The Consumer's Right to Privacy: A Comparative Analysis

Student Name: Natalie Delphine Joseph
Student Number: JSPNAT001
Supervisor: Professor Tjakie Naude'
Qualification: LLM

Research dissertation presented for the approval of Senate in fulfillment of part of the requirements for the Master Degree in Commercial Law (LLM) in approved courses and a minor dissertation. The other part of the requirement for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of the Master Degree in Commercial Law (LLM) dissertations, including those relating to length and plagersim, as contained in the rules of this University, and that this dissertation conforms to those regulations.

Signed by candidate

ignature

15 February 2010

Date

Contents

1 HISTORY AND THE BASIS FOR CONSUMERISM IN SOUTH AFRICA

1.1 Introduction

As South Africa has a very rich political history, when new pieces of legislation are drafted (then subsequently enacted) there is always an attempt to correct the mistakes of the past. This is the reason that the South African Constitution (Constitution)[1] provides many fundamental rights.[2]

The apartheid era was the depression of South Africa but through this South Africa has grown. This is why it is inherent to the South African legislature to view all circumstances - whether they are legal, political or economical –by enacting laws which will be to the greatest benefit of the least advantaged.[3] Of course, apartheid was horrible for those that went through it, but the effect on the present and future laws have been a positive one. Without all the suffering that was endured throughout the apartheid era, South Africa would never be a country with such a wide-spread and seeking Constitution.

Under apartheid laws certain race groups were afforded more protection, privacy and respect than others. Under the apartheid system certain laws, such as the Pass System[4] meant that people of certain race groups had to ensure that they could produce their pass and without their pass, that person could be jailed.[5] Also laws such as the Group Areas Act[6] which was a law that ensured particular race groups had to live in designated areas

---

[1] Constitution of the Republic of South Africa, 1996.
[2] Chapter 2 Bill of Rights in the Constitution of the Republic of South Africa, 1996.
[3] Rawls *A Theory of Justice* (1971) 118.This is similar to the theory of John Rawls which is called 'the original position' found in 'The Theory of Justice'
[4] Natives (Abolition of Passes and Co-ordinated Documents) Act 67 of 1952.
[5] The pass system was where black people were forced to carry identification with them at all times. It was a criminal offence to be unable to produce a proper pass when the police demanded a pass. Also no black person could leave their race's designated area to go into the urban area without acquiring a permit to enter the urban area in About.com: African History *Apartheid Legislation in South Africa* Available at http://africanhistory.about.com/library/bl/blsalaws.htm (Accessed 24-12-2009).
[6] Group Areas Act 41 of 1950.

and the Bantu Education Act[7] which established an education system suited to the 'nature and requirements' of the black people are some illustrations of discrimination. Although these laws did not deal with privacy in relation to marketing they did affect the dignity and respect afforded to the individuals.

1.2 The Constitution

This is the reason the Constitution and subsequent pieces of legislation are consistently drafted with the aim to atone for past injustices. Section 1(a) of the Constitution expresses the above aim of the South African government to make amends for past injustices. South Africa is a democratic country and is founded on principles which will ensure that human dignity is afforded to and maintained for all its citizens.

The fundamental rights contain the minimum allowances for how all South African citizens must be treated. Also, South Africa is now a country which is based on constitutional supremacy.[8] This means that all other laws must fall within the fundamental principles set out in the Constitution. Any legislation that is contrary to the Constitution will be struck down as unconstitutional.[9] The Bill of Rights is the 'cornerstone' of the South African democracy and therefore must be managed with all the founding democratic values in the Constitution (these are human dignity, equality and freedom).[10] Fundamental rights are given to South African citizens but all rights in the Constitution are subject to limitation.[11]

The Bill of Rights contains more than the right to privacy[12] to protect the consumer.[13] The right to education[14] is arguably applicable to the consumer because all consumers have the right to be educated about their consumer rights. Very often the

---

[7] Bantu Education Act 47 of 1953.
[8] Section 1 (c) Constitution of the Republic of South Africa, 1996.
[9] Section 2 Constitution of the Republic of South Africa, 1996.
[10] Section 7 Constitution of the Republic of South Africa, 1996.
[11] Section 36 Constitution of the Republic of South Africa, 1996.
[12] Section 14 Constitution of the Republic of South Africa, 1996.
[13] Section 1 Consumer Protection Act "consumer". The consumer is the person to whom the goods are being marketed to in the ordinary course of the supplier's business or entered into a transaction with the supplier in the ordinary course of business
[14] Section 29 Constitution of the republic of South Africa, 1996.

people that suffer are those that fall into the lower income bracket. And often, these are the people who have not been given the proper chance to be educated. The consumer needs to know what his or her rights are when dealing with consumer-related problems. This will be illustrated throughout the paper.

1.3 Consumer Development in South Africa

Before the Consumer Protection Act (CPA)[15] South African legislation did not fully account for the participation of South Africa in the world market. The laws concerning the possible risks associated with international trade and the growing participation of South Africans in e-commerce was considered in the Electronic Communication and Transactions Act (ECT Act)[16] but not to the degree in which was required for the consumer. Consumer laws also need to take into account the continuous changes in technology and public policy.

This is the reason that the CPA has been one of the most highly anticipated pieces of legislation for many years. It ranks in the company of other anticipated Acts such as the National Credit Act (NCA)[17] and the Regulation of Interception and Monitoring of Communications Act (RICA).[18] Excitement has occurred because these Acts contain such vital guidance for consumers which illustrates the intention of the legislature and how public policy has transformed over the years.

Prior to the CPA being drafted there were many different acts aimed at different types of consumer protection. The most relevant to the consumer's right to privacy[19] is firstly the Consumer Affairs Act,[20] which aimed to control unfair business practices. That is practices which directly or indirectly affect the harmful relations between businesses and consumers. However this Act dealt more with business practices than regulation

---

[15] The Consumer Protection Act 68 of 2008.
[16] Electronic Communication and Transactions Act 25 of 2002.
[17] National Credit Act 34 of 2005.
[18] Regulation and Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002.
[19] Chapter 2 Part B Consumer Protection Act.
[20] The Consumer Affairs (Unfair Business Practices) Act 71 of 1982.

concerning marketing procedures. This Act has since been repealed by the CPA. In fact the CPA goes further than only dealing with fair business trading. The CPA is a massive piece of legislation and the provisions contained within it need to be capable of being enforced.

Secondly, the Standards Act[21] controlled the standards at which goods and services were sold. This provided for the continued existence of the South African Bureau of Standards which promotes and maintains the standards of the goods or services being sold. Again, this Act dealt with the standard of the goods sold and not with marketing and pre-contractual issues which would govern the privacy of the consumer.

Thirdly, the Promotion of Access to Information Act (PAIA)[22] gives effect to the constitutional right to access to information[23] held by the State and any other person that is required for the exercise or protection of any rights. This Act, which is still relatively new, deals with how one would go about accessing certain information. This Act is also not relevant to how a consumer would handle the integrity of the privacy of their information being compromised. Nevertheless the PAIA will be discussed later.

Lastly RICA deals with the interception and monitoring of communications. Although this Act deals with privacy issues, the provisions are aimed more at the State's relationship with the citizens then between the retailer or manufacturer and consumer. Of course RICA can be applied between individuals but the aim of the Act is not to regulate marketing problems or the integrity of the consumer's privacy.

The growing importance of consumerism has finally been rewarded with the CPA. It would be disappointing to find that these long-awaited sets of rules are of no use to the consumer. But it should be remembered that there is more than the 'pure' consumer to be considered.

---

[21] The Standards Act 29 of 1993.
[22] The Promotion of Access to Information Act 2 of 2000.
[23] Section 32 Constitution of the Republic of South Africa, 1996.

If one considers the welfare of consumers then it would be obvious that there is more than one type of party to consider during consumer transactions. The manufacturer or supplier is also important as well as the State.[24] The manufacturer participates in the marketplace with the primary goal of profitability and is only concerned with consumer policy to the extent that the policy encourages or discourages the consumer to buy from them.[25] The State on the other hand has to play a balancing act because consumers are potential voters[26] (and therefore need to be kept happy) and if manufacturers are given unreasonable demands (for example expertise required that is too expensive for the manufacturer to afford) the manufacturers may refuse to participate in the economy.[27] However, almost nobody is only a consumer [28] and therefore the manufacturer is also the consumer in one respect or another. Thus it is fundamental to retailers and manufacturers to take responsibility.

The CPA will help the consumer gain some ground back, in a world where consumers are motivated by false promises, high prices and low quality.[29] These are interesting times to be a part of parliament in South Africa or many other countries.

If the Act is applied with the correct vision, the CPA can be beneficial to all parties concerned.[30]

The problem with consumer transactions is that most consumer transactions are made in small quantities and therefore people are skeptical and too busy to go to court to report and enforce their grievances.[31] This is the reasoning behind the National Consumer Commission.[32]

---

[24]Offe "Alternative Strategies in Consumer Policy" in Ramsey *Consumer Law* 141.
[25] Offe "Alternative Strategies" in *Consumer Law* 41.
[26] Offe "Alternative Strategies" in *Consumer Law* 41-42.
[27] Offe "Alternative Strategies" in *Consumer Law* 42.
[28] Offe "Alternative Strategies" in *Consumer Law* 63.
[29]Jazzbhay "Corporate Social Responsibility and the Consumer Protection Act" 22-09-2009 Available at http://www.law24.com/blogs/Saber+Ahmed+Jazzbhay/732-Corporate-Social-Responsibility-and-the-Consumer-Protection-Act (Accessed 30-09-2009).
[30] Jazzbhay "Corporate Social Responsibility".
[31] Epstein *In a Nutshell* 7.
[32] Chapter 5 Part B Consumer Protection Act.

1.4 Foundations of the CPA

The CPA actually recognises 'fundamental consumer rights'.[33] There are several fundamental consumer rights, namely a right to equality;[34] privacy;[35] the right to choose;[36] disclosure and information;[37] fair and responsible marketing;[38] fair and honest dealing;[39] fair, just and reasonable terms and conditions;[40] fair value, good quality and safety[41] and supplier's accountability to consumers.[42] The right to privacy is the fundamental right which will be the focus of this paper.

