Hamman, Abraham (2010). Nowhere to Hide – Big Brother is Watching You: Non-communicative Personal Cellphone Information and the Right to Privacy. Speculum Juris, 24(1): 70 – 95.

Nowhere to hide- big brother is watching you: non–communicative personal cellphone information and the right to privacy

Abraham Hamman
Lecturer
BA., LL.B., LL.M.
Lecturer
University of the Western Cape.

"It's impossible to move, to live, to operate at any level without leaving traces, bits, seemingly meaningless fragments of personal information." William Gibson

1 Introduction

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

This information is not ordinarily available to the police and it usually requires prior judicial authorisation to access this information. The problem is, that the cellphone 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. The Protection of Personal Information Bill[1] suggests new methods of operating with regard to the collection and/or dissemination of any personal information and aims to protect individual's right to data privacy and protection of personal information. If an individual has a right to privacy in his movement and location is not addressed by the Bill. This bill must, however still be passed by Parliament.

On the other hand, this type of information, if utilised by the police services, can play a crucial role in solving crime, and the use thereof should be encouraged to solve crimes, provided that the proper legal authorisation is obtained. Are the nature and extent of non-communicative information, and details obtained from cellphone records, such as, the location and movement of users, worthy of being protected by the right to privacy?
The right to privacy has been included in the South African Constitution[2] as a fundamental right and enjoys both common law and constitutional protection. Neethling has formulated the following definition:

"Privacy is an individual condition of life of separation from publicity. This condition of

[1] The Protection of Personal Information Bill [B9-2009] was tabled in Parliament on 25 August 2009. Available at: http://www.pmg.org.za/bill/20090825-protection-personal-information-bill-b9-2009. Accessed 14 April 2010.
[2] Section 14 of The Constitution of the Republic of South Africa, Act 108 of 1996 (the Constitution).

life em-braces 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."[3]

This definition has been accepted by both the Appellate Division[4] and the Constitutional Court[5], and will constitute the basis of the discussion of the right to privacy in this article.

The right to privacy includes the right to have control over personal information, and the right to be able to conduct personal affairs relatively free from unwanted intrusions.[6] It has usually been interpreted to include telecommunications and the contents thereof, which the state will be able to access only with prior judicial authorisation.[7]

It could be assumed that the same rule would apply also to the content of communications via cellphone. However, cellphone technology has spawned an industry-wide practice of cellphone companies recording and storing non-communicative information about users and usage. It is seldom realised what details are left in the wake of one single call. Personal information, such as, the number dialled, the time and duration of the call, the location of both the caller and the recipient, are routinely recorded in respect of each and every call made by all phones.[8]

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.

This information is not ordinarily available to the police and they do not have unlimited and unrestricted access to it. However, the police would be able to obtain access with prior judicial authorisation in the form of a subpoena issued by a court.[9] In addition, the cellphone companies themselves, their employees, computer hackers, and possibly even criminals, can have access to this information. The potential for abuse is enormous.

The key issue with regard to cellphones is whether the keeping and use of this non-communicative information by cellphone companies are intrusions on an individual's right to privacy. Does the right to privacy protect non-communicative personal information obtained from cellphone records?

---

[3] Neethling, *Die Reg op Privaatheid*, Doctoral Thesis Unisa, (1976) 287. Neethling, Potgieter, Visser *Law of Delict* 4 ed, (2001) 355.
[4] *National Media Ltd v Jooste* 1996 (3) SA 262 (A) 271.
[5] *Bernstein v Bester* 1996 (2) SA 751 (CC) para 68.
[6] Neethling, *Persoonlikheidsreg*, Butterworths 39 and *National Media Ltd v Jooste* 1996 (3) SA 262 271 –2. It gives a person the right to control what others know about him or her. 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 one. It also includes the right to make certain personal choices regarding sexual relations.
[7] Section 40 Regulation of Interception of Communications and Provision of Communication Related Information Act. No 70 of 2002 (RICA).
[8] 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 of the call 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 uses a cell phone on a specific day 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. Hamman A J, *The right to privacy and the challenge of modern cell phone* technology. Unpublished Master's Thesis UWC, (2004) 287.
[9] Subpoena usually issued in terms of Section 205 Criminal Procedure Act 51 of 1977. This would seem to be a justifiable infringement of the right to privacy in terms of section 36 of the Constitution.

Cellphone technology has been, and definitely will be, utilised by law enforcement agencies in order to combat crime.[10] The challenge is to protect citizens' privacy in this process.

2 Privacy under the common law

Before the entrenchment of the right to privacy in the Constitution it was recognised by the common law as an important right, which warrants protection.[11]

The following examples are breaches of privacy recognised 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.[12]

The common law right to privacy has also been deemed violated where a person's photograph is published as part of an advertisement without the consent of the person;[13] by a doctor informing third parties that his patient had HIV;[14] by the wire-tapping or 'bugging' of private premises;[15] and by peeping at a woman while she is undressing.16 [16] 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 also apply to non – communicative personal information which is obtained from cellphone records. The common law does not provide an answer to 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 was regarded as an infringement of

---

[10] In *S v Petersen* unreported case heard in the Cape High Court Case No. SS 95/98 advanced cell phone technology was utilised by the prosecution. The detailed billing records were obtained from 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 to make use of advanced cell phone technology.
The court found that the State had proved, with extracts from the cell phone records, that 12 calls had been made from one specific cell phone to another during a period of 52 minutes between 01:20 and 2: 12.It was also found that the calls were made according to the route that was mapped out by using the cell phone records. Cell phone records indicated precisely the area where calls were made from and the location of the recipient. An expert was able to plot all the detail on a map to indicate with precision where the user was when calls were made. Without the cell phone records used in this case there was no direct evidence against the accused, as there were no eyewitnesses.
The two accused were linked to the crime by means of cell phone technology with extreme accuracy by compiling a route map using the cell phone records. The irrefutable evidence of the mapped cell phone records destroyed the alibis ventured by the two accused.
Other information obtained from Sunday Times 26 September 1999 available at www.suntimes.co.za/1999/09/26/insight/in01.html and www.mnet.co.za/CarteBlanche/Display/Display.asp?Id=1637
In *S v Moodley* detectives used cell phone records to identify the perpetrator. Subpoenas were issued to the various cell phone companies to provide a database of all phone calls made from near the spot where Leigh Mathews had been murdered. The accused had made a mistake by phoning his girlfriend from near the bloody spot where the murder had taken place. The cell phone records indicated that he made one call on his phone within one minute after the ransom demand call was made on Matthews' phone to her father. Sunday times 31 July 2005 page 1 & 3.

