on 27 June 1981 at Nairobi.
[97] Convention For the Protection of Individuals with regard to the Automatic Processing of Personal Data

Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines);

3. European Union Directive on the Protection of Individuals with regard to the processing of Personal Data and the Free Movement of Such Data (EU directive)

These three instruments contain specific rules covering the handling of electronic data These rules describe personal information as data that are afforded protection at every step from collection to storage and dissemination.

The guidelines contain almost similar principles concerning the minimum guarantees that should be provided in national legislation and the duties are placed on all parties involved in the process. Guidelines are furnished regarding the quality, categories and security of data (information). Safeguards, sanctions and remedies are included in these principles for the benefit of users. It recommends that users should receive an extended protection to their right to privacy where information is kept by third parties. [98]

4.2.5. Summary of principles regarding data protection:

(a) The principle of lawfulness and fairness.

The processing of personal data shall be obtained and processed fairly and lawfully[99]

(b) Purpose specification principle

The purpose for which information is stored and for which they are to be used

---

Convention ETS. No 108 Strasbourg.191 available at http://www.privacy.org/pi/intl_orgs/coe/dp_convention_108.txt.

[98] Copy of directive available at www.cdt.org/privacy/eudiretive/EU_Directive_html.

[99] CoE Convention, Article 5 Quality of data
"Personal data undergoing automatic processing shall be obtained and processed fairly and lawfully..."

OECD Guidelines, Collection limitation principle
"There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and where appropriate with the knowledge or consent of the data subject."

EU Directive, A principle of fairness is also established regarding the collection of data under which an individual is given the option of whether to provide the information requested or not.

should be specified.[100]

(c) Principle of Accuracy

Information should be accurate, complete and kept up to date.[101]

(d) Use Limitation Principle

Information should only be used for the purpose it has been stored and not stored longer than is required.[102]

---

[100] CoE Convention, Article 5 Quality of data
" ...b stored for specified and legitimate purposes and not used in a way incompatible with those purpose. c adequate, relevant and not excessive in relation to the purposes for which they are stored;..."

OECD Guidelines, Data quality principle
"Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes should be accurate, complete and kept up to date."

Purpose specification principle
"The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."

EU Directive
An obligation is established to collect data only for specified, explicit and legitimate purposes and to maintain that information only if it is relevant, accurate and up-to-date.

[101] CoE Convention, Article 5 Quality of data
" ...d. accurate and, where necessary, kept up to date."

OECD Guidelines, Data quality principle
"Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes should be accurate, complete and kept up to date."

EU Directive An obligation is established to collect data only for specified, explicit and legitimate purposes and to maintain that information only if it is relevant, accurate and up-to-date

[102] CoE Convention, Article 5 Quality Of Data
"...e preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

OECD Guidelines, Use limitation principle
"Personal data should not be disclosed made available or otherwise used for purposes other than those specified in accordance with paragraph 9 except:
(a) with the consent of the data subject
(b) by the authority of law."

(e) Security Safeguard Principle

There should be reasonable security safeguards against the risk of unauthorised access.[103]

(f) Safeguards for the data subject Principle

The data subject should be able to establish if information about him/her is kept and the identity of the controller and have access to the information[104]

---

[103] CoE convention, Article 7, Data security
"Appropriate security measures shall be taken for the protection of personal data stored in automated files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."

OECD Guidelines, Security safeguards principle
"Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access destruction use modification or disclosure of data."

EU Directive
Where data is transferred from a European Union country to a non-European country, the data protection directive establishes a basic rule that the non Eu country receiving the data must provide "adequate level" of "data protection."

[104] CoE Convention, Article 8 Safeguards for the data subject
" additional safeguards for the data subject any person shall be enabled a to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file, b to obtain at reasonable intervals and without excessive delay or existence confirmation of whether personal data relating to him is stored in the automated data file as well as communication to him of such data in an intelligent form, c to obtain as the case may be rectification or erasure of such data if theses have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in articles 5 and 6 of this convention, d to have a remedy if a request for confirmation or as the case may be communication or erasure as referred to in paragraphs b and c of this article is not complied with."
OECD Guidelines, Individual participation principle
"An individual should have the right:
(a) To obtain from a data controller or otherwise confirmation of whether or not the the data controller has data relating to him
(b) to have communicated to him data relating to him within a reasonable time at a charge, if any, that is not excessive; in a reasonable manner and in a form that is readily intelligible to him
(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial and
(d) to challenge data relating to him and if the challenge is successful to have the data erased, rectified, completed or amended."

Eu Directive
The directive also provides data subjects with a number of important rights; including the right to access to data; the right to know where the data originated; the right to have inaccurate data rectified; the right of recourse in the event of unlawful processing of data; and the right to withhold permission to use their data in certain circumstances.

4.3. Conclusion

Article 12 of the Universal Declaration of Human Rights set a benchmark regarding the international recognition of the right to privacy. The basic content of this right is that no one should interfere with an individuals privacy, that of his family, his home or correspondence. A broader interpretation to include place of employment is also suggested.

Should interferences take place it must be lawful in terms of domestic laws and not arbitrary. The interference should in any event be reasonable in the circumstances.
The wording of the right to privacy in various other international instruments such as the ICCPR, UN Convention Migrant Workers, and UN Convention Protection of the Child is based on UDHR and almost identical to it.

The European Court of Human Rights when it had to decide on the general right to privacy as stipulated in article 8 held that telephone conversations are included in the notions of "private life" and "correspondence. That the right to privacy should be extended to not only protect the subscriber to a telephone service, but any user of a telephone.

The record and details of the telephone numbers dialed on a particular phone, the time and the duration of certain calls also received protection under article 8 and telephone taping was held to be a violation of the privacy rights, guaranteed under Article 8.

A broad interpretation was given to private life and the home to include the offices of lawyers to fall within the protected sphere of privacy. However information conveyed to a third party, although private, will not automatically receive protection under Article 8.

A number of regional instruments contain various guidelines encouraging organisations to process the recording of personal data in a responsible, fair and privacy-friendly manner. The content of the guidelines contained in the Coe convention, the principles in the OECD guidelines and in the EU directive are in essence very similar. All these

instruments work from the assumption that personal information is indeed worthy of protection and that the recording thereof and access thereto should be properly regulated. In the next chapter a comparative study of American and Canadian jurisprudence will be undertaken.

CHAPTER 5 COMPARATIVE JURISDICTIONS

A study will firstly be done of how privacy issues have been dealt with in the United States of America. Steytler [105]notes that South African courts most frequently cite the jurisprudence of the United States, Canada and some other common wealth countries. The reason for referring to America first, is because the jurisprudence of the United States of America has been influential in other countries also and an examination will be made under what circumstances information, details of an individual will be protected. The questions that need to be answered are:

When will a right to privacy exist in certain information?

Does the right to privacy protect information of individuals in possession of third parties?

5.1. United States of America:

An analysis will be made to determine if the nature of information obtained from cell phone records warrants protection and to determine if a right to privacy exists in this type of information. The word "privacy' is not mentioned in the Fourth Amendment or anywhere else in the American Constitution. There are some writers[106] who are of the opinion that scholars in America have been unable to agree upon one-size fits all definition of privacy and it actually consists of five distinct species[107]:

"1. **The Privacy of Warren and Brandeis**[108] (Tort Privacy): is the right to be let alone with respect to the acquisition and dissemination of information concerning the person, particularly through unauthorized publication, photography or other media.