1.4.1 Direct marketing in the CPA

The definition of 'direct marketing' which will be followed throughout this paper is:

> "[Approaching] a person, either in person or by mail or electronic communication, for the direct or indirect purpose of-
>
> (a) Promoting or offering to supply, in the ordinary course of business, any goods or services to the person; or
>
> (b) requesting the person to make a donation of any kind for any reason."[43]

This definition will be used as the basis throughout this discussion. This definition is widely worded to fall within the purposive approach of the CPA. This makes sense for the legislature because as discussed above the CPA is intended to provide the most protection possible for the consumer without frustrating the flow of the economy and marketplace to work efficiently for the manufacturer and the State.

---

[33] Chapter 2, Consumer Protection Act.
[34] Chapter 2, Part A Consumer Protection Act.
[35] Chapter 2 Part B, Consumer Protection Act.
[36] Chapter 2 Part C, Consumer Protection Act.
[37] Chapter 2 Part D, Consumer Protection Act.
[38] Chapter 2 Part E, Consumer Protection Act.
[39] Chapter 2 Part F, Consumer Protection Act.
[40] Chapter 2 Part G, Consumer Protection Act.
[41] Chapter 2 Part H, Consumer Protection Act.
[42] Chapter 2 Part I, Consumer Protection Act.
[43] Section 1 Consumer Protection Act.

that the CPA will be applicable to various consumer transactions. Including electronic communications which are those communications made through electronic transmissions.[46]

1.4.2 Fundamental Consumer Rights

It seems that the legislature was motivated by its paternal instincts to protect the consumer. Of course it is yet to be determined if the CPA will really protect or harm the consumer. Regulation of consumer protection is a process which requires technical expertise as described in the CPA for the transaction and political management for the consumer.[47] Therefore all fundamental rights will only be of use if they are actually capable of being enforceable and if they are capable of being adapted to protect the consumer.

The origin of 'fundamental consumer rights' appears to be from the United Nations.[48] Because the 'Preamble' makes reference to 'internationally recognized customer laws'[49] consumerism is taken to a new level of protection.

On consideration of fundamental consumer rights, the creation of the consumer's fundamental right to privacy is necessary, especially in today's time where problems such as identity theft is becoming more common.

1.4.3 Understanding the Consumer

When drafting the CPA the legislature had to create provisions that would be easily understandable for the consumer but also easy to enforce. The CPA has to be able to be understood by all consumers because the market will not work efficiently if the people are misinformed about the choices available to them.[50] The central intention of the CPA

---

[44] Section 1 'person' Consumer Protection Act.
[45] Section 5 (2) Consumer Protection Act.
[46] Section 1 'electronic communications' Consumer Protection Act.
[47] Ramsey *Consumer Law* xii.
[48] United Nations Guidelines for Consumer Protection (as expanded in 1999).
[49] Van Eeden *A Guide to the Consumer Protection Act* 2009 26-27.
[50] Cayne & Trebilcock "Market Considerations" in *Consumer Law* 1 29.

should be to provide some protection on behalf of the consumer in situations which would otherwise leave the consumer in a vulnerable bargaining position.[51]

1.4.4 Interpretation

The CPA provides that it must be approached with a purposive approach.[52] This means that the Act must be interpreted in a wide sense as long as the overall purposes of the Act are fulfilled. The main purpose of the Act is to promote and advance the social and economic welfare of consumers.[53] In order to do this there is certain criteria that are set out in section 3. One of the CPA's purposes is to promote fair business practices;[54] another is to protect the consumer from unconscionable, unfair, unreasonable, unjust or otherwise improper trade practices;[55] and improving consumer awareness and information and encouraging responsible and informed consumer choice and behaviour.[56]

Also the courts and all those that use the CPA may consider appropriate international laws and conventions.[57]

1.5 The Privacy and Data Related Revolution

As discussed above, South Africa's rich history affects the way the law works today. One of the fundamental rights found in the Bill of Rights is the right to privacy.[58] This is a right that has been implemented in the Universal Declaration of Human Rights as well.[59] It would be difficult to dispute the necessity of this right in South Africa and internationally.

---

[51] Cayne & Trebilcock "Market Considerations" in *Consumer Law* 1 33-34.
[52] Section 2 (1) Consumer Protection Act.
[53] Section 3(1) Consumer Protection Act.
[54] Section 3 (c) Consumer Protection Act.
[55] Section 3 (d) (i) Consumer Protection Act.
[56] Section 3 (e) Consumer Protection Act.
[57] Section 2 (2) (a) and (b) Consumer Protection Act.
[58] Section 14 Constitution of the Republic of South Africa Act, 1996.
[59] 1948 Universal Declaration of Human Rights.

The right to privacy is fundamental for a free world to exist. In past wars and past governments certain people were not afforded the luxury of keeping certain affairs to themselves. This is what stemmed the world's obsession with privacy.[60] This is the reason that the Constitution provides the basic right to privacy. It is called a 'basic' right to privacy because the Constitution deals more with the person's physical privacy than with the person's transactions. This does not mean that the right to privacy concerning direct marketing is excluded but it is only applicable through indirect application of section 14 of the Constitution. There is a need for the individual to protect intrusions of integrity.[61]

Wacks[62] identifies four functions of privacy.[63]These are, firstly, that privacy provides personal autonomy[64] (this is the principle which makes the individual desire not to be manipulated or dominated by others); personal release[65] (the feeling that you have the freedom to do what one pleases); self-evaluation[66] and opportunities to choose who you want to share certain intimacies with.[67] It seems that privacy and freedom are intimately linked to one another.

This is the reason that subsequent pieces of legislation tend to produce more protection in smaller doses but in many different areas. This is one of the many reasons that the Protection of Personal Information Bill (POPI Bill) is imminent to being passed as an Act.[68] In order to fully understand Section 11 and Section 12 of the CPA, the Bill needs to be investigated. This investigation may lead to the conclusion that the CPA and the POPI Bill may or may not harmonise but a thorough enquiry will be done later in the discussion.

---

[60]Kenyon & Richardson *New Dimensions* 1.

[61] Kenyon & Richardson *New Dimensions* 1.
[62] Wacks *Personal Information Privacy and the Law* (1989).
[63] Wacks *Personal Information* 11-12.
[64] Wacks *Personal Information* 11.
[65] Wacks *Personal Information* 12.
[66] Wacks *Personal Information* 12.
[67] Wacks *Personal Information* 12.
[68] The Protection of Personal Information Bill [B9-2009].

The right to privacy is fundamental for a free world to exist. In past wars and past governments certain people were not afforded the luxury of keeping certain affairs to themselves. This is what stemmed the world's obsession with privacy.[60] This is the reason that the Constitution provides the basic right to privacy. It is called a 'basic' right to privacy because the Constitution deals more with the person's physical privacy than with the person's transactions. This does not mean that the right to privacy concerning direct marketing is excluded but it is only applicable through indirect application of section 14 of the Constitution. There is a need for the individual to protect intrusions of integrity.[61]

Wacks[62] identifies four functions of privacy.[63]These are, firstly, that privacy provides personal autonomy[64] (this is the principle which makes the individual desire not to be manipulated or dominated by others); personal release[65] (the feeling that you have the freedom to do what one pleases); self-evaluation[66] and opportunities to choose who you want to share certain intimacies with.[67] It seems that privacy and freedom are intimately linked to one another.

This is the reason that subsequent pieces of legislation tend to produce more protection in smaller doses but in many different areas. This is one of the many reasons that the Protection of Personal Information Bill (POPI Bill) is imminent to being passed as an Act.[68] In order to fully understand Section 11 and Section 12 of the CPA, the Bill needs to be investigated. This investigation may lead to the conclusion that the CPA and the POPI Bill may or may not harmonise but a thorough enquiry will be done later in the discussion.

---

[60]Kenyon & Richardson *New Dimensions* 1.

[61] Kenyon & Richardson *New Dimensions* 1.
[62] Wacks *Personal Information Privacy and the Law* (1989).
[63] Wacks *Personal Information* 11-12.
[64] Wacks *Personal Information* 11.
[65] Wacks *Personal Information* 12.
[66] Wacks *Personal Information* 12.
[67] Wacks *Personal Information* 12.
[68] The Protection of Personal Information Bill [B9-2009].

Privacy is a concept which has always been entrenched in our systems, from religions to laws.[69] The Constitution aims to give you this right but something that seems like a simple request comes attached to many strings. It supports human dignity and other values such as freedom of association and freedom of speech. It has become one of the most important human rights of the modern age.[70]

The lack of a single definition for privacy should not imply that the issue lacks importance. The need to understand the nature of the right to privacy in order to have legal certainty and protection has always been emphasised.[71]

Nevertheless, it is important to remember that the Constitution holds a limitation clause.[72] This means that all the rights in the Bill of Rights may be limited in certain circumstances. This is the reason that acts such as RICA could be accepted. Even though RICA has the potential to be abused, the invasion of an individual's private affairs may only acceptable under certain circumstances.

In previous years data privacy protection in South Africa had minimum legislative interference. This is due to the common law not being developed sufficiently by the South African legislature in order to deal with the revolution of technology.[73]

The courts have emphasized that the circumstances of a particular case must be considered before passing judgment.[74] This is extremely relevant for scenarios in which public personalities or celebrities privacy has been invaded.

---

[69] Privacy International *Overview of Privacy* (2007) http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559062# (Accessed 7-09-2009) ranges from the Jewish religion, Christianity, Islam all the way to Ancient Greece.

[70] Privacy International *Overview of Privacy*.

[71] South African Law Reform Commission Discussion Paper 109 Project 124 October 2005 "Privacy and Data Collection" Available at http://salawreform.justice.gov.za/dpapers/dp109.pdf (18-01-2010) 1 10.

[72] Section 36 Constitution of the Republic of South Africa, 1996.

[73] McQuoid – Mason *The Law of Privacy in South Africa* (1978) 9.

[74] *O'Keeffe v Argus Printing and Publishing Co Ltd.* 1954 (3) SA 244 (CC).

1.5.1 Personal Information

'Personal information' has now been defined in the POPI Bill. The definition of ''personal information'' is information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— [75]

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
(b) information relating to the education or the medical, financial, criminal or employment history of the person;
(c) any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person;
(d) the blood type or any other biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the person; and
(h) 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.