[11] De Waal, Currie, Erasmus *The Bill of Rights Handbook* (2001) 268. 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'. 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).

[12] Mentioned by Ackerman J in *Bernstein v Bester* para 69.

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

[14] *Jansen Van Vuuren v Kruger* 1993 (4) SA 842 (A).

[15] *S v A* 1971 (2) SA 293 (T).

[16] *R v Holiday* 1927 CPD 395.

that right.[17]

3 The constitutional right to privacy

3 1 Section 14

Section 14 of the Constitution 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."[18]

The section consists of two parts.[19] The first part guarantees a general right to privacy and the second part protects against specific infringements of privacy. A right of privacy to information in possession of a third party (e.g. a cellphone company's information in its possession about an individual's movement and location) would probably fall under the first part. As a fundamental right it can be limited in accordance with the limitation clause, that is, by a law of general application.[20]

An assessment of an invasion of privacy in terms of the Constitution differs from a common law assessment. The common law operates in terms of a single enquiry: it must be determined that the invasion is unlawful and that there are no grounds of justification present.[21]Ackerman J in *Bernstein* held that the Constitutional Court should guard against applying the common law principles to interpret fundamental rights.[22] In terms of the Constitution it is not a single enquiry but a two-stage analysis:

1. The party who seeks to exclude certain evidence should first establish the scope of the right to determine whether certain conduct has infringed that right. An individual will have to prove that he/she has a subjective expectation of privacy and that society has recognised that expectation as being reasonable.
2. If an infringement occurred, or there has been an invasion of the right to privacy, it must be determined whether it was a legitimate limitation to allow the information to be admissible as evidence.[23]

The limitation of the right to privacy is a separate inquiry. If an infringement of a right has taken place, it must be determined whether such infringement was justifiable in terms of the Constitution.[24] If the infringement was not justifiable, the aggrieved party must

[17] *Epstein v Epstein* 1906 TH 87.
[18] The Constitution.
[19] De Waal, Currie, Erasmus 267.
[20] Neethling, Potgieter Visser 19.
[21] De Waal, Currie, Erasmus 269.
[22] *Bernstein* para 71.
[23] *Bernstein* para 90.
[24] 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

have certain remedies against those who infringed the right.

Right to privacy cases that have come before the Constitutional Court may be classified into two broad categories: inner core privacy and business privacy. In *NM and Others v Smith and Others CCT 69/05* it was held that the right to privacy protects citizens from the publication of private medical information without their consent.[25]

3 2 The inner core/ inner sanctum

The inner core/inner sanctum of the privacy of an individual is the most sacred private area of a person's life. The strongest protection will be afforded to that which constitutes the "inner core" of privacy or what takes place in the "inner sanctum" of an individual. The "inner core" of privacy was referred to in *Case v Minister of Safety and Security* as that which is done in the privacy of an individual's home and what type of erotic material is kept in the privacy of a home.[26] A person's family life, sexual relationships, sexual preferences and home environment form part of this inner core, which will be protected by the right to privacy.[27] But as a person moves into communal relations and activities, such as, business and social interaction, the scope of protected personal space shrinks accordingly.[28] The right to privacy, thus, will be reduced the further the individual moves away from this inner core.

3 3 Business

The privacy in the business of an individual is what takes place in the business life of an individual. In *Hyundai*,[29] the Constitutional Court qualified the "inner core" principle. Inthis case search warrants were authorised, which allowed 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 was seized. The Court held, per Langa DP, that persons continued to retain a right to privacy in the social capacities in which they acted. The Court stated that:

"The right [to privacy], however, does not relate solely to the individual within his or her intimate 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

---

(d) the relation between the limitation and its purpose; and less restrictive means to achieve the purpose

[25] *NM and Others v Smith and Others CCT 69/05.* The names and HIV status published in a book without the individual's consent was held to violate the privacy rights and dignitas of the person.

[26] *Case v Minister of Safety and Security* 1996 (3) SA 165 (CC).

[27] *Case v Minister of Safety and Security.* Stated 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. The offence of possession of obscene photographic matter, in contravention of section 2(1) of the Indecent or Obscene Photographic Materials Act 37 of 1967 was declared to be inconsistent with the Constitution and invalid. The Court held that the offence infringed the right to privacy of individuals and that there was no justification for this infringement. Didcott J held para 91:

> "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 which section 13 of the Interim Constitution… guarantees that I shall enjoy."

It was 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.*1999 (1) SA 6 (CC). What an individual decides regarding his family life, sexual preference and sexual relationships is regarded as being personal and he/she must be left alone regarding the decision.

[28] *Bernstein* para 67.

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"[30]

Even if there is a move away from the inner core, protection will still be afforded to an individual.

The more public the undertaking, and the more closely it is regulated, the more attenuated the right to privacy would be, and the less likely any possible invasion.[31] Although privacy rights can exist in a business, the more public the manner in which a business is being regulated, the possibility of an invasion of privacy will be reduced. The right to privacy will also be extended to personal space at places of employment and business.
In *Mistry*[32] it was held that the entering, searching and seizing in terms of the Medicines and Related Substances Control Act 101 of 1965 was an unjustifiable breach of the right to privacy.

3 4 Information and communications
It has been established that the right to privacy protects the content of telephone conversations. In *Protea Technology v Wainer* it was held that where an employee makes and receives calls that have nothing to do with his or her employer's business, a legitimate expectation of privacy exists in respect of the content of such calls.[33]

False and misleading information furnished by the police to obtain a direction to tap cell phones in *S v Naidoo,* resulted in the direction being declared invalid, and the monitoring of the cellphone conversations an unjustifiable violation of the right to privacy.[34] In *S v Nkabinde* the monitored conversations between an accused and his legal representative were also held to be an invasion of the right to privacy of the accused.[35] These cases, however, only relate to the content of telecommunications, they do not address the issue whether the protection of privacy will extend to non-communicative information, such as, movement and location, obtained from cellphone records. The divulging of private medical information without consent was regarded as an infringement of the right to privacy in *the NM and Others case*.[36]

From the above it is apparent that no authority exists in South African law that the right to privacy protects non-communicative personal information, such as, the movement and location of cellphone users.