2. **Fourth Amendment Privacy:** (relating to warrantless governmental searches and seizures), the right to be let alone, with respect to governmental searches and seizures which invade a sphere of individual solitude deemed reasonable by society. (as discussed below)

[105] Steytler N C *Constitutional Criminal Procedure* op cit 13.
[106] Gormley K "One Hundred Years of Privacy" 1992 *Wisconsin Law Review* 1335.
[107] Gormley para 1434.
[108] Warren and Brandeis, "The Right to Privacy" (1890) 4 *HLR* 193.

3. **First Amendment Privacy:** the right to be let alone, when an individual's freedom of speech threatens to disrupt another citizen's liberty of thought and repose.
4. **Fundamental-Decision Privacy:** the right to be let alone, with respect to fundamental (often unanticipated) decisions[109] concerning the individual's own person, which are explicitly reserved to the citizen (rather than ceded to the government) by the terms of the social contract. (Fourteenth amendment privacy.
5. **State Constitutional Privacy:** the right to be let alone, with respect to variety of private and governmental intrusions generally often overlapping with species number one through number four above, yet often extending greater protections to the citizen by virtue of independent state constitutional provisions."

It is submitted that non-communicative information obtained from cell phone records would probably fall under privacy referred in the Fourth Amendment. To establish if a right to privacy exists in certain information, which reveals certain details of an individual, an analysis will be made of how the privacy under the Fourth Amendment developed and what constituted unreasonable searches and seizures under the Fourth Amendment.

The Fourth Amendment to the United States Constitution reads:

> "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."

[109] *Griswold v Connecticut* 381 U.S. 479 (1965).
Where it was held that a law forbidding the use and distribution of contraceptives violated the right of "marital privacy".
Roe v Wade 416 U.S. 113 (1973).
The substantive right of privacy inherent in the due process clause was
"broad enough to encompass a woman's decision whether or not to terminate her pregnancy.

The Fourth Amendment required that there should be a warrant, before a search and seizure would be justified in terms of this amendment. A development also took place that there should be "a reasonable expectation of privacy", before a search is regarded as being unreasonable. It must be established that a reasonable expectation of privacy exists in certain information before prior authorization in the form of a warrant will be required.

5.1.1. Development of "a reasonable expectation of privacy"

To determine if a reasonable expectation of privacy exist in certain information, an analysis will be done of how the notion of "reasonable expectation" developed in American case law.

The physical invasion of property was at first required to warrant protection under the Fourth Amendment. In the 1928 case of *Olmstead v United States*[110], the court held that where no physical invasion of the defendant's premises occurred, there would not be protection under the Fourth Amendment. Wiretapping was thus not covered by the amendment because the government had not physically invaded the defendant's premises.

In *Goldman v United States,* it was found that a detector placed against the wall of an adjoining room, did not qualify as a search and seizure.[111] During this period the notion was reinforced that violations of the Fourth Amendment only took place where there was a physical trespass on property or seizure of material goods. It was thus allowed that government's agents could employ dictaphones and microphones as long as a defendant's property or person was not touched.[112]

[110] *Olmstead v United States* 277 U.S. 438 (1928).
[111] *Goldman v United States*, 316 U.S.129 (1942).
[112] *Lee v United States* 343 U.S. 747 (1952).
The Court found no violation of the Fourth Amendment where an undercover agent wore a concealed microphone, and his conversations with the defendant in a Chinese laundry was monitored by a fellow agent. It was found that there had been no physical trespass, since the defendant voluntarily spoke with the wired agent.

In the 1961 decision of *Silverman v United States,*[113] the courts changed their approach. They disallowed the use of a "spike mike" driven into the wall of a row house, where it tapped into the heating duct and allowed officers to monitor conversations within the defendant's entire house. However they still regarded physical invasion of the premises as a requirement and found the contact with the heating duct constituted a physical invasion of the premises.

5.1.2. The two-requirement test

Katz v United States[114] initiated the development that although the physical property of the defendant had never been violated, a reasonable expectation of privacy can be present. It was found that the government could not electronically eavesdrop on a conversation held by a person in a pubic booth by attaching a listening device to the outside of the booth without complying with the Fourth Amendment.

Charles Katz was arrested by federal authorities in Los Angeles, after an electronic listening device attached to the outside of a telephone booth was used to record his conversation, as he ran bookmaking activities through Boston and Miami. The Court found that this mode of gathering evidence did not comply with the Fourth Amendment, even though the physical property of the defendant had never been violated. Justice Stewart opinion was that the Fourth Amendment "protects people, not places"[115]. Then Justice Stewart's went on dealing with the privacy concept under the Fourth Amendment: "[w]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'

Justice Harlan in his concurring judgment in *Katz*, initiated a notion of *"reasonable expectation of privacy"*, which is regarded as the standard for search and seizure in criminal procedure.[116] A two-requirement test of reasonable expectation of privacy

[113] *Silverman v United States* 365 U.S. 505 (1961).
[114] *Katz v United States* 389 U.S. 347, 353 (1967).
[115] *Katz v United States* at 351.
[116] *Katz* at 360 –361.
This two requirement test of "reasonable expectation of privacy" was soon afterwards adopted by the majority of the court in *Terry v Ohio* 392 U.S. 1, 9 (1968).

developed. *Kyllo vs. United States* confirms this two-requirement test and it was held that:

> "[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable... a Fourth Amendment search does not occur- even in the explicit projection of a house – unless the individual manifested a subjective expectation of privacy in the object of the challenged search, and society [is] willing to recognize that expectation as reasonable"[117]

A Fourth Amendment search will occur when a subjective expectation of privacy that society recognizes as reasonable, is violated. It will thus depend on the following:

(a) Does a subjective expectation of privacy exist in certain information (the object of the search)?

(b) Is the subjective expectation being recognized by society as reasonable?

It was held in the case of *Kyllo* that no subjective expectation of privacy existed, because any amount of heat emerging from the home of the appellant was not concealed. The imager did not expose intimate details of his life. On appeal it was held that where the government uses a [sense-enhancing] device, not in general public use, to expose details of the home that would previously have been unknown without physical intrusion, the surveillance is a search and is presumptively unreasonable without a warrant.

In this case of *Kyllo* confirm the two-requirement test mentioned in *Katz*. Firstly there must subjectively be a reasonable expectation of privacy in the mind of the person whose right will be/ was infringed. Secondly in addition to the individual manifesting a subjective expectation of privacy in the object of the challenged search, the society [is] [must be] willing to recognize that the expectation as reasonable. The second requirement will bring an objective element into the test. If the society regards the expectation as reasonable, the Fourth Amendment protection will kick in.

1.The individual had an "actual" expectation of privacy and
2 That expectation was "one that society was prepared to recognize as 'reasonable' ".

[117] *Kyllo v United States* 533 U.S. 27 (2001) 190 F 3d 1041.

To ascertain if a reasonable expectation of privacy exist in information such as the location and movement of cell phone users, it must first be determined if cell phone users have a legitimate expectation of privacy in these details.

5.1.3. Information revealing certain details

To ascertain if an individual has a right of privacy in non-communicative information revealing details such as location and movement, certain decisions will be referred to. In *Smith v Maryland*[118] the Supreme Court held that an individual targeted in a pen registering does not have a reasonable expectation of privacy in the telephone numbers dialed from his home telephone number. The question was posed whether the government was required to obtain a warrant to get details of telephone numbers that was dialed. The register records the date, time, and length of calls, usually information that is already gathered by phone companies for billing purposes by a communications service provider. According to the court, an individual is assumed to know that in dialing numerical information as conveyed to the phone company, that the company records the information for a variety of legitimate business purposes.