Information exists in many different forms for example it can be spoken, written, printed, stored physically and electronically, and transmitted by post or electronically, it can be shown on films and broadcasted in all mediums of multimedia.[76] The end result is the same - that in whatever manner or form the information may exist - it has to be

[75] Protection of Personal Information Bill.
[76] SALRC "Privacy and Data Collection" 66 4.2.141.

protected. Unfortunately, in many businesses and legal safeguards the protection is yet to be developed.[77]

Unfortunately South Africa is a country which is plagued with an obsolete and unproductive identity document. This allows for easily forged or altered identity documents to be made which has resulted in large numbers of impersonations and identity theft. Taking the above factors into consideration it will be many years before the new identity card system becomes fully effective in South Africa. Subsequently this forces the legislature to take steps to attempt to combat the problems of identity theft.

1.5.1.1 Database Information

Databases are developed over time and in order to have a successful database there needs to be continuous communication between the consumer and the marketer. This communication creates the possibility for the consumer's privacy to be infringed.[78] The way in which direct marketers may comfort their consumers when using direct marketing methods is to disclose information such as their privacy policies and practices.[79]

1.6 The International Stimulus

When international laws are considered there seems to be a massive movement in this direction of affording consumers stronger rights and protections. Consumers are being seen as more than just the money but a voice which needs to be heard and considered.

The Canadian author, Ramsey, has an appealing view of what consumer protection is. [80] His definition of consumer protection law is all the ways in which the State "[c]onstitutes, defines and intervenes..." in the marketplace with for the purpose of

---

[77] SALRC "Privacy and Data Collection" 66 4.2.141.
[78] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.
[79] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.
[80] Ramsey *Consumer Law* (1992).

protecting the ultimate consumer.[81] This definition captures the very essence of consumer protection laws.

There is hope for an emergence of 'ethical consumerism' that has developed in the United States to filter into the South African community.[82] Corporate Companies drive their successes by ensuring that only their shareholders are happy. This is no longer the case as they are forced to consider the consumer.[83] This is because the backlash that may occur if their consumers are treated unfairly (and are therefore unhappy) is massive and would be extremely damaging to their brands.

1.6.1 The United Nations (UN)

The United Nations Guidelines for Consumer Protection (UN Guidelines) [84]is an international standard encouraged by the United Nations for transactions concerning the consumer. The objectives of the UN Guidelines are to consider the interests and needs of the consumer.[85]

The UN Guidelines encourage ethical conduct for when companies engage in the production and distribution of goods and services with consumers.[86] Another aim of the UN Guidelines is to assist with curbing abusive business practices by enterprisers that may adversely affect the consumer.[87] Also the UN Guidelines should encourage the development of market conditions which may lead to lower prices for the consumer.[88]If the marketplace consists of lower prices, the consumer will be more at ease and this will subsequently be to the benefit of all parties.

The UN Guidelines are meant to be precisely that – guidelines for countries to adopt their laws to be more consumer friendly. When various governments, such as South

---

[81] Ramsey *Consumer Law* (1992) xi.
[82] Jazzbhay "Corporate Social Responsibility".
[83] Jazzbhay "Corporate Social Responsibility".
[84] United Nations Guidelines for Consumer Protection (as expanded in 1999).
[85] Section I (1) UN Guidelines.
[86] Section I (1) (c) UN Guidelines.
[87] Section I (1) (d) UN Guidelines.
[88] Section I (1) (g) UN Guidelines.

Africa, draft their consumer laws the UN Guidelines as well as relevant international laws should be considered.[89] However upon consideration of foreign and international laws and standards each country has to make their comparative research with caution. This is because it would be dangerous to translate the experiences of other countries directly into your own law.[90]

The UN Guidelines also require that the legitimate needs of the consumer must be met.[91] The applicable legitimate interests for the consumer's right to privacy is that the consumer needs to be able to access adequate information in order to make informed decisions.[92] Also the consumer needs to be educated on all possible impacts of the consumer's choice.[93] Another legitimate interest that must be considered is that there is redress available for consumers. [94]

One of the major guidelines is that promotional marketing and sales practices should be guided by the principle of fair treatment.[95] This will allow for consumers to make informed decisions.

Governments in their respective countries should encourage the formulation of proper execution by businesses for codes of marketing and other business practices to be implemented.[96] This will ensure that the consumer is protected adequately in the specialised industry of marketing.

The consumer receiving adequate education on matters which affect him or her needs to be provided by the government.[97]It is also suggested that consumer education should become integral to the basic curriculum of the educational system.[98]The education

---

[89] Section II (2) UN Guidelines.
[90] SALRC "Privacy and Data Collection" 372 8.1.1.
[91] Section II (3) UN Guidelines.
[92] Section II (3) (c) UN Guidelines.
[93] Section II (3) (d) UN Guidelines.
[94] Section II (3) (e) UN Guidelines.
[95] Section III B (22) UN Guidelines.
[96] Section III B (26) UN Guidelines.
[97] Section III F (33) UN Guidelines.
[98] Section III F (36) UN Guidelines.

of the consumer needs to be considered and subsequently be appropriate for all consumer types. Especially the lower-income consumer groups because they need to be able to understand the consumer laws which are available to them and howto apply them to their problems.[99]

When considering the growth spurt of e-commerce the governments need to ensure that their consumer laws are implemented with consideration of international laws and standards.[100] This is to ensure that the consumer is not disadvantaged due to the inability to compete in international trade and transactions because of insufficient consumer protection laws.

1.7 E-Commerce

To consider the issues surrounding the consumer's privacy concerning direct marketing in electronic transactions and communications the ECT Act will be considered briefly because there are certain exemptions made in the CPA which differ from the ECT Act. Of course the ECT Act will only apply to electronic transactions but due to the growing rate of e-commerce, the effect technology has on consumers and privacy must be considered.

1.7.1 ECT Act Objectives

Two objectives of the ECT Act are to provide for human resource development in electronic transactions and to prevent abuse of information systems[101] which are the most important to bear in mind during this discussion. The ECT Act aims to remove and prevent barriers surrounding electronic communications and transactions,[102] promote legal certainty, confidence in respect of electronic communications and transactions,[103]

---

[99] Section III F (40) UN Guidelines.
[100] Section IV (69) UN Guidelines.
[101] Section 1 of the Electronic Communication and Transactions Act "information system" means a system for generating. sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet".
[102] Section 2 (1) (d) Electronic Communication and Transactions Act.
[103] Section 2 (1) (e) Electronic Communication and Transactions Act.

ensure that electronic transactions in the Republic conform to the highest international standards,[104] ensure that there is compliance with accepted international technical standards[105] and guarantee that the national interest of the Republic is not compromised through the use of electronic communications.[106]

1.7.2 Privacy in the ECT Act

The ECT Act deals with the protection of personal information in Chapter VIII. The scope, however, is confined to personal information that has been obtained through electronic transactions.[107]Unfortunately personal information is not defined within a comprehensive list in the ECT Act.

1.8 Conclusion

Social responsibility needs to be enforced by the consumers, the Act allows for such support. It seems that with the introduction of the Consumer Tribunal South African consumers may now have a real method of recourse to get the service which they require.[108] However South Africans should not get caught up in the novelty of the Act and be fooled by empty promises. Consumers need to be responsible for themselves and be capable of enforcing their rights.

The idea of ethics playing a role in consumerism is interesting and one wonders if it is possible. We should bear in mind that South Africa is still a young democracy and in educating the people of South Africa with ethical consumerism may very well become a massive part of the way the economy works. It is only fair that as South Africa moves into new positions in the economic spheres worldwide, that consumers and competitors may reap the benefits of these improvements. Morality, or lack thereof, has been a huge

[104] Section 2 (1) (h) Electronic Communication and Transactions Act.
[105] Section 2 (1) (m) Electronic Communication and Transactions Act.
[106] Section 2 (1) (r) Electronic Communication and Transactions Act.
[107] Section 50(1) Electronic Communication and Transactions Act.
[108] Jazzbhay "Corporate Social Responsibility".

thorn in South Africa's growth but with the correct education and empowerment anything is possible.[109]

It is accepted that there is a very real need for protection to be put in place for consumers.[110] In years gone by problems around advertising and the effects of advertising have been identified but governments have been reluctant to intervene.[111] Where there has been a need for regulation, the parties have had to depend on self-regulation.[112] This is also true for South Africa as the Advertising Standards Authority of South Africa (ASA) is an example of self-regulation. The success behind these regulations is yet to be determined. It is difficult to ignore that legislation has been pleading for a solid proliferation of consumer protection.[113]

Information privacy issues are not only consumer problems but due to international laws they may become trade hindrances.[114]

The CPA is supposed to comfort the consumer but it is still unclear as to how well the Act will work. Similarly to any other new legislation, the public and the government need to be wary of these new laws. Nevertheless only time may tell the result of this long-anticipated piece of legislation. Therefore this paper aims to investigate some of the new issues in consumer protection laws and some old issues. But the issue of the consumer's right to privacy will be the main focus of the paper.

---

[109] Jazzbhay "Corporate Social Responsibility".
[110] Epstein *Consumer Law in a Nutshell* 2 ed *(1981)* 4.
[111] Ramsey *Consumer Law* xiii.
[112] Ramsey *Consumer Law* xiii.
[113] Cayne &Trebilcock "Market Considerations in the Formulation of Consumer Protection Policy" in Ramsey *Consumer Law* (1992)1 4.
[114] Jordaan "Information Privacy Issues: Implications for Direct Marketing" 2007 *International Retail and Marketing Review Volume 3 Issue 1 May* 42 52.

2 ANALYSIS OF THE RELEVANT PROVISIONS OF THE CPA AND OTHER INFLUENCIAL ACTS AFFECTING THE CPA

Due to the changing times and technological complexities there are demands for consumers to significantly influence economic behaviour in the consumer marketplace.[115] Put simply, the marketplace needs to suit the needs of the consumer and this means that the manufacturers, suppliers as well as any other parties need to ensure that the consumer's needs are being satisfied.[116] This is the reason that the consumer is going to be able to receive protection from the CPA.

There are no laws which directly pertain to regulating the marketing industry. In fact, there is no legislation with its sole purpose of focusing on marketing. This is because over the years marketing has been treated in a similar manner to advertising. This means that marketing has been more or less self-regulating, as will be discussed below.

2.1 The Department of Trade and Industry's Approach

According to the Department of Trade and Industry (DTI) the consumer must acquire the knowledge and skills to be able to make informed decisions concerning goods and services.[117] The DTI seeks to educate the youth and consumers who fall within the lower income bracket to further their vision of empowering the impoverished. The right to consumer education is not the sole responsibility of the DTI because businesses and the Government must attempt to educate all consumers.[118] This is an illustration of how the right to education in the Constitution is applicable to consumer education.