It is submitted that privacy about a person's location and movement is not part of their

---

[29] Investigating Directorate: Serious Economic Offences 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) BCLR1079 (CC).
[30] *Hyundai* para 16.
[31] *Hyundai* para 27.
[32] *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127(CC).
[33] *Protea Technology v Wainer* 1997 (9) BCLR 1225 (W).
[34] *S v Naidoo* 1998 (1) BCLR 46 (D).
[35] *S v Nkabinde* 1998 (8) BCLR 996 (N).
[36] *NM and Others v Smith and Others CCT 69/05.* The names and HIV status published in a book without the individual's consent was held to violate the privacy rights and dignitas of the person.

"inner core". In *Simons v P4 Radio*[37], a matter heard by 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 this 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 had not said anything on air which necessitated the serious invasion of his privacy. The Tribunal held that it was hard to imagine a set of facts (short of an emergency) which would allow the divulging of a cellphone number without the permission of the person involved.[38] Such conduct was regarded as a very serious invasion of privacy.

The Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA)[39] also gives protection to communications when it states that a court order must be obtained to get access to the content of conversations.[40] But many third parties hold information (e.g. about the movement and location of cellphone users) and about persons (clients). The question that needs to be addressed is:
Does the right to privacy protect this information?

RICA was enacted to regulate the interception of certain communications and replaced previous legislation (e.g. Interception and Monitoring Prohibition Act 127 of 1992) dealing with this. It also places many more responsibilities on cellphone owners and cellphone companies, which attempt to eradicate the theft of, and trade in, stolen cellphones by compiling a data base of the identity of all cell phone users.

Once the database 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 cellphone user will be traceable. It will also be possible to locate a person using a cellphone within a range of a few metres.

Although, subject to certain exceptions, it is an offence to provide real-time or archived information to any person other than the customer,[41] RICA does not state that the right to privacy protects information regarding the non-communicative information (movement and location) of cellphone users. In fact, this Act stipulates that more information regarding cellphone users should be kept in databases by cellphone companies. The fact that the details of movement and location of users can be ascertained by looking at the records presents the possibility that rights of individuals will be infringed, without them even realising that these details can be accessed. Moreover, RICA has the result that even more information in respect of cell phone users will be in possession of third parties.

---

[37] *Simons v P4 Radio* [2003] JOL 10745 BCCSA (Broadcasting Complaints Commission of South Africa).
[38] *Simons* (n 38) para 11.
[39] Act 70 of 2002 Commencement of Act on 30 September 2005 except sections 40 and 62. Sections 40 and 62(6) which commenced on 30 November 2005 and section 62(1)-(5) to be proclaimed.
Cell phone operators have objected to certain sections of RICA that compel them to capture their prepaid subscribers' details using a paper-based system instead of an electronic one. http://www.bday.co.za
[40] Section 16 An application for an interception direction must be made to a designated judge.
[41] Section 50(1), 50 (2).

3 5 The protection of personal information bill[42]

The Protection of Personal Information Bill, if passed by Parliament will give effect to the constitutional right to privacy of personal information. New methods of operating with regard to the collection and/or dissemination of any personal information stored must be regulated. It aims to protect individual's right to data privacy and protection of personal information.[43]

The purpose of the Bill is to give effect to the constitutional right to privacy, to regulate the manner in which personal information may be processed, to provide for persons with rights and remedies to protect person al information from processing not in compliance with the Bill and to establish an information protection regulator to ensure respect for and promote, enforce and protect the rights protected by the Bill.[44]

Personal information such as information relating to race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental status, health, well-being, disability, religion, conscience, belief, culture, language and birth of the person will be regulated.

Other types of information are protected.[45] The Bill also contains reference to "Special Personal Information" which is information concerning a child who is subject to parental control in terms of the law; or a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life, or criminal behaviour.

The processing of personal information and any activity or operation involving personal information, whether automated or not, will also be regulated.[46] This will include personal information stored in databases; address books; payroll systems or manual filing systems; information sent via email; in word processing programmes; exchanged in contracts with suppliers and recorded on CCTV and in telephone records.

The processing of personal information must comply with certain requirements, which are referred to as eight "information protection principles" ("Principles") in the Bill[47]. The regulator may authorise the processing of information that is in breach of the bill in certain circumstances such as where public interest in the processing of the personal information substantially outweighs any resultant interference with the data subject's right

---

[42] Protection of Personal Information Bill [B9-2009]. Available at http://www.pmg.org.za/bill/20090825- protection-personal-information-bill-b9-2009

[43] Information obtained from www.poliy.org.za/article/protection-of-personal-information-bill-2009-10-21. Accessed 15 April 2010.

[44] www.deneysreitz.co.za/index.php/news/protection_of_personal_information. Accessed 14 April 2010.

[45] Information relating to the education or the medical, financial, criminal or employment history of the person, any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person; the blood type or any other biometric information of the person; the personal opinions , views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person; and the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

[46] It includes the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distributing or making available in any other form, merging, linking, as well as blocking, erasure or destruction of information.

[47] The principles contained in sections 7 to 25 of the Bill deals with accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards, data participation subject.

to privacy.

The Bill further addresses issues pertain to the processing of personal information for purpose of direct marketing.[48]Companies must within one year from the date that the bill comes into force, ensure that their processing off personal information complies with the legislation and is notify to the regulator. The minister any extend this one year grace periods to a maximum of three years.
The Bill, if passed by Parliament, will undoubtedly impact on how companies and other institutions manage the processing of any personal information of their employees and customers. The cost of compliance for companies and other institutions will certainly be substantial. The bill, however does not address the issue about the right to privacy in non-communicative cellphone information.

Since the Constitution prescribes that international law must be considered when a court, tribunal or forum interprets the Bill of Rights, and that regard may also be had to foreign law,[49] a study of these sources may provide some assistance regarding the right to privacy (in respect of movement and location) of cellphone users, as well as the proper regulation of access to such information held by third parties.

4 International law

International law will be referred to in order to ascertain how privacy has been defined, and what the extent and scope of the realm of privacy are.

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 that consideration be given to establishing privacy protection guidelines in relation to personal data.

The privacy benchmark at international level can be found in Article 12 of the 1948 Universal Declaration of Human Rights (the UDHR), which 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."