Because the user voluntarily conveyed this information to the phone company, the installation of and use was not a search and no warrant was required. It seems that if there is an element of voluntaries present, the expectation of privacy is diminished. The fact that this detail was conveyed to the phone company is being regarded as waiving the reasonable expectation of privacy in this information.[119]

If information is revealed about to another person /other institutions there also seem to be no expectation of privacy in that information. The bank records of an individual were subpoenaed in *United States v Miller.*[120] It was held that a restrictive meaning should be ascribed to reasonable expectation of privacy in this case, where a bank depositor claimed that the government had to satisfy Fourth Amendment standards in order to obtain his financial records from his bank.

---

[118] *Smith v Maryland* 442 U. S 735 (1979).
[119] See also *M.S v Sweden* above.
[120] *United States v Miller*, 425 U.S. 435 (1976).

The Court held that the depositor had no legitimate expectation of privacy in financial information voluntary conveyed to the banks and because the information was exposed to their employees in the ordinary course of business. The Court found that the depositor takes the risk in revealing his affairs to another. Once the information is revealed that person may convey the information to others. An exclusion of the reasonable expectation of privacy seemed to have developed in *Smith* and *Miller's* cases. If the information was voluntarily conveyed there cannot be reasonable expectation of privacy in the information. This is contrary to what has been decided in *Malone* and *Simons*.

The expectation of privacy must not only be subjective, but the second requirement is if society is willing to regard this expectation as being reasonable.

5.1.4. Requirements for a warrant.

Once a reasonable expectation of privacy has been established in a thing/item /information it must be determined whether the search was conducted in a reasonable manner. Put differently was the warrant properly obtained and issued. The Fourth Amendment to the United States Constitution is quite clear in this regard that no warrant shall be issued unless the following criteria have been met;

(a) There must be probable cause;

(b) The probable cause statement must be furnished under oath or affirmation;

(c) The place that is the subject of the search must be described and

(d) The person thing/item to be seized must also be described.

Because of the exclusion of the reasonable expectation of privacy which seemed to have developed in *Smith* and *Miller's* cases, it is submitted that the United States Supreme Court will in all probability not afford protection to the non-communicative cell phone information.

5.2. Canada

The jurisprudence that developed under the Canadian Charter of Rights and Freedoms has been the most influential in South African courts.[121] A study of Canadian jurisprudence will be done to ascertain how information revealing certain details about individuals has been dealt with. An investigation will also be done to determine if the right to privacy should protect information in possession of third parties. There is no explicit right to privacy in Canada's Constitution and Charter of Rights and Freedoms. However, in interpreting section 8 of the Charter, which grants the rights to be secure against unreasonable search or seizure, Canadian courts have recognized an individual's right to a reasonable expectation of privacy.[122]

Privacy at the federal level is protected by two acts: the 1982 federal Privacy Act and the 2001 Personal Information and Electronic Documents Act (PIPEDA).The federal Privacy Act of 1982 regulates the collection, use and disclosure of personal information held by federal public agencies and provides individuals a right of access to personal information held by those agencies, subject to some exceptions, including an exemption for court records.

PIPEDA is applicable to private sector organizations that process personal information "in the course of a commercial activity," and for federally regulated employers with respect to their employees. It does not apply to information collected for personal, journalistic, artistic, literary, or non-commercial purposes.

The Canadian Charter of Rights and Freedoms guarantees certain rights for individuals. Section 8 and 24 of the Canadian Charter[123] reads as follows:

> S 8 Everyone has the right to be secure against unreasonable search or seizure
>
> S 24. (1) Anyone whose rights or freedoms, as guaranteed by this chapter,

[121] Steytler NC *Constitutional Criminal Procedure* Butterworths 1998 op cit 13.
[122] *Hunter v Southam* [1994] 2 S.C.R.145.
[123] Section 8 Canadian Charter of Rights and Freedoms.

have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy, as the court considers appropriate and just in the circumstances.

(2) where, in proceedings under subsection (1), a court concludes that evidence was obtained 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 in disrepute.

The right to privacy is also being regarded as not to be subjected to unreasonable searches or seizures. If evidence were obtained contrary to these principles it will be excluded if it is found that the admission of the improperly obtained evidence would bring the administration of justice into disrepute. In *Dyment*[124] it was stated that:

> "In modern society the retention of information about oneself is extremely important and that we may for one reason or another, wish to be compelled to reveal such information, but there will be situations when we will feel that we are not compelled and that information about us should not be revealed to others."

5.2.1. The two-stage test

Canada also developed a notion of "reasonable expectation of privacy". In *Hunter v Southam*[125] the Supreme Court of Canada ruled that the guarantee provided for in section 8 of the charter is only applicable where individuals have a reasonable expectation of privacy. The purpose of section 8 is to protect individuals from unjustified state intrusions. In *British Columbia Securities Commission v Branch*[126] in referring to *Hunter* the Court state that the context within which the violation takes place must be considered, for it is the context which determines the expectation of privacy.

In *R v McKinley*[127] it was held that individuals have different expectations of privacy in

[124] *R v Dyement* [1988] 2 S.C.R 417.
[125] *Hunter v Southam* [1984] 2 S.C.R. 145.
[126] *British Columbia Securities Commission v Branch* (1995) 97 CCC (3d) 565 (SCC).
[127] *R v McKinley* [1990] 1 S.C.R. 627 645.

different contexts and with regard to different kinds of information and documents. There should be a standard of review of what is reasonable in a given context and this standard must be flexible if it is to be realistic and meaningful. The test is Canada is therefore also a two-stage test. Firstly an individual must manifest a reasonable expectation of privacy in the item/information. Secondly an objective review to determine if the expectation was indeed reasonable will determine if the intrusion was justified or not. A reasonable expectation of privacy is to be determined on the basis of the totality of the circumstances. The factors to be considered in accessing the totality of the circumstances may include, but are not restricted to,

(a) The presence at the time of the search
(b) The possession of the property or place searched
(c) The ownership of the property or place,
(d) Historical use of the property or item,
(e) The ability to regulate access, including the right to admit or exclude others from the place
(f). The existence of a subjective expectation of privacy and
(g) The objective reasonableness of the expectation.[128]

It was held in *Thompson Newspaper Ltd, v Canada*[129] that whether the public authority takes the documents or compels that person to hand them over it impacts on the person's right to privacy and will be regarded as a seizure in terms of section8.

5.2.2. R v Plant

The case of *Plant* is critical for this investigation. It specifically deals with the ambit of the problem at hand and it was held that the right to privacy should be confined to a biographical core of personal information, which may reveal intimate details of an individual's lifestyle and personal choices. To ascertain if information will qualify to receive this protection the following pertinent questions were discussed:

[128] *R v Edwards* [1996] 1 S.C.R. 128.
[129] *Thompson Newspaper Ltd, v Canada (1990) 67 DLR (4th) 161 (SCC).*

(a). When will a reasonable expectation exist in certain information of an individual and what must the nature of the information be to justify to be protected by the right to privacy?

(b) It further dealt with information about an individual, which is in possession of a third party.

5.2.2.1 The facts

On 9 March 1990 after the Calgary police received an anonymous tip, which indicated that marihuana was being grown at a certain dwelling; the police used a computer terminal, which was linked to the city of Calgary main frame .The main frame, was designed to allow police to check the electrical consumption at specified addresses.