---

[115] Trebilcock "Winners and Losers in the Modern Regulatory System: Must the Consumer Always Lose?" in Ramsey *Consumer Law* 87 87-88.
[116] Trebilcock "Winners and Losers" in *Consumer Law* 87-88.
[117] The Department of Trade and Industry "What are a Consumer's Rights and Responsibilities?" Found at http://www.dti.gov.za/protectingconsumers/consumerrights.htm (Accessed 3-1-2010).
[118] DTI "Consumer's Rights and Responsibilities?".

The Consumer Protection Bill, in line with the DTI's mandate, was enacted to the current CPA and has not been shy of discontent.[119] Some critics believed that Consumer Protection Bill had many superfluous provisions that could create interpretation problems.[120] This may or may not be the case but only once the CPA has been enacted and used will interpretation problems be discovered. Furthermore, these critics,[121] viewed the Consumer Protection Bill as a large codification of common law and generally accepted practices which are common place in the South African market.[122]

2.2 Direct Marketing

The definition of "direct marketing" is worded widely and has been set out in chapter one.[123] This allows for the purpose of the CPA to be fulfilled. The definition may be separated into different elements which make up the complete definition. These are:

a) who the consumer is;

b) promotion or offer;

c) in the ordinary course of business and

d) goods or services and donation.[124]

These elements can be simply understood which allows for this section of the Act to be easily understandable.

---

[119] Lee & Du Plessis "The Consumer Protection Bill: Kill it Says New Marketing Body" 2006 *Journal of Marketing Jun/ July* 3.
[120] Lee & Du Plessis "The Consumer Protection Bill" 2006 *Journal of Marketing* 3.
[121] Composed by marketing specialists and corporate lawyers.
[122] Lee & Du Plessis "The Consumer Protection Bill" 2006 *Journal of Marketing* 3.
[123] Section 1 'direct marketing' Consumer Protection Act.
[124] Section 1 'direct marketing' Consumer Protection Act.

Possible complications concerning the elements of direct marketing is the inclusion of "promote or offer". "Promote or offer" is imperative for marketing to work effectively. It is for this reason that advertising becomes a factor to be considered.

Jordaan identifies several advantages to direct marketing.[125] A few include the manner and speed in which information processing technology is growing which allows for the collection of information to be done in a simpler and more prompt manner which is appealing to the marketer and the consumer who is volunteering their information.[126] Also the effects of direct marketing are uncomplicated to measure and therefore the databases have become more feasible.[127] Furthermore, direct marketing allows for the target group to be reached.[128]

The direct marketers need to collect information only when it is necessary for them to create or continue a viable relationship with the consumer.[129] This will illustrate to the consumer that the direct marketer has his or her best interest at heart. Although this may not be the first intention of the direct marketer, a happy consumer will mean the consumer is more willing to engage with the direct marketer thus increasing sales.

The consumer wants reassurance that the private information which they provide to the direct marketer will be maintained with integrity. Research illustrates that when a consumer engages in direct marketing, it does not necessarily mean that the consumer trusts the marketer.[130] The direct marketer needs to illustrate commitment to the consumer by providing efficient and fair privacy policies and practices.[131] These policies and practices should be known by the consumer; moreover, allowing for the consumer to feel secure in their relationship with the direct marketer.

This may mean that the direct marketer will have to guarantee that only certain employees have access to the information and that the information will not be sold or

---

[125] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.
[126] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.
[127] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.
[128] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.
[129] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 50.
[130] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 50.
[131] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 50.

traded with other direct marketers. Due to technology, databases are easy and affordable to maintain and trade with.[132]Also it is more convenient to keep records of the direct marketing successes.[133]

Direct marketers need to allow consumers greater control over the handling of their personal information.[134] This means the consumer should be able to access their information and maintain and control who gains access to the information. Of course different industries will require different levels of information security.[135] Organisations should ensure that the information privacy principles which they use are not only compliant with what their particular industry requires but should also consider international laws, standards and recommendations.[136] This is one of the reasons the Safe Harbour Privacy Principles were created.

During direct marketing a consumer may feel compelled to purchase the goods or services offered, as some consumers may have difficulty deciding, feel pressured to make the purchase or the consumer may find after the purchase has been made that their financial status is not what they initially thought. There are multiple reasons that the consumer may regret his or her purchase. It is for this reason that the CPA provides a 'cooling-off period' which affords the consumer with the right to receive a cooling-off period after receiving direct marketing presentations.[137]

2.2.1 The Consumer's Use of His or Her Rescission Options

The CPA gives the consumer five days to rescind a transaction which resulted from any direct marketing.[138] The inclusion of "any" may be problematic for the supplier but until the CPA is enacted and applied, it is unclear what the ramifications of this wording will be. It is understandable that the Legislature needs to ensure that the consumer is protected

---

[132] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 42.
[133] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.
[134] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 51.
[135] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 51.
[136] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 52.
[137] Section 16 Consumer Protection Act. This section does not apply to transactions which Section 44 of the ECT Act applies to.[137] The consumer's right to the cooling-off period is not to interfere with the right to rescind in terms of industry dependant laws on rescinding purchases.
[138] Section 16 (3) Consumer Protection Act.

but it seems that the supplier may be put into an unfortunate position, since, the consumer may rescind without having to provide a reason or pay a penalty as long as the rescission is made in the prescribed manner.[139] The consumer is not the only party with a responsibility when a cooling-off period is being used. As the consumer rescinds the transaction, the supplier is compelled to return any payments received within the allocated time.[140]

2.3 Unsolicited Goods and Services

The main apprehension that consumers have concerning the direct marketing approach is that they spend unnecessary time handling the unsolicited goods or services.[141] This is because the consumer receives so-called junk mail,[142] spam and phone calls at inconvenient times. Spam is something that is not defined in South African legislation, however, spam is understood to be something a person receives whether they want it or not. Following this understanding it is logical that consumers are agitated by spam. Consumers want to have a choice and spam is something that they have no control over.

Many consumers seek to control whether their private details are on databases or not.[143] There seems to be a 'power' in being in control of that aspect. This is not surprising in light of the history of the majority of South African consumers. Research that has been done on the consumer's behavioural patterns concerning direct marketing indicate that younger consumers (aged 18 to 29 years old) are reluctant to purchase via mail because they are unaware of name removal procedures which are available; moreover less educated consumer are reluctant parties to direct marketing sales.[144] In the

---

[139] Section 16 (3) Consumer Protection Act.
[140] Section 16 (4) Consumer Protection Act.
[141] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.
[142] *America Online Inc v National Health Care Discount, Incorporated* 121 F.Supp..2d 1255 (N.D. Iowa 2000) Available at http://homepages.law.asu.edu/~dkarjala/cyberlaw/AOLv.NatHealthCare9-29-00.html (Accessed 13-01-2010).
[143] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 44.
[144] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 44.

same light, the direct marketer should allow the consumer to choose which direct marketing method is best suited for him or herself.[145]

If goods or services are found to be unsolicited they may be returned to the supplier at the supplier's cost. Goods and services will be categorized as unsolicited if during direct marketing of the goods or services a supplier or a representative of the supplier has left goods with the consumer or performed services for the consumer without requiring or arranging payment.[146] If any consumers receive unsolicited goods and they are aware that the good are unsolicited the consumer must not aggravate any means by which the supplier attempts to recover the goods.[147] Additionally the consumer does not have any responsibility to maintain the unsolicited goods.[148]

Once the consumer receives any direct marketing through electronic communication, the communication must contain the name of the sender and address which the consumer may use to unsubscribe.[149] When the details of the consumer's personal information is published, the marketer must inform the consumer of the intended inclusion and the intended purpose and use of the directory.[150] This allows the consumer to be aware of what is being done with their personal information and to remove their details if they would prefer to keep their personal information off any databases.

2.4 Secure Payment Methods

The ECT Act deals with consumer protection in Chapter VIII. One of the important concerns for the consumer in e-transactions is that the consumer may not be able to alter their choices once their goods or services are selected. However the ECT Act requires the consumer to be able to review their purchases or various transactions before providing

---

[145] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 51.
[146] Section 32 (2) read with section 21 (a) Consumer Protection Act.
[147] Section 21 (3) (a) Consumer Protection Act.
[148] Section 21 (3) (b) and (c) Consumer Protection Act.
[149] Section 66 (3) Protection of Personal Information Bill.
[150] Buys "New Laws to Restrict Marketing Activities" 2009 *Journal of Marketing Volume* Nov/Dec 28.

payment.[151] In truth, if the website does not allow for these e-vendor functions the consumer is entitled to rescind the transaction without notice or reason and without paying any penalty within 14 days of the transaction.[152] The ECT Act contains provisions for handling spam[153] and it is clear that any unsolicited goods, services or communications cannot create an agreement by itself.[154] Therefore, the consumer cannot be contractually liable due to unilateral terms and conditions set out in the unsolicited communication[155]- these provisions will be repealed once the POPI Bill becomes an Act.[156]

When payments are made electronically the ECT Act requires a secure payment system to be in place.[157] This is an important section for e-commerce because the consumer needs their private banking information to remain confidential. If the e-vendor fails to provide a sufficiently secure method for the consumer to make payments, any damages incurred by the consumer through the fault of the e-vendor's insufficient payment system will render the e-vendor liable.[158] The e-vendor will be liable for any damages that the consumer incurs due to the consumer's personal banking information being stolen or leaked negligently to a non-secure shopping environment which has been offered by the e-vendor[159]

2.5 The Consumer's right to Privacy in the CPA

The business of direct marketing is built on the consumer's private information. All this information is stored on the marketer's database, which is the reason that these databases are so valuable.[160] These details allow for the direct marketers to curtail their marketing

---

[151] Section 43 (2) Electronic Communication and Transactions Act, 2002.
[152] Section 43 (3) Electronic Communication and Transactions Act, 2002.
[153] Section 45 Electronic Communication and Transactions Act, 2002.
[154] Section 45 (2) Electronic Communication and Transactions Act 2002.
[155] Snail "The Rights of the e-consumers: Consumer Law" 2007 *Without Prejudice Vol 7 Issue 6 July* 18.
[156] Buys "New Laws to Restrict Marketing Activities" 2009 *Journal of Marketing Volume* Nov/Dec 28.
[157] Section 43 (5) Electronic Communication and Transactions Act, 2002.
[158] Snail "The rights of the e-consumer" 2007 *Without Prejudice* 18.
[159] Section 43 (6) Electronic Communication and Transactions Act, 2002.
[160] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.

strategy,[161] which allows for the direct marketer to approach consumers that has been selected due to consideration and examination of the consumer's interests.