Numerous other international human rights instruments contain provisions in almost the same language, which specifically recognise the right to privacy. Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR)[50] is worded similarly to

[48] Information for the purpose of direct marketing by means of automatic calling machines, facsimile machi9nes, SMSs or electronic mail is prohibited unless the data subject has given consent to the pro-cessing.
[49] Sec 39 (1) of The Constitution.
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.
[50] "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 12 of the UDHR.

The UN Human Rights Committee commented that Article 17 of the ICCPR should be given a broad interpretation to include 'the place where a person resides or carries out his usual occupation'.[51]

Article 14 of the 1990 United Nations Convention on Migrant Workers[52] contains privacy provisions similar to those in the UDHR and the ICCPR.

In similar vein, the privacy rights of a child are protected in Article 16 of the United Nations Convention on Protection of the Child.[53] Should any interference with a child's privacy take place, it must be lawful in terms of domestic laws and not arbitrary. The interference, in any event, should be reasonable in the circumstances. If legislation is enacted which allows interference, it must specify in detail the precise circumstances in which such interference will be permitted.[54]

The United Nations Guidelines Concerning Computerized Personal Data Files[55] are intended to encourage both those UN member states without data protection legislation in place to take steps to enact legislation based on the Guidelines, as well as international organisations to process personal data in a responsible, fair and privacy-friendly manner. The compilation and keeping of data- recorded information must be accurate and only for a specific purpose. People should have the right to know what information about them is stored.

4 2 Regional Instruments

4 2 1 The Convention for the Protection of Human Rights and Fundamental Freedoms

The European Convention for the Protection of Human Rights and Fundamental Freedoms created the European Commission of Human Rights and the European Court of Human Rights to oversee the enforcement of the rights stipulated in Article 8, 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."

---

[51] Steytler *Constitutional Criminal Procedure* (1998) 79.

[52] "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."

[53] "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."

[54] Steytler 80.

[55] Adopted by the General Assembly of the United Nations on 14 December 1990. Available at www.datenschutz-berlin.de/gesetze/internat/aen.htm.

4 2 2 *Decisions of the European Court of Human Rights*

The European Court of Human Rights regards Article 8 as reflecting a general right to privacy.[56] In *Klass v Germany* the Court held that telephone conversations are included in the notions of "private life" and "correspondence"[57]. This protection was extended in *Kruslin v France* to protect not only the subscriber to a telephone service, but any user of a telephone.[58]

In *Malone v United Kingdom* it was held that telephone tapping is a violation of the privacy rights guaranteed under Article 8.[59] As a result of this metering, information about the details of the numbers dialled on a particular phone, as well as the time and duration of calls, could be ascertained.[60] The release of that type of information to the police was not permissible without the consent of the subscriber. Information regarding the telephone numbers dialled from a specific telephone was an integral element of telephone communications; it was regarded as private and important enough to be protected as falling within the notions of "private life" and "correspondence" under Article 8.

In *Niemitz v Germany* 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.[61] Information conveyed to a third party, although private, will not automatically receive protection under Article 8. In *M.S v Sweden* it was held that it would depend on the manner in which the information was conveyed to the third party.[62] If the information had been disclosed earlier 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. Although there had been an interference with the applicant's right to respect for private life under paragraph 1 of Article 8, the interference had been justified under paragraph 2. Although the medical records contained personal information that was indeed of a very personal and sensitive nature, it had been conveyed earlier 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, play an important part in the right to receive protection for the information.

4 2 3 *American Convention of Human Rights*

Article 11 of the American Convention on Human Rights[63] sets out the right to privacy in terms similar to the UDHR. It is interesting to note that the African Charter on Human

---

[56] Steytler 80.
[57] *Klass v Germany* 6 September Series A no 28 at 41.
[58] *Kruslin v France* 24 April 1990 Series A no 176-a.
[59] *Malone v United Kingdom* 2 August 1984 Series A no 82.
[60] *Malone v United Kingdom* Para 83.
[61] *Niemits v Germany* 16 December 1992 Series A no 251 B.
[62] *M.S. v Sweden* (74/1996/693/885) 27 August 1997.
[63] "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."

and Peoples' Rights[64] does not make any reference to privacy rights.

4 2 4 *Instruments dealing with data protection*

Over the past 20 years technology has developed at an alarming pace and resulted in the automatic processing, collection and storage of personal information of individuals. A need arose to have regulations to safeguard the rights of individuals. Various regional instruments[65] contain principles that are very similar to the United Nations Guidelines Concerning Computerized Personal Data Files. It is apparent that a general right to privacy exists, but the international instruments do not indicate that the right to privacy protects non-communicative personal information, such as, the movement and location of cellphone users.

5 Comparative Jurisdictions

5 1 The United States of America

The jurisprudence of the United States of America has been influential both in South Africa and other countries. Although the word "privacy' is not mentioned in the Fourth Amendment or anywhere else in the American Constitution, the Fourteenth Amendment has been interpreted to include a general right to privacy, a right to be let alone, with respect to fundamental decisions concerning the individual's person.[66] Protection was given to adults to engage in private conduct in the exercise of their liberty under the Due Process Clause of this Amendment.[67]

It is Gormley's[68] opinion that scholars in America have been unable to agree upon any one-size-fits-all definition of privacy and that it actually consists of five distinct species.[69]

It is submitted that non-communicative information obtained from cell phone records

---

[64] Adopted by the 18th Assembly of the Heads of State and Government of the OAU on 27 June 1981 at Nairobi.

[65] 1. The Council of Europe: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CoE Convention);65

2. Organisation for Economic Cooperation and Development Guidelines on the 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)

[66] *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".

[67] Nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

[68] Gormley "One Hundred Years of Privacy" 1992 *Wisconsin Law Review* 1335.

[69] Gormley para 1434.

> **"1. The Privacy of Warren and Brandeis** (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.
>
> **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) decisions69 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 a variety of private and governmental intrusions generally often overlapping with species number one through number four above, yet often extending greater protections

probably falls under the Fourth Amendment, which deals with search and seizure and which 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."

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

At first the physical invasion of property was required to warrant protection under the Fourth Amendment. Violations of the Fourth Amendment only took place where there was a physical trespass on property, or seizure of material goods; government agents could employ dictaphones and microphones to listen to conversations as long as a defendant's property or person was not touched.[70]

In 1961, in *Silverman v United States,*[71] the Court changed its approach. It disallowed the use of a "spike mike", driven into the wall of a row house, which tapped into the heating duct and allowed officers to monitor conversations within the defendant's entire house. However, the Court still required some physical invasion of the premises and found that it was constituted in this case by the contact with the heating duct.