The police, without obtaining prior judicial authorization, used a terminal linked to the electric utility's computer to check the electrical consumption of the accused. The electrical consumption of the accused over a period of six months was four times higher than the average of two other residences with which his consumption was compared.

This information was used to obtain a search warrant to search the premises. One of the questions the court had to decide was: did the information obtained from the computer records of the electricity company reveal intimate details of the lifestyle and personal choices of an individual? If it was found that the accused had a reasonable expectation of privacy in this information, the police had to obtain a warrant to access the information.

It was held that to answer the questions the following factors had to be considered

1. the nature of the information itself;
2. the nature of the relationship between the party releasing the information and the party claiming its confidentiality;
3. the place and manner where the information was obtained; and
4. the seriousness of the crime being investigated.

The court stated that in considering the abovementioned factors a balancing of interests

must take place. On the one hand the individual's dignity, integrity and autonomy must be protected and on the other hand the interest of effective law enforcement must be considered. There was disagreement on how this matter should be resolved and the court delivered was not unanimous in judgment. Firstly an analysis of the majority judgment will be done and thereafter the minority judgment will be referred to.

5.2.2.2. Majority judgment

The majority of the Court[130] considered the following factors: the nature of the information; the relationship between the party releasing the information and the party claiming its confidentiality; the place and manner where the information was obtained; and the seriousness of the crime being investigated.

(a) The nature of the information

The Court held information seized must be of a "personal and confidential" nature. The information must be such that it tends to reveal intimate details of the lifestyles and personal choices of the individual. The computer records revealing the pattern of electricity consumption in a residence cannot be said to reveal intimate details of a person's life. It revealed the pattern of electricity consumption in the residence. It was held that the electricity consumption revealed very little about the private decisions of the occupant of the dwelling.[131] It only revealed how much electricity was consumed by the occupants in that dwelling. An inference could not be drawn that an individual made certain personal and private decisions by only looking at the electricity consumption.

In the Court of first instance,[132]it was held that: The information was created in the context of a commercial transaction. The information was collected in order for the electricity company to furnish the user with an electricity account. It is different compared to the privacy expected with regard to confidential information in attorney/client and patient/doctor relationships. It was held in this court that the

[130] The majority judgment of Lamer C.J, La Forest, Sophinka, Gonthier, Cory and Iacobucci JJ, was delivered by Sophinka J.
[131] *R v Plant* [1993] 3 SCR 281.
[132] Court of Appeal of Alberta (1991), 116 A.R. 1.

information belonged to the electricity supplier and not to the appellant. It was created for billing purposes, for the company's use and not for the customer's use. Thus in the court a quo, the use of the information also determined the nature thereof and had an influence if the information should be protected or not.

(b) The relationship between the party releasing the information and the party claiming its confidentiality

It was held that the nature of the relationship between the appellant and the commission could not be characterized as a relationship of confidence. The records were prepared as part of an ongoing commercial relationship and there were no evidence that the commission was contractually bound to keep the records confidential. The court however qualified the above statement in saying that it was not suggesting that records prepared in a commercial context can never be subject to the privacy protection in terms of section 8. It was stated that if it were found that commercial records contain material, which meets the "personal and confidential" standard, the commercial nature of the relationship would not prevent the information to be protected by the right to privacy.

It was further held that it was generally possible for an individual to inquire about the electricity consumption at a particular address and that the information was subject to inspection by members of the public at large. No policies had developed against releasing electrical consumption information to police. It was the policy of the Calgary commission to permit police access to the computer bank. The access was granted through a computer password held by the police.

(c) The place and manner where the information was obtained:

The court found that the place and manner in which the information was retrieved also indicated that the appellant had no reasonable expectation of privacy in respect of the computerized electricity records. The police were able to obtain the information on-line, in terms of an agreement with the commission. There was no intrusion into private places, nor did it involve state agents invading personal computer records, which were confidentially maintained by private citizens. It was held that the fact that the police used

a password may have suggested an element of privacy, but it could also have suggested that it was merely intended to ensure that the information was available to the police on-line. It was stated that the search was in any event not conducted in an intrusive or high handed manner.

(d) The seriousness of the crime being investigated

The court held that the seriousness of the offence militated in favour of the conclusion that the requirements of the law enforcement agency outweighed the privacy claimed by the appellant. The court held further that although the participation in the illicit trade of marijuana may not have been as serious as the trade in other narcotics such as cocaine, it remained an offence, which is taken very seriously by law enforcement agencies.

In conclusion, the majority held that the nature of the information, the relationship between the appellant and the commission, the place and manner of the search and the seriousness of the offence under investigation, did not warrant a conclusion that the appellant had a reasonable expectation of privacy in relation to the computerized electricity records which outweighed the state's interest in enforcing the laws relating to narcotics offences.

5.2.2.3. The minority judgment

The minority judgment of Mclachlin J, stipulated that the question that had to be decided was: Did the individual have a reasonable expectation that the information in possession of the utilities commission would be kept in confidence and restricted to the purpose for which it is given? It was held that although the electricity consumption records was found to be close to the line, the evidence of the records disclosed a sufficient expectation of privacy to require that the police should obtain a warrant before the information was solicited. The information should not have been divulged to strangers without proper legal authorization.

The following reasons were furnished for the finding:

There was no evidence that the records was available to the public, the police only

obtained access by reason of a special arrangement they had with the utilities commission. In disagreeing with the majority it was found that the details of electricity consumption was capable of telling much about the individual's lifestyle. It indicated how many people were residing in the dwelling and what sort of activities probably took place inside the dwelling. The records told a story about what happened inside a private dwelling, the most private of places.

It was held that a reasonable person who looked at the facts would in all probability conclude that the records would only be used for the purpose, for which they were made, namely the delivery and billing of electricity. The reason that the police wanted access to the records was precisely that they wanted to learn about the appellant's personal lifestyle, the fact that he was growing marihuana. Although the records are not as revealing as many other types of records, they disclosed important personal information.

The minority stated that the point that should have been considered was not if the relationship between the individual and the company was one of confidence, but whether the particular records disclosed a reasonable expectation of confidence. It was also disagreed with the majority finding that the records were generally available to the public. Only the police had access to the information. The police had to use a special computer which they had been given in confidence, to access the information. This aspect was regarded to be a very important factor. If it was found that the records were open to the public the minority might have agreed with the majority that the appellant had no reasonable expectation of privacy in the records.

The judge also disagreed with the majority on the aspect that the police did not have to intrude into places ordinarily considered private like a house or hotel room to get the information. It was found that computers may and should be regarded as being private. Especially if the computers contain information, which is subject to legal protection and in which the subject has a reasonable expectation of privacy. Computers can contain a wealth of personal information. Information, depending on its character may be as private as any found in a dwelling house or hotel room.

Regarding the seriousness of the offence, reservations were expressed to apply a case by case approach to determine whether a warrant is required or not, to obtain information. It was held that the test should remain whether the individual has an expectation of privacy in the information. If that test is met, a search without a warrant will constitute a violation, even if the suspected offence is a serious one.

It is submitted that the views of the minority judgment should be preferred in evaluating the reasonable expectation of privacy in information obtained from the electricity company. The details of electricity consumption was capable of telling much about the individual's lifestyle namely it indicated how many people were residing in the dwelling and what sort of activities probably took place inside the dwelling. The majority held the contrary, that the electricity consumption revealed very little about the private decisions of the occupant of the dwelling and that it only revealed how much electricity was consumed by the occupants in that dwelling. It is submitted that an inference could be drawn that an individual made certain personal and private decisions by only looking at the electricity consumption.