How a consumer feels about their privacy will dictate a lot about their buying patterns. Several studies illustrate this point: when consumers are concerned about invasion or infringement of their privacy they are willing to alter their behavioural buying patterns.[162] This is a concern for both online and offline transactions.[163]Research illustrates that individuals are sceptical when confidential information and thus their privacy may be compromised.[164] However consumers are not as concerned about identity theft as they are about what the government as well as private organisations will do with the consumer's private information.[165]

2.5.1 Preventing Communication

The most important sections of the CPA for the purposes of the aforementioned discussion are section 11 and section 12. The consumer's right to privacy includes the right to refuse,[166] require another person to discontinue or to pre-emptively block any approach or communication with that person if the approach is for purposes of direct marketing.[167]

Due to the consumer's right to privacy, when a consumer is approached for the purposes of pursuing or demonstrating direct marketing options the consumer is well within his or her rights to demand that further communication not occur.[168] This is a valuable right for the consumer to prevent unwanted communications.

The wording "...within reasonable time after the communication..." is unclear as to the legislature's intentions.[169] It is peculiar that compared to other sections in the CPA

---

[161] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.
[162] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 44.
[163] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 44.
[164] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 42.
[165] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 42.
[166] Section 11 (1) (a) Consumer Protection Act.
[167] Section 11 (1) (b) and (c) Consumer Protection Act.
[168] Section 11 (2) Consumer Protection Act.
[169] Section 11 (2) Consumer Protection Act.

which are specific about time limits, this section makes reference to a 'reasonable' time limit.

In order to protect the consumer's privacy from unsolicited direct marketing procedures, the Minister of Trade and Industry is supposed to prescribe specific dates and times for when the consumer may be contacted.[170] This is for the consumer to preserve some privacy in their home from any promotional offers.[171]However, until the Minister prescribes the specific dates, days and times direct marketing can occur at any time.

2.6 Direct Marketing Regulation in South Africa

The Direct Marketing Association of South Africa (DMASA) is a body that aims to regulate and protect the direct marketing industry.[172] In order to do this the DMASA has to take both the consumer and the industry into consideration to safeguard them from unethical or ignorant practioners.[173] The DMASA is globally aligned and has strong ties throughout the network of direct marketing.[174]

Technology is growing at an advanced rate and subsequently the direct marketing industry is as well.[175] This is because direct marketing is becoming the more effective manner as well as the more economic option for the supplier to communicate with their consumer.[176]

---

[170] Section 12 (2) Consumer Protection Act.
[171] Section 12 (1) Consumer Protection Act..
[172] The Department of Trade and Industry "*The DMA is Essential for the Stability and Growth of Direct in South Africa*" Available at http://www.dmasa.org/core/index.php?option=com_content&view=article&id=54&Itemid=59 (Accessed 3-1-2010).
[173] The DTI "*Essential for the Stability and Growth*".
[174] The DTI "*Essential for the Stability and Growth*".
[175] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 42.
[176] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 42.

2.6.1 Advertising Playing a Role in Direct Marketing

Marketing is perceived to be separate from advertising.[177] However advertising will be considered in relation to its affect on direct marketing. On consideration of the "direct marketing" definition in the CPA, one of the elements of "direct marketing" is to "...promote or offer...". Therefore advertising is an element of direct marketing. In fact, it is a large part of direct marketing as it is one of the elements of the definition that is most susceptible to creating problems for the consumer. It is important to remember that advertising and marketing may overlap in many areas. An example is that an advert is merely an invitation to do business.[178]

The most effective way to educate consumers and thereby developing the markets is by use of advertising.[179] Actually advertising plays a valuable role in a modern developed society due to it being a source of information for the consumer.[180] Some have said that advertising is the icon of the modern consumer.[181] This is because advertising practices has been a central issue in consumer protection because it integrates economic and cultural aspects of the consumer marketplace.

In 1969 the advertising industry in South Africa assumed the moral and financial responsibility for monitoring itself. This organisation is the ASA. The ASA adopted a code (ASA code) based on the British Code of Advertising Practice and on the International Code of Advertising Practice which was prepared by the International Chamber of Commerce.[182] The European Advertising Standards Alliance (EASA) brings

---

[177] Dicey "Marketing vs. advertising: are the battle lines drawn? : advertising" 2008 *Journal of Marketing, Apr/May* 28.
[178] *Crawley v Rex* (1909 TS 1105).
[179] Woker *Advertising Law in South Africa* (1999) 1.
[180] Woker *Advertising Law* 7.
[181] Ramsey *Consumer Law* xiii.
[182] Woker *Advertising Law* 20.

together advertising bodies that self-regulate.[183] Even though South Africa is not a European country, they do form part of the EASA.[184]

The ASA is an independent body that regulates advertising in the public interest through self-regulation.[185] The ASA functions to ensure that advertising meets the standards set out in the ASA Code.[186] The ASA Code is accepted as the basis for self-regulation in the South African Advertising industry.[187] The ASA Code has two main purposes: protect the consumer and ensure that there is professionalism amongst advertisers.[188] The ASA Code is designed to complement other pieces of legislation not replace or contradict them.[189] The ASA Code expects all advertisers to respect individual privacy and susceptibilities.[190] This aim corresponds with the CPA and the thinking behind the POPI Bill.

The ASA Code deals with unsolicited home visits[191] which allows for advertising to be done at a consumer's home. The advertiser must provide the consumer with an opportunity to decline such visit or call.[192] Also, negative option selling is not encouraged by the ASA.[193]

---

[183] European Advertising Standards Alliance *"The EASA Advertising Self Regulatory Charter"* available at http://www.easa-alliance.org/About-SR/Charter-Validation/page.aspx/237 (Accessed 15-01-2010).

[184] Advertising Standards Authority of South Africa *"International Ties"* available at http://www.asasa.org.za/Default.aspx?mnu_id=18 (Accessed 15-01-2010).

[185] Advertising Standards Authority of South Africa *"Home"* found at http://www.asasa.org.za/Default.aspx?mnu_id=95 (Accessed 15-01-2010).

[186] Advertising Standards Authority of South Africa *"Preface"* found at http://www.asasa.org.za/Default.aspx?mnu_id=12 (Accessed 15-01-2010).

[187] ASASA *"Preface"*.

[188] ASASA *"Preface"*.

[189] ASASA *"Preface"*.

[190] ASASA *"Preface"*.

[191] Advertising Standards Authority of South Africa *"Section VI-Marketing"* http://www.asasa.org.za/Default.aspx?mnu_id=39 (Accessed 15-01-21).

[192] ASASA *"Section VI-Marketing"*.

[193] ASASA *"Section VI-Marketing"*. Negative option selling is when an agreement between the supplier and the consumer automatically comes into existence because the consumer fails to decline the inducement made by the supplier, Section 31 Consumer Act.

The ASA's Code interprets direct sales advertising to be when a product or service is advertised to be sold at or provided for in the home of the consumer.[194] This has similar connotations as the "direct marketing" definition in the CPA.

Protecting the individual is important to the ASA however they exist for the consumer and the advertisers to be able to get what they want while maintaining a balance. The ASA has a powerful and far-reaching influence on South African companies and how they handle their marketing and branding.[195]

2.6.2 Direct Marketing: Opting In or Out

Some consumers are wary of providing their private information for marketing lists because they may battle to remove their details. Thus an "opt out" list has been created. In 2007 DMASA launched an "opt out register". Once a consumer has registered themselves on the "Don't Contact Me" list all direct marketers need to compare their list of consumers against the "Opt out Register".[196]

In addition DMASA will be launching an "opt in" list.[197] This will be a list which consumers will choose to be put on because they would like to receive information pertaining to certain products or services.[198] This will be easier for the consumer because they would have chosen their categories and interests. Most importantly, the consumer would choose what private information he or she wants to disclose. The consumer should view this as an attractive option because the consumer will be able to select the means of communications. The "Opt in" list appears to hold many solutions to the consumer's unwanted direct marketing issues. Maintenance of this list will be difficult for the DMASA but with proper planning and implementation it may be feasible.

---

[194] ASASA "*Section VI-Marketing*".
[195] Van Wyk & Botes "Misleading: Advertising" 2009 *Without Prejudice Volume 8, Issue 10, Nov* 41.
[196] Direct Marketing Association of SA "*Opt* in" Available at http://www.dmasa.org/core/index.php?option=com_content&view=article&id=74&Itemid=68 (Accessed 12-01-2010).
[197] DMASA "*Opt in*".
[198] DMASA "*Opt in*".

2.7 Concerns Affecting Direct Marketing

There were concerns over the Consumer Protection Bill (CP Bill), which may still be applicable to the CPA. An example is that the legislature has been accused by some to have deterred from the basics of contract law in order to protect the consumer.[199]

Not all direct marketing is undesirable. Usually once the consumer overcomes their initial apprehension about the direct marketers' privacy policies and practices the consumer will then appreciate the benefits of that relationship.[200] This is because the marketer can then curtail their marketing objectives to meet the consumer's wants, needs and interests. Building a relationship with the marketer will be to the benefit of the consumer.[201]

Even though some consumers are aware of the possible privacy risks concerned with direct marketing they tend to continue to participate. This is because the consumer believes that the benefits outweigh the risks of the sale.[202] It appears that the more time the consumer spends engaging in direct marketing the more the consumer becomes aware of the exposure he or she has encountered and develops a more favourable attitude toward the direct marketing approach. Organisations are aware of these privacy concerns that the consumer has yet many ignore these concerns instead of curtailing their privacy policies and practices.