Katz v United States initiated the development of a reasonable expectation of privacy.[72] 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 conversations as he ran bookmaking activities in 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 not been violated. Justice Stewart's opinion was that the Fourth Amendment "protects people, not places".[73] In dealing with the privacy concept under the Fourth Amendment, he went on to say that "what a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[74]

Justice Harlan, in his concurring judgment, initiated the notion of *"reasonable*

---

to the citizen by

[70] *Olmstead v United States* 277 U S 438 (1928), the Court held that where no physical invasion of the defendant's premises occurred, there would not be protection under the Fourth Amendment. Wiretapping thus was not covered by the Amendment because the government had not invaded the defendant's premises physically. In *Goldman v United States*, 316 U S.129 (1942)., it was found that a detector placed against the wall of an adjoining room, did not qualify as a search and seizure. 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.

[71] *Silverman v United States* 365 U.S. 505 (1961).

[72] *Katz v United States* 389 U.S. 347, 353 (1967).

[73] *Katz* 351.

[74] Katz.

expectation of privacy", which is now regarded as the standard for search and seizure.[75] It is a two-requirement test, which was confirmed in *Kyllo vs. United States* in the following manner:

"[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."[76]

First there must 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 in the object of the search, society must be willing to recognise that expectation as reasonable. The second requirement thus brings an objective element into the test.

5 1 1 *Information revealing certain details*

Does American law grant an individual a right of privacy in non-communicative information revealing details, such as location and movement? In *Smith v Maryland*[77] the Supreme Court held that an individual targeted in a pen registering[78] does not have a reasonable expectation of privacy in the telephone numbers dialled from his home. An individual was assumed to know that in dialling a number, certain numerical information (date, time, and length of the call) was recorded by the communications service provider for billing purposes.[79]

Because the user voluntarily conveyed this information to the phone company, the installation and use, of a pen register was not a search, and no warrant was required. It seems that if there is an element of voluntariness present, the expectation of privacy is diminished; the fact that the details were voluntarily conveyed to the phone company is regarded as a waiver of the reasonable expectation of privacy in this information.[80]

If information is revealed to a third party, there also seems to be no expectation of privacy in such information. The bank records of an individual were subpoenaed in *United States v Miller*.[81] 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

---

[75] *Katz* 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). The test stipulates:
1.That the individual had an "actual" expectation of privacy and
2 That the expectation was "one that society was prepared to recognize as 'reasonable' ".
[76] *Kyllo v United States* 533 U.S. 27 (2001) 190 F 3d 1041. It was held 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.
[77] *Smith v Maryland* 442 U. S 735 (1979).
[78] The pen register is a device that records the date, time, and length of calls, information that is usually gathered already by phone companies for billing purposes by a communications service provider.
[79] Smith v Maryland
[80] See also Swedish judgment *M.S v Sweden*.

had to satisfy Fourth Amendment standards in order to obtain his financial records from his bank.

The Court held that a depositor had no expectation of privacy in financial information voluntarily conveyed to the bank, and because the information was exposed to its employees in the ordinary course of business. The Court found that an individual assumes the risk, in revealing his affairs to another, that the latter may then also reveal this information.

An exclusion of the reasonable expectation of privacy seems to have developed in the *Smith* and *Miller* cases. It is submitted that the United States Supreme Court will in all probability not afford protection to non-communicative cellphone information.

5 2 Canada

The jurisprudence developed under the Canadian Charter of Rights and Freedoms (the Charter) has been most influential in South African courts.[82] There is no explicit right to privacy in either Canada's Constitution or Charter. However, in interpreting section 8 of the Charter, which grants the right to be secure against unreasonable search or seizure, Canadian courts have recognised an individual's right to a reasonable expectation of privacy.[83]

Privacy at the federal level is protected by two Acts: the 1982 Privacy Act and the 2001 Personal Information and Electronic Documents Act (PIPEDA). The Privacy Act regulates the collection, use and disclosure of personal information held by federal public agencies, and grants individuals a right of access to personal information held by those agencies, subject to certain exceptions, including an exemption for court records. PIPEDA is applicable to private sector organisations that process personal information "in the course of a commercial activity", and also applicable to 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 right to privacy is also regarded as not subject to unreasonable searches or seizures. Evidence obtained as a result thereof will be excluded if it is found that the admission of the improperly obtained evidence would bring the administration of justice into disrepute.[84]
There will be certain situations when individuals will feel that information about them should not be revealed.[85]

---

[81] *United States v Miller*, 425 U.S. 435 (1976).
[82] Steytler 13.

[83] *Hunter v Southam* [1994] 2 S.C.R.145.
[84] The Charter guarantees certain rights.
Section 24 reads:

> (1) Anyone whose rights or freedoms, as guaranteed by this chapter, 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 in a manner that infringed or denied any rights or freedoms guaranteed by this charter, the evidence shall be excluded if it is established that having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice in disrepute.

[85] *R v Dyement* [1988] 2 S.C.R 417. 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,

5 2 1 *The two-stage test*

Canada has also developed a notion of "reasonable expectation of privacy". In *Hunter v Southam* the Supreme Court ruled that the guarantee provided in section 8 of the Charter is applicable only where individuals have a reasonable expectation of privacy[86]. The purpose of section 8 was to protect individuals from unjustified state intrusions. In *British Columbia Securities Commission v Branch,* the Court, referring to *Hunter,* stated that the context within which the violation takes place must be considered, for it is the context which determines the expectation of privacy.[87]

In *R v McKinley* it was held that individuals have different expectations of privacy in different contexts and with regard to different kinds of information and documents.[88]

There should be a standard to determine what is reasonable in a given context, and this standard must be flexible if it is to be realistic and meaningful. The test in Canada is, therefore also a two-stage one. First, an individual must manifest an expectation of privacy in the item/information. Secondly, an objective review to examine whether 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.[89]

It was held in *Thompson Newspaper Ltd v Canada*[90] that, whether a public authority takes documents or compels someone to hand them over, it infringes the right to privacy, and the conduct will be regarded as a seizure in terms of section 8.

5 2 2 *R v Plant*

The case of *Plant*[91] is critical for our enquiry. 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.[92]

On 9 March 1990 the Calgary police received an anonymous tip that marijuana was being grown at a certain dwelling. Without obtaining prior judicial authorisation, they used a terminal linked to the Utilities Commission's computer to check the electrical consumption at the dwelling: over a period of six months it was four times higher than the

---

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."