5.2.3. Privacy in movement and location

The investigation in this work will now proceed to ascertain if any authority exist for an argument that a person can have a reasonable expectation in movement and location.

In the dissenting judgment in *R v Wise*[133] it was stipulated that a reasonable expectation could exist in information that reveals the movement of an individual. The majority decision did not mention anything about the right to privacy of movement or whereabouts, nor did it mention anything about the existence of a reasonable expectation of privacy in movement. La Forrest J in his dissenting judgment (hereinafter referred to as the judgment of the court) made some interesting remarks, which are very relevant to this research. The Court held that the installation of the tracking device in the appellant's car constituted an unlawful trespass and violated the privacy rights under section 8 of the Charter. The use of the device that monitored the movements of the individual also violated section 8.

[133] *R v Wise* [1992] 1 S.C.R. 527.

It was stated that an individual has a reasonable expectation of privacy not only in his communications, but in his movements as well, even when traveling on a public road. It was held that if an individual is in a vehicle and on a public road, the person's privacy rights are also protected. In this case the movements of an individual were tracked.

The Court drew the distinction between the risk individuals run by having their activities monitored by others and the police monitoring the movements of individuals. It was held that a person's daily moves, whilst traveling, can be observed and even be monitored by others. However, it is not the same as the risk that agents of the state, in the absence of prior authorization, will be able to track every move of individuals. If the police in this case made use of this technology, every move will be tracked. It was not a casual glance, look or observation as in the case of other individuals, but a question that every move will be tracked, which will not be the case if ordinary citizens just look at individuals passing them and being noticed whilst driving or walking somewhere.

It was found that it is constitutionally unacceptable that the state should justify the unauthorized surveillance of individuals on the mere fact that other individuals can observe a person. The degree, to which that person took measures to shield his activities from the scrutiny of other persons, should not be decisive to decide if a person had a reasonable expectation of privacy in his movements. Thus, if a person tries to conceal his movements or were hiding, it should not be indicative that he had a reasonable expectation of privacy.

The surreptitious electronic tracking of a person's movement was held to be a grave threat to the privacy of an individual. Therefore, to track the movements of an individual, prior judicial authorization should be required. It was held that the issue of a prior judicial authorization will call for an objective showing of reasonable and probable cause and this should generally be required of those seeking to employ electronic devices in the pursuit of individuals. It is submitted that this approach is correct.

It seems that a prisoner does not have a reasonable expectation of privacy in movement. In *R v Dorfer* [134] the court dealt with prisoners. Details about the time and place where the appellant would receive treatment, was furnished to the police. The information about the movements of a specific prisoner was given to police with the subject's consent. The Court held that in prison the whereabouts of an offender at any given time is information not expected to be confidential and it relates to the proper functioning of a criminal justice system. Thus a prisoner it seems cannot rely on the fact that he has a reasonable expectation of privacy regarding his movements. One could then draw the inference that persons in police custody, arrested persons, or those who are lawfully detained will not have a right to privacy in their movements. It flows from this argument that everyone else does have a right to privacy in movement.

In *Dagg* v *Canada*[135] it was found that a person could have a reasonable expectation in his arrival and departure from a certain location and that this movement should also be protected.

A request was filed with the Department of Finance for copies of logs containing the names, identification numbers and signatures of employees entering and leaving their workplace on weekends.[136] These logs were kept by security personnel for safety and security reasons, but not for verifying overtime claims. The relevant logs were disclosed, but the employee's names, identification numbers and signatures were deleted on the basis that this information disclosed personal information and was thus exempted from disclosure.

The appellant sought a review of the Minster's decision and filed a complaint with the information commissioner, arguing that deleted information should be disclosed by virtue of exceptions to personal information in the Privacy Act.[137] The Federal Court, trial division, on a review of the Minster's decision, found the information not to be personal

[134] *R v Dorfer* (1996) 104 CC (3d) 528 (BCCA).
[135] *Dagg v Canada (Minister of Finance)* [1997] 2 S CR 403.
[136] *Dagg v Canada (Minster of Finance) [*1997] 2 S.C.R. 403.
[137] Privacy Act Canada 1983.

but this decision was reversed on appeal.

The appeal was upheld and the court found that the purpose of the Privacy Act is to protect the privacy of individuals with respect to personal information about themselves held by a government institution and to provide individuals access to that information. The court stated that the employees of the respondent had a reasonable expectation that the information in the sign-in logs would not be revealed to the general public.

The information requested revealed the following personal details: the times during which employees attended their workplace on weekends over a period of one month. A reasonable person would not expect strangers to have access to detailed, systematic knowledge of an individual's location during non-working hours, even if that location is his or her work place. The Court found that the request did not only include personal information such as the name of an individual, but also disclosed other personal information such as times of their arrival and departures.

Information obtained from the sign-in logs kept by the security personnel at the place of employment, reveal intimate details of the lifestyle and personal choices of an individual. The information related to facts, which could give the details of: the name, identity number, signature (the identity), the location of an individual, time of arrival and departure from a certain location. If it revealed personal details, in which a reasonable expectation of privacy exists, it should not be released without consent or prior judicial authorization.

Once an individual has established a reasonable expectation of privacy in certain information; the inquiry must then proceed to determine whether the search [divulging of information] was conducted in a reasonable manner.[138] To determine whether the search was reasonable will depend if it was necessary to obtain prior judicial authorization.

[138] *R v Edwards* [1996] 1 SCR 126; *Hunter v Southam* [1984] 2 SCR 145.

5.2.4. Prior Judicial Authorization

The purpose of prior judicial authorization was stipulated in *Hunter v Southam*[139], which reads:

> "The purpose of a requirement of prior authorization is to provide an opportunity, before the event, for the conflicting interests of the state and the individual be assessed, so that the individual's right to privacy will be breached only where the appropriate standard has been met, and the interests of the state are thus demonstrably superior. For such an authorization procedure to be meaningful it is necessary for the person authorizing the search to be able to assess the evidence as to whether that standard has been met, in an entirely neutral and impartial manner."

It was stated that it is preferable to have a system of prior authorization to prevent unjustified searches before they happen rather than having a system of subsequent validation. If prior judicial authorization is required, what evidence must be available before authorization is granted or what should the requirements be before an order to this effect is made?

In *Hunter v Southam*[140] it was stated that reasonable and probable grounds, established under oath, to believe that an offence has been committed and that there is evidence to be found at a place of the search, constitutes – the minimum standard, consistent with section. 8 for authority for search and seizure.

It was held in *Plant*[141] that the search must be brought within the parameters of section. 8, to require prior judicial authorization. It was held that the accessing of the information from the electricity records did not involve an intrusion into places ordinarily considered private and not of a personal and confidential nature. The manner and place of search indicated a minimal intrusion the seriousness of the offence outweighed the privacy interest claimed by the appellant. In *Plant* it was stated that the appellant did not have a

[139] *Hunter v Southam* [1984] 2 SCR. 145.
[140] *Hunter v Southam* supra.
[141] *Plant* supra

reasonable expectation of privacy in relation to computerized records, which outweighed the interest of the state in enforcing the laws relating to narcotic offences. The Court came to the conclusion that the appellant had no reasonable expectation of privacy with respect to computerized electricity records and therefore it was necessary to obtain prior judicial authorization.