Although there is a great concern worldwide over the consumer's right to information privacy the effect on South African consumers is still not clear.[203]

Interestingly it seems that consumers are more comfortable with online sales than traditional sales methods. This is likely because online direct marketing has less reported crimes.[204] Although due to the growing rate of e-commerce the main concern surrounding

---

[199] Schimmel "In the Beginning: Advertising" 2009 *Without Prejudice Volume 1 Issue 1 Feb* 7-8.
[200] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.
[201] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 43.
[202] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 44.
[203] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 45.
[204] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 50-51.

the marketing environment is on the World Wide Web.[205] This is because the internet has ways of tracking and creating personal profiles and often these profiles are created without the user being aware of what is happening.[206] Computers can keep record of sites visited, which are the most popular and what information the consumer provides to that particular site.

A problem for the consumer is that courts have been uninterested to intervene in consumer contraventions.[207] It is because of that thinking that the consumer has often been left in vulnerable positions. Obviously crimes such as rape, robbery and murder are worse contraventions of laws but that does not mean that the consumer needs to be left to be disadvantaged. Although consumer problems may be mundane when being compared to heinous crimes but consumer matters often leave the people in the lower income bracket the most exposed. [208]

The CPA allows for a registry which may be maintained to keep a list of which consumers do not want to be bothered with direct marketing[209] (as discussed above). The body which holds the Registry may not charge a consumer for making a demand or registering a pre-emptive block. This means that the costs for maintaining the registry need to be carried by either the direct marketer, an organisation such as the DMASA or the government. If the government is the party to carry the cost inevitably it is the consumer paying for the service through their taxes.

Any persons authorising, directing or controlling any direct marketing needs to ensure that the appropriate procedures to facilitate the demands which will come are implemented.[210] This may be problematic for the direct marketers as this will increase expenditure to maintain the appropriate procedures. Also the implemented procedures need to be maintained by skilled workers - this is another expense.

---

[205] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 51.
[206] Jordaan "Information Privacy Issues" 2007 *International Retail and Marketing Review* 51-52.
[207] An example can be found in *S v Pepsi-Cola (Pty) Ltd* 1985 (3) SA 141 (C) 142. Here the Van Heerden J was surprised that an alleged contravention of the Gambling Act 51 of 1965 was being investigated when there were more heinous crimes occurring.
[208] Woker *Advertising Law* 13.
[209] Section 11 (3) Consumer Protection Act.
[210] Section 11 (4) (a) Consumer Protection Act.

Once the provision concerning regulation of direct marketing in relation to dates, days and times has been decided by the Minister and once the provisions are contravened the National Consumer Commission (NCC) is responsible to enforce it. There are various means for the NCC to enforce the Act.[211] Some of the activities that the NCC has to complete to enforce the CPA are: a) receiving and accordingly exploring complaints about contraventions of the CPA[212] and b) investigate and evaluate the complaints.[213]Also the NCC has to monitor the market in order to be updated on possible consumer activities which may lead to the CPA being contravened.[214] Once the NCC has investigated and issued a compliance notice, in accordance with section 100 of the CPA, any failure to comply will be considered an offence.[215] Penalties for contravention of the CPA vary according to the contravention.[216] In addition the NCC must monitor the organisations that are assisting in the regulation of the consumer market[217]and where necessary the NCC must refer matters which go beyond the scope of the NCC to the appropriate bodies.[218]

It was predicted that the over-regulation of consumer sectors will result in increased costs due to large administrative burdens that the CPA has put in place.[219] Although the CPA is less extensive than the Consumer Protection Bill there are still a lot of administrative burdens placed on companies and organisations in order for them to be CPA acquiescent. These costs will be passed onto the consumer at a later stage.[220] There is a belief that the funds that will be used to implement the CPA should rather be spent educating the consumer about devious business practices.[221]

---

[211] Section 99 Consumer Protection Act.
[212] Section 99 (b) Consumer Protection Act.
[213] Section 99 (d) Consumer Protection Act.
[214] Section 99 (c) (i) Consumer Protection Act.
[215] Section 110 (2) Consumer Protection Act.
[216] Section 111 Consumer Protection Act.
[217] Section 99 (c) (ii) Consumer Protection Act.
[218] Section 99 (g), (h) and (i) Consumer Protection Act.
[219] Lee & Du Plessis "The Consumer Protection Bill" 2006 *Journal of Marketing* 3.
[220] Lee & Du Plessis "The Consumer Protection Bill" 2006 *Journal of Marketing* 3.
[221] Lee & Du Plessis "The Consumer Protection Bill" 2006 *Journal of Marketing* 3.

3 PROTECTING THE CONSUMER'S PERSONAL INFORMATION

3.1 The Need for Privacy Protection

Protecting the individual's personal information has become increasingly difficult as time passes. This is because society is changing and one of the leading factors affecting society's rapid transformation is the growing rate of technology. Privacy is a valuable and advanced aspect of personality which is the reason it requires great protection.[222]

A person's right to privacy means that a person should be allowed control over his or her personal information and therefore is capable of conducting his or her affairs free from unwanted intrusions.[223] Unfortunately some information will enter the public domain whether the consumer wants that information to be available to the public or not.

However individuals cannot solely depend upon the State to protect their privacy because interpretation of legislation may be detrimental to them. This means that even though all judges use the same legislation, they may interpret the law differently.[224]

The right to privacy has to be balanced between the individual and the public or the State. The right should protect the individual's privacy but must be balanced against the legitimate interests of others that need to obtain information about the individual.[225] However, this is unlikely to be problematic for the consumer when dealing with unsolicited communications from marketers.

---

[222] SALRC "*Privacy and Data Collection*" i 1.

[223] *National Media Ltd ao v Jooste* 1996 (3) SA 262 A 271-272.

[224] An example of this is the *Campbell v MGN Limited* case where the judge allowed for the appellant's right to privacy to be infringed because he believed that she had exposed herself by using her celebrity status. In *Campbell (Appellant) v MGN Limited (Respondents)* [2004] UKHL 22 Available at http://www.publications.parliament.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm (Accessed 30-09-2009).

[225] Deneys Reitz Attorneys "Protection of Personal Information" 21-09-2009 Available at http://www.deneysreitz.co.za/index.php/news/protection_of_personal_information (Accessed 17-01-21).

The mere collection and storage of information may constitute an infringement of an individual's right to privacy if it is preceded by unreasonable procedures. A further and possibly a more serious infringement may occur where information relating to an individual is compiled in such a manner that begins to answer questions about that person, providing surveillance of his or her private behaviour.[226] This practice is referred to as information matching or profiling.[227]

Profiling is the process of inferring a set of characteristics (typically behavioural) about an individual and then treating that individual in light of these characteristics.[228] This is not an offence. However the problem which arises with information profiling is that some information may be used to make direct links back to the consumer. This is an invasion of the consumer's privacy.

Privacy is more of a concern for the consumer because he or she is the party that is exposed. Organisations which utilise the consumer's personal information are not affected if the integrity of the information is compromised. The protection of information privacy provides a general limit for people gaining, publishing, disclosing or using information about others without their consent. This allows individuals to control who communicates with them and who has access to their information.[229]

3.2 Current Protection Available for the Consumer's Privacy

The right to privacy is not only regulated by the Constitution [230] but the common law as well. However the constitutional right to privacy has had a limited impact on the consumer's data privacy protection. The common law recognizes personality rights which are rights to privacy, dignity, good name and bodily integrity.[231] This means that if

---

[226] SALRC "*Privacy and Data Collection*"93 5.7.1.
[227] SALRC "*Privacy and Data Collection*"93 5.7.1.
[228] SALRC "*Privacy and Data Collection*" 94 5.7.4.
[229] SALRC "*Privacy and Data Collection*" 13.
[230] Section 14 Constitution of the Republic of South Africa, 1996.
[231] *Stoffberg v Elliot* 1923 CPD 148; *Lymbery v Jefferies* 1925 AD 235; *Lampert v Hefer* 1955 (2) SA 507 (A); *Esterhuizen v Administrator, Transvaal* 1957 (3) SA 710 (T)).

consumers need to enforce their right to privacy using the common law, he or she would have to ensure the infringement affects the narrow rights set out above. However none of the traditional common law principles are directly related to information privacy.

Apart from the Constitution, there is no apposite legislation which deals specifically and fully with information protection. Considering the extent and seriousness of the threat to the individual's personality, it is surprising that South Africa's measures to protect the individual information protection have not been enacted yet. [232]

The Constitutional Court has emphasised the indispensable link between the common law and constitutional right to privacy.[233] Although, due to the dependency between the common law and the Constitution there is still apprehension around the degree to which the Bill of Rights has application in common law disputes.

In *Mistry v Interim Medical and Dental Council of South Africa*[234] the court held that even though breach of informational privacy was not expressly provided protection in Section 13 of the interim Constitution[235] (which is subsequently Section 14 the Constitution), it would be covered by the broad protection of the right to privacy guaranteed by Section 13. Therefore the list in Section 14 of the Constitution is not completely dogmatic by way of application.

The right to privacy is not absolute. As a fundamental right it can be limited in accordance with the limitation clause of the Bill of Rights.[236] Each limitation of the right to privacy is case dependant and the opposing interests or rights will have to be considered.[237]

---

[232] SALRC "*Privacy and Data Collection*"1.
[233] *Bernstein ao v Bester NO ao* 1996 (2) SA 751 (CC); 1996 (4) BCLR 449 (CC) at 787.
[234] *Mistry v Interim Medical and Dental Council of South Africa ao* 1998 (4) SA 1127(CC); 1998 (7) BCLR 880 (CC) 14.
[235] Interim Constitution of the Republic of South Africa Act 2, 1994.
[236] Section 36 Constitution of the Republic of South Africa, 1996.
[237] SALRC "*Privacy and Data Collection*"16.