[86] *Hunter v Southam* (n 84) 145.

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

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

[89] *R v Edwards* [1996] 1 S.C.R. 128. The factors to be considered in assessing 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
(g) The objective reasonableness of the expectation.

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

[91] *R v Plant* [1993] 3 SCR 281. Confirmed in *R. v. Tessling*, [2004] 3 S.C.R. 432, 2004 SCC 67

average of two other residences with which it was compared.

This information was used to obtain a search warrant. One of the questions the Court had to decide was: did the information obtained from the computer records of the Utilities Commission reveal intimate details of the lifestyle and personal choices of the accused? If it was found that the accused had a reasonable expectation of privacy in this information, the police would have needed to obtain a warrant to access it.

It was held that to answer the questions various factors had to be considered, and that in considering them 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 as to how this should be resolved and the Court's judgment was not unanimous.

The majority of the Court[93] considered the following factors:

(a) *The nature of the information*

The Court held that the information seized must be of a "personal and confidential" nature that tends to reveal intimate details of the lifestyle and personal choices of the individual. The computer record only revealed how much electricity was consumed; an inference could not be drawn from the electricity consumption that an individual had made certain personal and private decisions.[94]

(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 Utilities Commission could not be characterised as a relationship of confidence. The records were prepared as part of an ongoing commercial relationship and there was no evidence that the Utilities Commission was contractually bound to keep the records confidential. The Court, however, qualified the above statement by saying that it was not suggesting that records prepared in a commercial context can never be subject to privacy protection in terms of section 8; if it were found that commercial records contained material which meets the "personal and confidential" standard, the commercial nature of the relationship would not prevent protection by the right to privacy.

It was held further that it generally was 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

---

[92] "Although the information about the distribution of the heat was not visible to the naked eye, the FLIR heat profile **did not expose any intimate details of the accused's lifestyle or part of his core biographical data".** It only showed that some of the activities in the house generated heat. ***My emphasis***

[93] The majority judgment of Lamer C.J, La Forest, Sophinka, Gonthier, Cory and Iacobucci JJ, was delivered by Sophinka J.

[94] In the Court of first instance, it was held: 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. That is different to the privacy expected with regard to confidential information in attorney/client and patient/doctor relationships. The information belonged to the electricity supplier and not to the individual. It had been 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 on whether it should be protected or not.

electrical consumption information to the police. It was the policy of the Utilities Commission to permit police access to the computer bank through a computer password held by them.

(c) ***The place where, and manner in which, the information was obtained***
The Court found that the place where, and manner in which, the information was retrieved also indicated that the appellant had no reasonable expectation of privacy. The police were able to obtain the information on-line, in terms of an agreement with the Utilities 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 might have suggested an element of privacy, but it could also have suggested that it was intended merely to ensure that the information was available to the police on-line. It was stated that, in any event, the search was 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 resulted in the requirements of the law enforcement agency outweighing the privacy claimed by the appellant. The Court held further that although participation in illicit trading of marihuana might not be as serious as trade in other narcotics, such as cocaine, it remained an offence which was taken very seriously by law enforcement agencies.

The majority, therefore, held that a consideration of all these factors did not warrant the conclusion that the appellant had had a reasonable expectation of privacy in relation to the computerised electricity records which outweighed the state's interest in enforcing the laws relating to narcotics offences. Although the Court stated that the information did not reveal intimate details of the lifestyle and personal choices of the individual, it found that the conclusion might differ if there were a contractual obligation towards the consumer to keep it confidential.

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 had been given? The Judge held that although electricity consumption records were close to the line, the evidence disclosed a sufficient expectation of privacy to require that the police obtain a warrant before the information was obtained. The information should not have been divulged to strangers without proper legal authorisation.

The following reasons were furnished for the finding:
(a) ***Records not available to public***
There was no evidence that the records were available to the public; the police only obtained access by reason of a special arrangement with the Utilities Commission. The details of electricity consumption were capable of telling much about an individual's lifestyle. They indicated how many people were residing in the dwelling and what sort of activities probably took place there. The consumption records told a story about what happened inside a private dwelling, the most private of places.

(b) ***Records disclosed personal information***
A reasonable person who looked at the facts would in all probability conclude that the records would only be used for the purposes for which they had been 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 electricity records are not as revealing as many others, they disclosed important personal information.

(c) ***Records disclosed a reasonable expectation of privacy***
The point that should have been considered was not whether the relationship between the individual and the Utilities Commission was one of confidence, but whether the particular records disclosed a reasonable expectation of confidence. The Judge also disagreed with the majority finding that the records were available generally totheto 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 as a very important factor. If it had been 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.

(d) Computers should be regarded as private
The Judge also disagreed with the majority view that the police had not had to intrude into places ordinarily considered private, like a house or hotel room, to get the information. It was found that computers might, and should, be regarded as being private, especially if they contain information which is subject to legal protection and in which the individual has a reasonable expectation of privacy. Computers can contain a wealth of personal information. Such information, depending on its character, may be as private as any found in a dwelling house or hotel room.

(e) Test should be expectation of privacy
Regarding the seriousness of the offence, reservations were expressed about using a case by case approach to determine whether a warrant to obtain information was required or not. 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 held by the Utilities Commission. The details of electricity consumption were capable of telling much about the individual's lifestyle, namely, they indicated how many people were residing in the dwelling, and what sort of activities probably took place there. The consumption records told a story about what happened inside the privacy of a private residence. That was precisely the reason for getting access to the records, to learn more about the personal lifestyle of the appellant. Only the police had access to the records, by means of a special computer which they had received in confidence. The majority held to the contrary: that the electricity consumption revealed very little about the private decisions of the occupants of the dwelling, and that it only revealed how much electricity was consumed by them in that dwelling.

5 2 3 *Privacy in movement and location*

Does any Canadian authority exist for the view that a person can have a reasonable expectation of privacy in movement and location? In his dissenting judgment in *R v Wise*[95] La Forest J stipulated that such an expectation could exist in information that reveals the movement of an individual. He held that the installation of a 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.

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 travelling on a public road. It was held that if an individual is in a vehicle and on a public road, his privacy rights are also protected. In this case the movements of an individual were tracked earlier.