The Court however stated in In *R v Wise* [142] that the surreptitious electronic tracking of one's movement is a grave threat to individual privacy. Therefore to track ones movements prior judicial authorization should be required. The issue of a prior judicial authorization will call for an objective showing of reasonable and probable cause and this should be generally be required of those seeking to employ electronic devices in the pursuit of individuals.

5.3. Conclusion

In America, the right to privacy has developed in relation to search and seizures. Before a warrant will be authorized a person must have a reasonable expectation of privacy. Case law has developed based on the Fourth Amendment reasonable expectation of privacy. In the matter of *Katz* a two-requirement test developed. Firstly an individual must have a subjective expectation of privacy in the object of the search. Secondly society must be willing to recognize that this subjective expectation is reasonable.

This expectation must be regarded by society as reasonable to qualify for protection under the Fourth Amendment. An objective criterion is build into the test.

Voluntarily conveyed information to institutions such as bank or telephone companies as in the cases of *Smith v Maryland* and *United States v Miller* seems not to receive protection because it was voluntarily conveyed and disclosed to a wide area of people. If information forms part of commercial records the protection thereof is diminished. American jurisprudence does not seem to provide answers to the questions posed in this thesis. An exclusion of the reasonable expectation of privacy seemed to have developed

[142] *Wise* supra.

in *Smith* and *Miller's* cases. Because of the fact that voluntarily conveyed information and information in a commercial context do not receive protection under the right to privacy, it is submitted that the United States Supreme Court will in all probability not afford protection to the non-communicative cell phone information.

The Canadian case of, *R v Plant* stands out as setting the standard of what type of information should be regarded as personal and confidential and revealing intimate details of the life of an accused. Here the electricity consumption was regarded as not being information of a personal nature as it did not reveal intimate details of the accused.

In *R v Wise* the court stated a right to privacy in movement could exist. In the case of *Dagg* it was found that where you are at a specific time and place, your location is of a personal nature and that you have a reasonable expectation of privacy in this type of information. The fact that you are at you workplace outside normal working hours does not diminish your right to privacy in your location.

Compared to the United States of America, Canada goes further in protecting information. It is submitted that the views of the majority as well as the minority of the Court in *Plant* can be used as assistance in an argument that non-communicative cell phone information revealed details of the personal and private decisions of users. Similarly the decision in *Dagg* confirms that movement and location can receive constitutional protection.

In the final chapter the principles from international law, the United States and Canada will be set out and then applied to the issue at hand. I will attempt to argue that as a result of the investigation made herein that non-communicative information obtained from cell phone records should receive protection under the right to privacy.

CHAPTER 6 CONCLUSION

This issue in this thesis is whether the divulging of this non- communicative information, such as the location and movement of cell phone users, by cell phone companies is an intrusion on an individual's right to privacy? If so, should this intrusion of the right to privacy be regulated? To answer these questions reference will briefly be made to international law, the jurisprudence of the United States of America and of Canada. Then the principles extracted will be applied to information obtained from cell phone records.

6.1. Principles from International law

Article 12 of the Universal Declaration of Human Rights set a benchmark regarding the international recognition of the right to privacy. The basic content of this right is that no one should interfere with an individuals privacy, that of his family, his home or correspondence. A broader interpretation to include place of employment is also suggested. Should interferences take place it must be lawful in terms of domestic laws and not arbitrary. The interference should in any event be reasonable in the circumstances.

The wording of the right to privacy in various other international instruments such as the ICCPR, UN Convention on Migrant Workers, and the UN Convention on the Protection of the Child is based on UDHR and almost identical to it. Everyone has a right to privacy and this fundamental right is of such great importance that no one may be arbitrarily, unlawfully be deprived of this right. It is submitted that this protection can similarly be extended to cell phone users that their right to privacy should not be interfered with.

The European Court of Human Rights held that telephone conversations, the record and details of telephone numbers dialed on a particular phone are included in the notions of "private life" and "correspondence. Telephone taping was held to be a violation of the privacy rights, guaranteed under Article 8 and the right to privacy was also extended to every the user of a telephone and limited to the owner of the article. Law offices were

also included to fall within the protected sphere of privacy.

A number of regional instruments contain various guidelines encouraging organisations to process the recording of personal data in a responsible, fair and privacy-friendly manner. Principles contained in the United Nations Guidelines on data processing, The Coe convention, OECD guidelines and in the EU directive are in content very similar. There is an assumption in all these regional instruments that personal information is indeed worthy of protection and that the recording thereof and access thereto should be properly regulated. It is submitted that information obtained from cell phones is included in the type of information that warrants protection as envisaged in these instruments.

6.2. Principles from United States of America and Canada

In the United States the protection of privacy rights applicable to this thesis is found in the Fourth Amendment of the United States' Constitution. No searches are permitted unless a warrant is obtained. If an individual seeks the protection under the right to privacy a reasonable expectation of privacy must be manifested in the object of the search. Society must be able to determine objectively that the subjective expectation is reasonable. It seems that voluntarily conveyed information and information, which are disclosed in a commercial context, would not receive protection under the right to privacy. Cell phone users will have to prove that a right to privacy exists in information obtained from cell phone records. It has to be proved that a reasonable expectation exist in the type of information revealed by cell phone records. It must be proved that a user has a reasonable expectation of privacy in movements and location.

A two-stage approach regarding the reasonable expectation of privacy is also applied in Canada. Firstly an individual must have a reasonable expectation of privacy and then there must be an objective determination to ascertain if the expectation was indeed reasonable. Information to be protected must be of such a nature that it reveals intimate details of the personal decisions and choices of an individual. The time that a person frequent his/her place of employment, even after hours was regarded as being private.

6.3. The nature of non-communicative cell phone information

To ascertain if protection will be afforded to certain information[143] will depend on the nature of the information. According to Steytler,[144] the question that needs to be answered is: "Should it (the information) be worthy of protection?" The right to privacy should be confined to a biographical core of personal information, which may reveal intimate details of an individual's lifestyle and personal choices.

It must first be determined if information of users obtained from the cell phone records is worthy of protection. To be worthy of protection it will have to be determined if this information can be regarded as revealing intimate details of the lifestyle and personal choices of an individual.Can one say that cell phone users have a reasonable expectation of privacy in the non-communicative information such as movement and location? The first question is if the nature of the information is such that it is worthy of being protected and if it is of a "personal and confidential" nature. The information must be such that it tends to reveal intimate details of the lifestyles and personal choices of the individual[145].

The following information can be extracted from the records of cell phone users. The time that a call was made, the duration of the call, the precise geographical area of the person making the call (the caller) and the precise geographical area of the person to whom the call was made (the recipient). If the details of a number of calls made by a user during a specific period are monitored, the movement of the individual can be tracked for that specific period.

Can it be said that the abovementioned details are personal; does it reveal intimate details about the decisions and personal choices of an individual? It is submitted that it is indeed the case. Put differently by looking at the non-communicative information certain inferences can be drawn and certain deductions can be made which will reveal the personal decisions and choices of individuals. On the face of it the information does not

[143] See *Protea Technology Ltd v Wainer* 1997 (9) BCLR 1225 (W) at 604 definition of confidential information "... expression must surely mean such information as the communicator does not intend to disclose to any other person other than the person to whom he is speaking..."
[144] Steytler N C *Constitutional Criminal Procedure* 104.

reveal anything about the political opinion, sexual preference of an individual. However inferences can be drawn by looking at the location such as a bar, shebeen, sports arena, club, church any other place of entertainment or worship that is frequented by the individual. The nature of the information is such that much more is revealed than dialed telephone numbers[146] which receive protection under article 8 and also goes further that the furnishing of a cell phone number without a user's consent.[147]

It is submitted that if the criteria in *Plant's* case is applied to the non-communicative cell phone information, the information will be regarded as being personal and revealing the personal choices and decisions of an individual. Determining where and when someone visited a certain dwelling/establishment can ascertain the political, religious and sexual orientation and preferences of that person. Inferences can indeed be drawn that an individual made certain personal and private decisions by only looking at the cell phone records as opposed to looking at the records of electricity consumption.[148]

The non-communicative information was not created in the context of a commercial transaction. The numbers dialed and especially the duration of calls gets collected in order for the cell phone companies to furnish users with an account. It is however not necessary to have details of location and movement to account to clients. These details are only incidentally being captured because of the manner in which various cell phones communicate via cell phone towers when a call is made. It is not information that exclusively belong the cell phone companies.