3.2.1 Legislation

In South Africa, section 51 (1) of the ECT Act provides a regime, whereby consent for processing the consumer's information is required from the data subject, unless the data controller (responsible party) is required or permitted by law to process the information.[238]

The PAIA[239] which was enacted to give effect to Section 32(2) of the Constitution (discussed in Chapter Two) provides that the responsible party must, on the data subject's request, allow the data subject reasonable access to his or her information records. This entitlement of access[240] is necessary for effective and equitable control of information. Only that person will be able to ascertain whether the information is correct and necessary for the purposes of processing and for the protection of a legitimate interest. However there may be exceptions to the right of access to information in particular circumstances.[241]

3.3 The International Influence

Transparency is a primary condition for effective information protection. Internationally, the responsible parties are enjoined to be open about their processing activities.[242] This obligation may include the requirement to inform (and to receive authorisation from) the supervisory authority of their processing activities.[243]

This area of law has become a major issue worldwide but has still lacked suitable regulation. This is the reason the South African Law Commission (SALC) drafted the POPI Bill. The EU has a directive called the Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data

---

[238] SALRC "*Privacy and Data Collection*" 26 4.2.43.
[239] Promotion of Access to Information Act 2 of 2000.
[240] Section 11 (public bodies) and 50 (private bodies) of PAIA, 2000 for the right of access to records.
[241] SALRC "*Privacy and Data Collection*" 89 4.2.197.
[242] Principle 6 of the OECD Guidelines.
[243] SALRC "*Privacy and Data Collection*" 68 5.5.1.

and on the free movement of such data (EU Data Directive)[244] to protect personal information of the consumer which is on a database from being abused. This will be discussed in more detail in Chapter Four

The modern international privacy benchmark is in the 1948 Universal Declaration of Human Rights, which specifically protects territorial and communications privacy.[245]

During the drafting of the POPI Bill there were two international instruments that were extremely influential. They are the Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CoE Convention) and the 1981 Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.[246] These agreements are valuable as they contain technology neutral principles. The OECD Guidelines provides eight information protection principles.[247]

The UN Guidelines indicate the need for national states to establish national data protection authorities that are impartial, independent and technically competent.[248] Some recognition should be taken of the UN Guidelines. The United Nations' Guidelines Concerning Computerised Personal Data Files (hereafter termed UN PD Guidelines) were adopted by the UN General Assembly in 1990.[249] The UN PD Guidelines are intended to encourage those UN Member States without information protection legislation in place to take steps to enact such legislation based on the UN PD Guidelines. The UN PD Guidelines are aimed at encouraging governmental as well as non-governmental organisations to process personal data in a responsible, fair and privacy-

---

[244] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[245] Universal Declaration of Human Rights, 1948.
[246] SALRC "*Privacy and Data Collection*"v.
[247] SALRC "*Privacy and Data Collection*" 5 4.1.13.
[248] SALRC "*Privacy and Data Collection*" 7 5.2.8.
[249] United Nations' Guidelines Concerning Computerised Personal Data Files Doc E/CN.4/1990/72, 20.2.1990.

friendly manner. The UN PD Guidelines are not legally binding and seem to have had little influence on information regimes.[250]

The formulation of the code for fair information practices is derived from several sources, including codes developed by the OECD (1980), the CoE (1981) and EU Data Directive (1995).[251] One should remember that the codes are guidelines which still require interpretation to be done by countries to suit their own position.[252] However it was emphasised that the real test will lie in the implementation of the principles and that the degree to which these principles are adopted will be dependant on the cost of implementing them.[253]

Due to the fact that the POPI Bill has been modelled according to the EU's model (to be discussed in Chapter Four) the POPI Bill is in line with international practices.[254] However it is still not certain that South Africa has the financial resources to implement the 'adequate' protection required by the EU to comply with the trade standards.

3.4 The POPI Bill

The main reason the POPI Bill has been enacted is that the SALC wants to provide protection for the data subject's personal information and for the data subject to be able to maintain some control over the information.[255] The POPI Bill has been recommended to become an Act because there was a shared belief amongst the Ministry that existing privacy laws were too scattered.[256]

---

[250] SALRC "*Privacy and Data Collection*" 11 4.1.29.
[251] SALRC "*Privacy and Data Collection*" 14 4.2.3.
[252] SALRC "*Privacy and Data Collection*" 14 4.2.3.
[253] SALRC "*Privacy and Data Collection*" 16 4.2.114.
[254] Reinhart "New Laws to Restrict Marketing Activities" 2009 *Journal of Marketing Volume* Nov/Dec 28.
[255] Bortz &Ginsburg *Object of the Bill* Available at http://www.rhp.co.za/protection_bill.html (Accessed 17-01-2010).
[256] Varney, *Protection of Information Bill Briefing* Available at http://www.pmg.org.za/report/20080611-protection-information-bill-briefing (accessed 2 October 2009).

In fact, the right to privacy includes the right to protect against unlawful collection, retention and dissemination of the consumer's personal information.[257] Although the individual's privacy must be maintained in terms of the Constitution, the POPI Bill must regulate to harmonise with international standards.[258]

The POPI Bill will regulate the activities and use of other people's personal information while considering the constitutional right to privacy.[259] It seems as though Parliament has decided to approach the issue of spam which was not adequately dealt with in the ECT Act by legislating on spam in the POPI Bill.[260]

An additional aim of the POPI Bill is to provide for the rights of persons regarding unsolicited electronic communications and automated decision making and to regulate the flow of personal information across the borders of the Republic. Also, the purpose of the POPI Bill is to give effect to the overriding constitutional right to privacy within justifiable limits. This is to balance your privacy rights against other fundamental rights as well as to protect important interests around the Republic and across international borders.[261] There is also a general outcry for one to protect his or her own personal information and for the consumer to be aware of what he or she allows into the public sphere.[262]

There seemed to be a concern that there is a considerable amount of confusion over the roles and responsibilities for Information and Communications Technology (ICT) in the South African government departments. Currently at least seven public service agencies have a role to play in government ICT issues.[263] The POPI Bill also

---

[257] Preamble of the Protection of Personal Information Bill.
[258] Preamble Protection of Personal Information Bill.
[259] Buys "New Laws" 2009 *Journal of Marketing Volume* 28.
[260] Michalson "Protection of Personal Information Bill - The Implications For You" 24 August 2009 *Online Legal Available* at http://www.michalsons.co.za/protection-of-personal-information-bill-the-implications-for-you/3041?gclid=CMO8ucWqq58CFY8A4wodpQxw1g (Accessed 17-01-2010).
[261] Section 2 (1) (a) Protection of Personal Information Bill.
[262] Section 2 (1) (b) and (d) Protection of Personal Information Bill.
[263] a)The Department of Public Service and Administration (DPSA) which has responsibility for developing ICT policies for the public service as a whole;
b) The Public Service Commission (PSC) which has the responsibility of monitoring those policies;

introduces an Information Protection Regulator.[264] This Regulator is referred to throughout the POPI Bill and will play a large role in the exchange of personal information data between the responsible party and the data subject.

The POPI Bill deals with unsolicited electronic communications.[265] This section allows for the marketer to only communicate with consumers through direct marketing methods once consent has been obtained from the consumer.[266] Also the communication may only be sent if the personal information of the consumer was obtained in the same context of the sale of goods and services, this means that the marketer cannot sell, trade or pass on any of the consumer's personal information without the consent of the consumer.[267]

The POPI Bill has eight information protection principles (IP Principles) which must be followed by all responsible parties. These principles are: accountability, processing limitation, further processing limitation, purpose of collection to be specified, information quality, openness, security safeguards and data subject participation.

The accountability principle[268] imposes a responsibility on the responsible party to ensure that the IP Principles are adhered to.

---

c) The National Treasury which has the responsibility of supervising the main transversal systems and managing the Central Computer Services (CCS) (now part of SITA);
d) The Department of Trade and Industry (DTI) which has a responsibility for promoting the IT industry;
e) The Department of Communications (DoC) which has been given the responsibility to act as secretariat for the development of an ICT strategy for the country with the ultimate responsibility for such a strategy being vested in the Deputy-President's Office (ODP);
f) The State Information Technology Agency which has as its objective to provide information technology, information systems and related services in a maintained information systems security environment to, or on behalf of, participating departments and organs of state.
g) The Department of Arts, Culture, Science and Technology which has been charged with developing the technology foresight study of ICT in South Africa.
h) Auditor General which has been charged to ensure compliance and certification of these policies and framework.

[264] Protection of Personal Information Bill.
[265] Section 66 Protection of Personal Information Bill.
[266] Buys "New Laws" 2009 *Journal of Marketing Volume* 28.
[267] Buys "New Laws" 2009 *Journal of Marketing Volume* 28.
[268] Section 7 Protection of Personal Information Bill.

The processing limitation principle entails that the personal information must be processed within a lawful manner and reasonable measures must be taken to protect the individual's privacy.[269] Also the purpose must provide the reason that the personal information is required.[270] Once the purpose is disclosed, the data subject can disclose relevant information. However consent from the data subject is required.[271] Collections must be made directly from the data subject,[272] subject to certain exemptions where there is a need to confer with outside resources,[273] the data subject has consented to it[274] or said information is in the public domain.[275]

Another principle is that the purpose of the collection must be explicitly specified and lawful.[276] The data subject must be aware of the above purpose specification.[277] This principle provides guidance as to when the records must be retained and such records must be destroyed within a reasonable time after the information is no longer needed.[278]

In addition there is a further processing limitation principle. This requires that the processing of the personal information needs to be aligned with the purpose of the collection.[279]

The information quality principle requires that the information is complete, accurate, not misleading and continuously updated with the removal of irrelevant details.[280]

Furthermore the openness principle creates an obligation for the responsible party to notify the data subject as well as the Information Protection Regulator.[281] This will be

---

[269] Section 8 Protection of Personal Information Bill.
[270] Section 9 Protection of Personal Information Bill.
[271] Section 10 (1) Protection of Personal Information Bill.
[272] Section 11 (1) Protection of Personal Information Bill.
[273] Section 11(2) (c), (d) and (e) Protection of Personal Information Bill.
[274] Section 11 (2) (b) Protection of Personal Information Bill.
[275] Section 11 (2) (a) and (f) Protection of Personal Information Bill.
[276] Section 12 Protection of Personal Information Bill.
[277] Section 13 Protection of Personal Information Bill.
[278] Section 14 Protection of Personal Information Bill.
[279] Section 15 Protection of Personal Information Bill.
[280] Section 16 (1) Protection of Personal Information Bill.

an imposition on the responsible party due to the fact that a lot of administration will be required to keep the Regulator and data subject updated. Requiring the responsible party to update two different parties is extremely burdensome. It is not necessary to update the data subject in certain circumstances named in Section 17 (6) of the POPI Bill. However, some of these grounds for non-compliance with notifying the data subject are left to be interpreted subjectively by the responsible party.[282]If there is an investigation surrounding the data subject's personal information, the data subject must be informed during and once the investigation is complete,[283] unless the Regulator does not think that it is necessary to inform the data subject.[284]

The security safeguards principle requires that security measures which are explained in the POPI Bill will have to provide for the integrity of the personal information to be maintained.[285] Any person who handles the personal information needs to have the requisite authority.[286] Confidentiality and respect for the contents of the personal information must be maintained by all persons who handle the information.[287] The responsible party must ensure that the operator who processes the information must take all reasonable steps to comply with the laws surrounding the protection of personal information.[288] If the security of the personal information has been compromised the responsible party needs to notify the data subject and the Regulator.[289] This notification needs to be done in a timely fashion subject to certain exceptions[290] found in the POPI Bill. Therefore the data subject may take any necessary preventative measures in order to protect him or herself.[291]

---

[281] Section 17 (1) and (2) Protection of Personal Information Bill.
[282] Section 17 (6) (b) Protection of Personal Information Bill. "non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act".
[283] Section 89 Protection of Personal Information Bill.
[284] Section 89 (a) Protection of Personal Information Bill.
[285] Section 18 Protection of Personal Information Bill.
[286] Section 19 (a) Protection of Personal Information Bill.
[287] Section 19 (b) Protection of Personal Information Bill.
[288] Section 20 Protection of Personal Information Bill.
[289] Section 21 (1) Protection of Personal Information Bill.
[290] Section 21 (3) Protection of Personal Information Bill.
[291] Section 21 (5) Protection of Personal Information Bill.