A distinction was drawn 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 travelling, could be observed and even monitored by others. However, that was not the same as the risk that agents of the state, in the absence of prior authorisation, would be able to track every move made by an individual. It was not the case of another individual's casual glance, look or observation, but a question of every move being tracked.

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

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

It seems that a prisoner does not have a reasonable expectation of privacy in his movements. In *R v Dorfer* details about the time when, and place where, the appellant would receive treatment were furnished to the police. The Court held that in prison the whereabouts of an offender at any given time is information that is not expected to be confidential and is related to the proper functioning of a criminal justice system.[96] Thus a prisoner, it seems, cannot rely on the fact that he has a reasonable expectation of privacy

[95] *R v Wise* [1992] 1 S.C.R. 527. 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 or location).
[96] *R v Dorfer* (1996) 104 CC (3d) 528 (BCCA).

regarding his movements. One then could draw the inference that persons in police custody, arrested persons, or those who are lawfully detained, also will not have a right to privacy in their movements.

Dagg v *Canada* held that a person could have a reasonable expectation of privacy in information relating to his arrival and departure from a certain location.[97]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. 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 Minister's decision and filed a complaint with the Information Commissioner, arguing that the deleted information should be disclosed by virtue of exceptions to the protection of personal information in terms of the Privacy Actof 1982[98] The Federal Court (Trial Division), on a review of the Minister's decision, found the information not to be personal, but the Federal Court of Appeal reversed this decision on appeal.

An appeal from the Federal Court of Appeal was upheld, and the Supreme Court of Canada held that the Minister should reconsider his decision. The dissenting judgment, delivered by La Forest J, found that the purpose of the Privacy Act was 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. He 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.

La Forest J stated that 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 their location during non-working hours, even if that location was his or her place of employment.

He further found that the information obtained from the sign-in logs kept by the security personnel at the place of employment revealed intimate details of the lifestyle and personal choices of an individual. If information revealed personal details, in which a reasonable expectation of privacy existed, it should not be released without the individual's consent or prior judicial authorisation.

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 the proper manner.[99] To determine whether the search was properly done will depend upon whether it was necessary to obtain prior judicial

[97] *Dagg v Canada (Minister of Finance)* [1997] 2 S CR 403.
[98] Privacy Act Canada 1983.
[99] *R v Edwards*126; *Hunter v Southam*145.

authorisation.

5 2 4 *Prior judicial authorisation*

The purpose of prior judicial authorisation was defined in *Hunter v Southam*:

"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 to 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."[100]

It was further stated that it was preferable to have a system of prior authorisation to prevent unjustified searches, rather than having a system of subsequent validation. Reasonable and probable grounds, established under oath, to believe that an offence has been committed and that there is evidence to be found at the place of the search, constitute the minimum standard, consistent with section 8, for authority for search and seizure.[101]

It was held in by the majority in *Plant*[102] that the search must be brought within the parameters of section 8 to require prior judicial authorisation. It was held that accessing the information from the electricity records did not involve an intrusion into places ordinarily considered private, and that the information was not of a personal and confidential nature. The manner and place of search indicated a minimal intrusion, and the seriousness of the offence outweighed the privacy interest claimed by the appellant. The appellant did not have a reasonable expectation of privacy in relation to the computerised records which outweighed the interest of the state in enforcing the laws relating to narcotic offences; and, therefore it was not necessary to obtain prior judicial authorisation.

However in *R v Wise*[103] it was stated by La Forest J that the surreptitious electronic tracking of one's movements is a grave threat to individual privacy, which required prior judicial authorisation. Prior judicial authorisation called for an objective indication of reasonable and probable cause, which generally should be required of those seeking to employ electronic devices in the pursuit of individuals.

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

---

[100] *Hunter v Southam* 145.
[101] *Hunter v Southam* 145.
[102] Plant.
[103] *Wise*.

6 Conclusion

Based on the information gleaned from the comparative evaluation of Canadian, American and European jurisdictions it will be attempted to establish a framework which can be utilised for South African practice.

6 1 The Nature of Non-Communicative Cellphone Information

Whether protection will be afforded to certain information will depend on the nature of the information. According to Steytler,[104] 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; information which is of a "personal and confidential" nature.

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.

It is submitted that the abovementioned information is personal and reveals intimate details about the decisions and personal choices of an individual. By looking at this non-communicative information certain inferences can be drawn and certain deductions can be made which will reveal an individual's personal decisions and choices. On the face of it the information does not reveal anything about, for example, the political opinion or sexual preference of an individual. However, inferences relating thereto can be drawn by looking at the locations (such as a bar, shebeen, sports arena, club, church, and any other place of entertainment or worship) that are frequented by the individual. Much more is revealed than dialled telephone numbers[105], and it also goes further than the mere furnishing of a cellphone number without a user's consent.[106] This type of information is referred to in the Protection of Personal Information Bill as special personal information[107].

Although the bill does not specifically state that a person has a right in his movement and location, it is argued that it is indeed this type of information that can be ascertained by looking at this non communicative cellphone information.
It further is submitted that if the criteria identified in *Plant's* case are applied to non-communicative cell phone information, the information will be regarded as being personal and revealing of the personal choices and decisions of an individual. Determining where and when someone visited a certain dwelling/establishment may indicate the political, religious or sexual orientation and preferences of that person. Indeed, when one look at cell phone records, inferences can be drawn that an individual

[104] Steytler 104.
[105] *Malone v United Kingdom*.
[106] *Simons v P4 Radio*.
[107] Bill also contains reference to "Special Personal Information" which is information concerning a child who is subject to parental control in terms of the law; or a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life, or criminal behaviour.

made certain personal and private decisions.

The non-communicative information was not created in the context of a commercial transaction. The numbers dialled, and especially the duration of calls, are collected in order for the cell phone companies to furnish users with an account. It, however, is not necessary to include details of location and movement in accounts to clients. These details are captured only incidentally because of the manner in which various cell phones communicate via cellphone towers when a call is made. Information about the movement and location of cellphone users is not the exclusive property of cellphone companies.

Further, only cellphone subscribers who enter into cellphone contracts receive accounts; prepaid cellphone users do not. It, therefore, cannot be said that the non-communicative information forms part of the commercial records of cellphone companies.[108]

The nature of the relationship between the cell phone user and the cellphone company can be characterised as a relationship of confidence. The records of the duration of calls and of numbers dialled are kept as part of an ongoing commercial relationship. Cell phone companies are obliged to keep the records of their contract subscribers (not prepaid customers) confidential. It is generally not possible for an individual to inquire about the cellphone accounts or records of other users, and the information is not subject to inspection by members of the public at large.