The information of the movement and location of users are not created for accounting purposes. In fact the company for everyday use does not require it. The information about the location and movement is not required by companies to furnish users with accounts. Only cell phone subscribers who enter into cell phone contracts receive accounts. Prepaid

[145] *Plant* supra.
[146] *Malone v United Kingdom* 2 August 1984 Series A no 82.
[147] *Simons v P4 Radio* [2003] JOL 10745 BCCSA.
[148] *Plant* supra.

cell phone users do not even receive accounts from companies. It cannot be said that the information forms part of the commercial records of cell phone companies.[149]

The nature of the relationship between the cell phone user and the company can be characterized as a relationship of confidence. The records the duration of calls and numbers dialed are being kept as part of an ongoing commercial relationship and cell phone companies are obliged to keep the records of their contract subscribers confidential. This is however not the case of prepaid customers who do not enter into contracts with the cell phone companies. It is not generally possible for an individual to inquire about the cell phone accounts/records of other users and the information is not subject to inspection by members of the public at large.

The place and manner in which information is retrieved by law enforcement officials also indicates that cell phone users have a reasonable expectation of privacy in respect of the cell phone records The police are only able to obtain the information in terms of prior judicial authorization in terms of a s 205 subpoena in terms of the Criminal Procedure Act.[150] An individual does have a reasonable expectation that the information in possession of the cell phone companies would be kept in confidence and restricted to the purpose for which it is given.

6.3.1. Is the information voluntarily conveyed?

It was held that if information about an individual is being voluntarily conveyed to third parties, the individual has no reasonable expectation of privacy in the information.[151] It is submitted that the information regarding the movement and location of cell phone users is not voluntarily conveyed to the cell phone companies. It is debatable whether some users are even aware that they are transmitting details about their movement and location whilst communicating over a cell phone. It is a contentious issue that the cell phone companies have access to this type of non-communicative information, probably without

[149] *United States v Miller*, 425 U.S. 435 (1976).
[150] Act 51 of 1977.
[151] *Smith v Maryland* 442 U. S 735 (1979).

the knowledge and consent of the users. However, it is outside the scope of this research to embark on an analysis if the obtaining and recording of information is validly done. It is accepted for purpose of this research that the cell phone information has been validly obtained. For cell phone information to be regarded as being voluntarily conveyed, will mean that every cell phone user must be aware that these details are recorded.

It s submitted that cell phone users do have a reasonable expectation of privacy in their movement and location. The objective element in this inquiry will be satisfied in that society will be willing to regard this expectation as being reasonable.[152] If it is accepted that prisoners[153], persons in police custody, arrested persons, or those who are lawfully detained have a limited expectation of privacy in their movements, the same cannot be said of cell phone users. It is argued that everyone else including cell phone users indeed do have a right to privacy in movement. The right to privacy should protect information about the movement[154] and location[155] of cell phone users.

The fact that a person has a reasonable expectation in his arrival and departure from a certain location even if that location is the place of employment[156], the movement of arrival and departure of location ascertained from cell phone records should also be protected.

The nature of information obtained from cell phone records reflecting the location and movement of users is such that it should receive protection in terms of the right to privacy. Similarly information about the location of cell phone users should not be divulged without the consent of users or without obtaining prior judicial authorization.

6.4. How should this intrusion of the right to privacy be regulated?

The content of an individual's telecommunications is private and confidential. The state

[152] The two-requirement test referred to in *Katz v United States* 389 U S 347, 353 (1967) *Kyllo v United States* 533 U.S. 27 (2001) 190 F 3d 1041.
[153] *R v Dorfer* (1996) 104 CC (3d) 528 (BCCA).
[154] *R v Wise* [1992] 1 S.C.R. 527.
[155] *Dagg v Canada (Minster of Finance)* [1997] 2 S.C.R. 403.
[156] *Dagg* case supra.

will only be able to access the content of telecommunications with prior judicial authorization.[157] If it is accepted that a right to privacy exist in the non-communicative information the question that needs to be addressed is; how should the interference with the right to privacy in information be regulated?

International law prescribed that there should not be any unlawful interference with the privacy of individuals. Interferences are only allowed if it is not arbitrarily and unlawfully. Should interferences take place it must be lawful in terms of domestic laws and not arbitrary. The interference should in any event be reasonable in the circumstances. If legislation is enacted which allows interference it must specify in detail the precise circumstances in which such interferences will be permitted.[158]

Although in the *Petersen* case the police obtained authorization to obtain the cell phone records, the question is whether the accused was entitled to the protection of the information regarding their movements. Put differently, could the police have obtained the information from the cell phone companies when there was not enough evidence to obtain a section 205 warrant?

For instance if the police have established the time of death at a particular place- could they trawl through cell phone records for persons who may have been there at a certain place and at a certain time to establish a suspicion? Should they look at records of everyone at the scene of the crime to enable them to round up suspects? At what stage should police be allowed to have access to this type of information? As earlier illustrated in the *Petersen* case access to this type of information can assist in the prevention and solving of crime.

It is submitted that there should at least be a suspicion from the police's side before prior judicial authorization in the form of a subpoena will be issued. They should not be allowed to access to the records in order to form a suspicion. This is not the purpose of

[157] Section 40 RICPCRI Act.
[158] Steytler page 80.

prior judicial authorization. The purpose of prior judicial authorization as stipulated in *Hunter v Southam*[159] can be summarized as follows: To provide an opportunity for the conflicting interests of the state and the individual to be assessed. An individual's right to privacy will only be breached if an appropriate standard has been met and where the interests of the state are superior. The assessment of the evidence must be done in an entirely neutral and impartial manner.

It was stated that it is preferable to have a system of prior authorization to prevent unjustified searches before they happen rather than having a system of subsequent validation[160]. If prior judicial authorization is required, certain evidence must be available before authorization is granted or there should be requirements before an order to this effect is made.

In *Hunter v Southam*[161] it was stated that reasonable and probable grounds, established under oath, to believe that an offence has been committed and that there is evidence to be found at a place of the search, constitutes the minimum standard, consistent with section 8 for authority for search and seizure. The search must be brought within the parameters of section8 to require prior judicial authorization. It was held that the accessing of the information from the electricity records did not involve an intrusion into places ordinarily considered private and not of a personal and confidential nature.[162] The manner and place of search indicated a minimal intrusion the seriousness of the offence outweighed the privacy interest claimed by the appellant.