The retrieval of information 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 able to obtain the information only by virtue of prior judicial authorisation, which is achieved in South Africa by the issuing of a subpoena in terms of section 205 of the Criminal Procedure Act.[109] An individual does have a reasonable expectation that the information in possession of the cell phone companies will be kept in confidence and restricted to the purposes for which it is obtained.

6 1 1 *Is the information conveyed voluntarily?*

It has been held in the US that if information about an individual is conveyed voluntarily there is no reasonable expectation of privacy therein.[110] It is submitted that the information regarding the movement and location of cell phone users is not conveyed voluntarily to the cell phone companies. It is debatable whether some users are even aware that they are transmitting these details. It is a contentious issue that cell phone companies have access to this type of non-communicative information, but for present purposes it is accepted that the information has been validly obtained. For cell phone information to be regarded as being voluntarily conveyed, the individual cell phone user must be aware that these details are recorded.

In determining whether or not information regarding the location and movement of cell phone users should fall within the ambit of privacy protection it is useful to use the criteria of the two-tier approach. It is submitted that cell phone users do have a

[108] *United States v Miller*.
[109] Act 51 of 1977.
[110] *Smith v Maryland*.

reasonable expectation of privacy in their movement and location, which will satisfy the first leg of the requirement, which is the subjective expectation. The objective element in this inquiry will be satisfied in that society will be willing to regard this expectation as being reasonable.[111] While it can be accepted that prisoners,[112] 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. They do have a right to privacy in their movement[113] and location.[114]

If a person has a reasonable expectation of privacy in his arrival at, and departure from, a certain location even if it is their place of employment,[115] then the movement of arrival at, and departure from, a location ascertained from cellphone records should also be protected. In addition, information about the location of cellphone users should not be divulged without their consent or without obtaining prior judicial authorisation.

6 2 How should this intrusion of the right to privacy be regulated?

The content of an individual's telecommunications is private and confidential. The state will be able to access it only with prior judicial authorisation.[116] If it is accepted that a right to privacy exists in non-communicative information, the question that needs to be addressed is: how should interference with that right be regulated?

International law prescribes that there should not be any unlawful interference with the privacy of individuals. Interferences are allowed only if they are not arbitrary or unlawful in terms of domestic laws, which must specify in detail the precise circumstances in which such interferences will be permitted.[117]

In the *Petersen*[118] case the police obtained authorisation to access the cellphone records. But could they have obtained the information if there were not enough evidence to obtain a section 205 warrant?

For instance, if the police have established an individual's time of death at a particular place, could they trawl through cell phone records for persons who may have been there at that time to establish a suspicion? Could they look at the 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 which can assist in them in the prevention and solving of crime?

There should be no objection to the obtaining and the publication of the information if the cellphone user has consented to the divulging thereof. In the absence of prior obtained consent from the user, it is submitted that the police will always require a section 205 warrant, and they can only obtain a section 205 warrant if certain conditions are met.

---

[111] The two-requirement test referred to in *Katz v United States* 353.
Kyllo v United States.
[112] *R v Dorfer*.
[113] *R v Wise*.
[114] *Dagg v Canada (Minster of Finance) [*1997] 2 S.C.R. 403.
[115] Dagg.
[116] Section 40 RICA Act.
[117] Steytler 80.
[118] S v Peteresen.

The police should have at least a suspicion before prior judicial authorisation in the form of a subpoena is granted; they should not be allowed to access the records in order to form a suspicion. This is not the purpose of prior judicial authorisation.[119]

It is preferable to have a system of prior authorisation to prevent unjustified searches than to have a system of subsequent validation.[120] If prior judicial authorisation is required, certain evidence must be available or certain requirements should be complied with, as was stipulated in *Hunter v Southam*[121]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 the place of the search, constituted the minimum standard.

The issue in *Plant*[122] can be distinguished from the issue regarding cellphone information. In that case it was stated that the appellant could not be said to have a reasonable expectation of privacy in relation to the computerised electricity consumption records which outweighed the interests of the state in enforcing the laws relating to narcotic offences; therefore, it was not necessary to obtain prior judicial authorisation. It is submitted that if the principles adopted in *Plant* are applied to cellphones, it will be found that a reasonable expectation of privacy does exist in non-communicative cellphone information. Therefore, to obtain details, such as, the location and movement of users, which are indicative of their personal choices and lifestyle would necessitate prior judicial authorisation.

6 3 Application of principle

If access to information in the possession of third parties is not regulated properly by legislation, the anonymity of users will be lost. Information obtained from a customer's personal bank records reflecting withdrawal dates, the times and locations of transactions at ATM machines, as well as details of credit card purchases, will all provide details of an individual's whereabouts and movements. Technology advances at an alarming pace and in future third parties could be in possession of, and have access to, information containing biometric features (such as fingerprints, palmprints, voice and eyescan DNA features).[123] If all information in the possession of third parties is not regulated properly, it effectively will remove an individual's right to determine what information about them others should know.

6 4 Conclusion

In conclusion, it is submitted that the nature and extent of non-communicative information (such as, location and movement of users) obtained from cellphone records is worthy of being protected by the right to privacy, since they disclose details about a person's personal lifestyle and choices. Although it is not strictly part of the inner core/inner sanctum or the privacy rights that can exist in a business of an individual, a person's family life, sexual relationships, and sexual preferences can be disclosed by

---

[119] The purpose of prior judicial authorization was defined in *Hunter v Southam* and 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 be breached only 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.

[120] *R v Wise*.

[121] *Hunter v Southam*.

[122] *Plant*.

[123] Van Tonder K "Biometrics Identifiers and Privacy" (August 2003) *De Rebus August* 19.

looking at the non-communicative information. Because a reasonable expectation of privacy exists in this type of information, access thereto should be regulated properly. 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 authorisation. At least in the Protection of Personal Information Bill[124] information such as a data subjects religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life, or criminal behaviour is regarded as special personal information which warrants protection.

Although the Bill does not specifically state that a person has a right in his movement and location, it is argued that it is indeed this type of special personal information as referred to in the Bill, that can be ascertained by looking at this non communicative cellphone information.

[124] The Protection of Personal Information Bill [B9-2009].