The issue in *Plant*[163] can be distinguished from the issue regarding cell phone information. It was stated that the appellant could not be said to have a reasonable expectation of privacy in relation to computerized records, which outweighed the interests of the state in enforcing the laws relating to narcotic offences. The Court came

[159] See chapter 5 for discussion.
[160] *R v Wise* supra.
[161] [1984] 2 SCR 145.
[162] *R v Plant* the computer records revealing the pattern of consumption in a residence was said not to reveal intimate details of the appellant's life – since electricity consumption reveals very little about he personal lifestyle or private decisions of the occupants of the residence.

to the conclusion that the appellant had no reasonable expectation of privacy with respect to computerized electricity records and therefore it was not necessary to obtain prior judicial authorization. It is submitted that if the same principles in *Plant* is applied to cell phones, it will be found that a reasonable expectation in privacy exist in the non-communicative cell phone information. The details such as the location and movement of users are indicative of the personal choices and lifestyle of users which necessitates prior judicial authorization.

6.5. Application of principle

If the access of information in possession of third parties generally is not properly regulated by legislation, anonymity of users will be lost. Information obtained from a customer's personal bank records reflecting withdrawal dates, times and locations from ATM machines, as well as credit cards purchases will also provide details of an individual's whereabouts and movements. Technology increases at an alarming pace and in future third parties could be in possession and have access to information containing biometrics features such as (fingerprints, palmprints, voice and eyescan DNA features)[164]. If all these information is in possession of third parties and not properly regulated, it will effectively take away an individual's right to determine what information others should know about the individual.

6.6. Conclusion

In conclusion it is submitted that the nature and extent of non-communicative information and details obtained from the cell phone records such as location and movement of users is worthy of being protected by the right to privacy. It does disclose details about the personal lifestyle and choices of individuals. Because a reasonable expectation of privacy exists in this type of information, access thereto should be properly regulated. The records should not be trawled in order to form a suspicion. A suspicion should have been present before an application is made to obtain any form of prior judicial authorization.

---

[163] *Plant* supra.
[164] Van Tonder K "Biometrics Identifiers and Privacy" *De Rebus* August 2003 at 19.

BIBLIOGRAPHY

BOOKS

Chaskalson, M, Kentridge J, Klaaren, J, Marcus, G, Spits, D & Woolman, S (reds) *Constitutional Law of South Africa* 2 ed Juta Kenwyn: 2002.

De Waal, J, Currie, I, Erasmus, G *The Bill of Rights Handbook* Juta Kenwyn: 2001.

Neethling, J, *Die Reg op Privaatheid*, Doctoral Thesis Unisa, 1976.

Neethling, J, Potgieter, JM, Visser, PJ *Law of Delict* Butterworths Durban 4th ed: 2001.

Neethling, J, *Persoonlikheidsreg* Butterworths Durban: 1998.

Steytler, N C, *Constitutional Criminal Procedure* Butterworths Durban: 1998.

ARTICLES

Gormley K, "One Hundred Years of Privacy" 1992 *Wisconsin Law Review* 1335.

Van Tonder K "Biometrics Identifiers and Privacy" *De Rebus* 2003 August 19.

Warren and Brandeis "The Right to Privacy" (1890) 4 *HLR* 193.

WEBSITE ADDRESSES / INTERNET SOURCES

www.oxfordreference.com.

www.electronics.howstuffworks.com

www.nashuamobile.co.za

www.suntimes.co.za

www.mnet.co.za

www.pmg.org.za

www.law.wits.ac.za

www.cdt.org.

www.sahr.org.za

www.privacy.org

www.oecd.org

www.hrweb.org

www.sahr.org.za.

www.migrantrsrights.org

www.unicef.org/crc/fulltext.htm

TABLE OF CASES

SOUTH AFRICA

Bernstein v Bester 1996 (2) SA 751 (CC) 789.

Case v Minister of Safety and Security 1996 93) SA 165 (CC).

Epstein v Epstein 1906 TH 87.

Ferreira v Levin No and Others; Vryenhoek and Others v Powel No and Others 1996 (1) SA 984(CC).

Investigating Directorate: Serious Economic Offenses and Others v Hyundai Motor Distributors Pty Ltd and Others; in re Hyundai Motor Distributors Pty Ltd and Other v Smit No and Others 2000 (10) BCLR 1079 (CC).

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

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

*National Coalition for the Gay and Lesbian Equality v the Minster of Justice*1999 (1) SA 6 (CC).

National Media Ltd. AO v Jooste 1996 (3) SA 262 (A).

O'Keefe v Argus Printing and Publishing Co Ltd 1954 (3) S A 244 (C).

Protea Technology Ltd v Wainer [1997] 3 ALL SA 594 (W).

Protea Technology v Wainer 1997 (9) BCLR 1225 (W).

R v Holiday 1927 CPD 395.

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

S v Mboniswa [2003] JOL 11011 (C).

S v Naidoo 1998 (1) BCLR 46 (D).

S v Nkabinde 1998 (8) BCLR 996 (N).

S v Petersen and Another unreported case Cape High Court Case no: SS 95/98.

Simons v P4 Radio [2003] JOL 10745 BCCSA.

EUROPE

Klass v Germany 6 September series a no 28 at 41.

Kruslin v France 24 April 1990 Series A no 176-a.

M.S. v Sweden (74/1996/693/885) 27 August 1997.

Malone v United Kingdom 2 August 1984 Series A no 82.

Niemits v Germany 16 December 1992 Series A no 251 B.

UNITED STATES OF AMERICA

Goldman v United States, 316 U S.129 (1942).

Griswold v Connecticut 381 U.S. 479 (1965).

Katz v United States 389 U S 347, 353 (1967).

Kyllo v United States 533U.S. 27 (2001) 190 F 3d 1041.

Lee v United States 343 U.S. 747 (1952).

Olmstead v United States 277 U S 438 (1928).

Roe v Wade 416 U.S. 113 (1973).

Silverman v United States 365 U.S 505(1961).

Smith v Maryland 442 U. S 735 (1979).

Terry v Ohio 392 U.S. 1, 9 (1968).

United States v Gomez, 16 f.3d 254 (8the cir 1994).

United States v Miller, 425 U.S. 435 (1976).

CANADA

British Columbia Securities Commission v Branch (1995) 97 CCC (3d) 565 (SCC).

Dagg v Canada (Minister of Finance) [1997] 2 S CR 403.

Hunter v Southam [1984] 2 S.C.R. 145.

R v Dorfer (1996) 104 CC (3d) 528 (BCCA).

R v Dyment [1988] 2 S.C.R 417.

R v Edwards [1996] 1 S.C.R. 128.

R v McKinley [1990] 1 S.C.R. 627 645.

R v Plant [1993] 3 S.C.R. 281.

R v Wise [1992] 1 S.C.R. 527.

Thompson Newspaper Ltd, v Canada (1990) 67 DLR (4th) 161 (SCC).

CONVENTIONS, DIRECTIVES GUIDELINES, ISSUE PAPERS

1. American Convention of Human Rights 1969.
2. Convention For the Protection of Individuals with Regard to the Automatic Processing of Personal Data. 1981 (CoE Convention).
3. Conventions for the Protection of Human Rights and Fundamental Freedoms, 1950.
4. European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data (EU directive).
5. International Covenant on Civil and Political Rights (ICCPR) (1966).
6. Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD guidelines).
7. South African Law Reform Commission Issue Paper on Privacy and Data Protection Issue Paper 24 Project 124.
8. United Nations Convention on Migrant Workers 1990.
9. United Nations Convention on Protection of the Child 1989.
10. United Nations Guidelines Concerning Computerized Data files, 14 December 1990.
11. Universal Declaration of Human Rights (UDHR) 1948.