Finally the data subject participation principle allows for the data subject to inquire which third parties have accessed his or her personal information.[292] Also, a data subject may require the responsible party to alter or delete any information that is inaccurate, false or out of date.[293] The responsible party must notify the data subject with reasonable proof that the request was carried out and what has happened to said information.[294] Importantly, the PAIA will apply.[295]

There are certain exceptions and exemptions for there to be a deviation from the IP Principles.[296] The enforcement of the IP Principles is to be done by the Information Protection Commission.[297] The manner of enforcement is found in Chapter 10 of the POPI Bill.

The POPI Bill creates an 'Opt in' policy. This is illustrated through Chapter Eight of the POPI Bill. This is because if the data subject, who is the person to whom the data relates, does not respond to the responsible parties', for example the direct marketer, direct marketing options the responsible party may no longer send the data subject direct marketing options. This is different to the CPA because the CPA has an 'Opt out' policy (as discussed in Chapter Two). However, the POPI Bill's handling of unsolicited communications is more suitable. The 'Opt in' option is already being implemented by the DMASA, as discussed in Chapter Two.

Another issue in the POPI Bill concerns the supplier or marketer. The POPI Bill, as it stands is not difficult to implement for the consumer but implementation for the marketer will be a challenge. This is because the POPI Bill contains specified methods, documentation and systems to be implemented by the marketer for the use of the data. [298]

---

[292] Section 22 Protection of Personal Information Bill.
[293] Section 23 (1) Protection of Personal Information Bill.
[294] Section 23 (2) and (4) Protection of Personal Information Bill.
[295] Section 24 Protection of Personal Information Bill.
[296] Chapter III Part B and Chapter IV Protection of Personal Information Bill.
[297] Section 34 Protection of Personal Information Bill.
[298] Michalson "Implications for You" 2009.

The responsible party may face certain problems when implementing the information principles such as the owner of the information base incurring additional costs to comply with the information legislation; this could also mean that the responsible party may end up paying large penalty amounts for poor or non-compliance.[299]

The POPI Bill contains a provision for cross-border data transfers.[300] This section requires that the recipient of personal information about the data subject, in a foreign country, be subject to laws that are similar to South Africa's information protection principles.[301] The data subject must consent to the personal information being sent to a foreign third party.[302] The transfer of the information must be required in terms of pre-contractual or contractual terms between the data subject and the responsible party,[303] or the responsible party and the third party in a foreign country.[304] Also the transfer of information must be to the benefit of the data subject.[305]

Those marketers that fail to comply with the provisions of the POPI Bill may face civil liability[306] and criminal fines.[307] The failures to comply with the POPI Bill will be handled by the Privacy Regulator.[308] The marketers need to consider the CPA and the POPI Bill thoroughly to ensure that they are not subject to unnecessary fines for non-compliance.[309]

---

[299] SALRC "*Privacy and Data Collection*" 19 5.2.31.
[300] Chapter 9 Protection of Personal Information Bill.
[301] Section 69 (a) Protection of Personal Information Bill.
[302] Section 69 (b) Protection of Personal Information Bill.
[303] Section 69 (c) Protection of Personal Information Bill.
[304] Section 69 (d) Protection of Personal Information Bill.
[305] Section 69 (e) Protection of Personal Information Bill.
[306] Section 94 Protection of Personal Information Bill.
[307] Buys "New Laws" 2009 *Journal of Marketing Volume* 28.
[308] Buys "New Laws" 2009 *Journal of Marketing Volume* 28.
[309] Buys "New Laws" 2009 *Journal of Marketing Volume* 28.

3.5 Comments

It was argued by the South African Law Reform Committee (SALRC) that a clear distinction needs to be established between the use of personal information for marketing of services and products, and its use for processing product applications, verification of personal details, credit assessment, fraud prevention and statutory reporting obligations.[310]

Often the consumer is left frustrated by the direct marketing activities that he or she receives. This is why the SALRC discussed that an opt-out approach represents a proportional balance between the consumer's privacy being protected and the actuality that modern business marketing strategies require to optimise business opportunities.[311] Also the SALRC believed that this approach is similar to the approach suggested in Article 14 of the EU Data Directive in respect of the data subject's right to object. The main objective of the opt-out approach is that consumers should be able to opt out of direct marketing procedures at any time subject to reasonable limits.[312] Once again, this illustrates the consumer's need to have some of control over circumstances where their personal information is utilised.

It was, however, noted that the question about opt-in *versus* opt-out is one that has become contentious in recent years, due to the USA's recent federal legislation about spam.[313]

Harris' view on the opt-out policy which was considered by the SALRC illustrates how the opt-out approach has the potential to become extremely burdensome on the consumer. This is because the consumer may feel overwhelmed by the number of received e-mails that cloud out the consumer's employee responsibilities because of time spent opting-out of spam.[314]

---

[310] SALRC "*Privacy and Data Collection*"28 4.2.47.
[311] SALRC "*Privacy and Data Collection*"29 4.2.48.
[312] SALRC "*Privacy and Data Collection*"29 4.2.48.
[313] SALRC "*Privacy and Data Collection*"29 4.2.49.
[314] SALRC "*Privacy and Data Collection*"29-30 4.2.50.

Transparency between the consumer and the marketer needs to exist. Therefore the consumer needs to be aware of the activities which surround his or her information. This is the reason the consumer needs to be notified of activities affecting his or her personal information. The consumer receiving notification appears to serve three main purposes.[315] It illustrates transparency in respect of the processing of personal information and can be the starting point for lodging a complaint with the competent authorities. Also it is helpful for the responsible parties in order to raise their awareness of notification duties and keeps them updated with compliance of information protection requirements and lastly it is helpful for information protection authorities because it allows them to keep abreast of the information processing situation in their countries.

The SALRC is of the opinion that the PAIA does not deal with correction[316] sufficiently and therefore it should be dealt with in a more comprehensive manner in the POPI Bill. This will allow for individuals to view all information that is collected about them and they must be able to alter incorrect information[317]

The benefits of the POPI BILL which were identified by the SALRC are that consolidating the national information protection legislation will provide a consistent approach to privacy and information protection across all sectors of the economy. Also the legislation will provide guidance and clarity in the regulatory and legislative environments pertaining to privacy and information protection. However, it is believed that the current legal conditions are hampered by legal uncertainty.[318] The POPI Bill will also create an overall stable and investment-friendly regulatory and legislative framework which will be beneficial to the South African economy.[319]The POPI Bill will give effect to both the common law and the Constitution in recognising the protection of the right to privacy.[320]

---

[315] SALRC "*Privacy and Data Collection*" 70 5.5.10.
[316] Section 88 Promotion of Access to Information Access.
[317] SALRC "*Privacy and Data Collection*"89 4.2.198.
[318] SALRC "*Privacy and Data Collection*" 32-33 5.3.4.
[319] SALRC "*Privacy and Data Collection*" 32-33 5.3.4.
[320] Section 14 Constitution of the Republic of South Africa, 1996.

Most of the POPI Bill commentator's feet that security issues should form part of the new privacy legislation.[321] However, some believe that security issues have been adequately addressed in other legislation.[322]

The appointment of a commissioner to act as a policeman in ensuring compliance with information privacy legislation was not completely supported. Creating a bureaucracy to monitor information privacy legislation would not be in the best interests of South Africa, because, unlike first world countries, South Africa has neither the economy nor infrastructure to effectively operate such a system.[323] This should be considered when investigating the POPI Bill as South Africa's economy is not in the best state and further impediments made on the National Budget will result in citizens being unhappy.

The Commission did not regard the self-regulatory system to be a suitable system for South Africa.[324] Also it is envisaged that a single statutory regulatory authority will be able to administer both the information privacy legislation and the access to information legislation.[325]

Generally there is no real objection to the compiling of statistical information and profiles from personal information, where it is not possible to trace the personal information of any identifiable individual from such profiling.[326] Profiling continues to be a valuable marketing tool.[327] If personal information is being used for this purpose

---

[321] SALRC "*Privacy and Data Collection*"77 4.2.172.
[322] SALRC "*Privacy and Data Collection*" 77 4.2.172.
[323] SALRC "*Privacy and Data Collection*"48 5.3.41.
[324] SALRC "*Privacy and Data Collection*"57 5.4.4.
[325] SALRC "*Privacy and Data Collection*" 57 5.4.4.
[326] The Internet Service Provider (ISPA) says that in practice internet users are uniquely identifiable by the IP (Internet Protocol) address, which is assigned to them when they connect to the Internet. While it may not be immediately practical or possible for any third party to tie that IP address to a name and address, it is technically possible to track that IP address as the person 'surfs the web'. Some advertisements leave a cookie on your computer, which is an additional level of unique identification, and this cookie can be used to harvest personal information and surfing habits. In the same measure, by merely accessing the image of an online advert, you are leaving an 'imprint' of your IP address in a log on a web server.
[327] SALRC "*Privacy and Data Collection*" 94-95 5.7.

without the consent of the data subject it should constitute an unacceptable infringement on his or her privacy.[328]

As was accepted by the SALRC, the ease with which electronic data flows across borders leads to a concern that information protection laws could be circumvented by simply transferring personal information to other countries, where the national law of the country of origin does not apply. This information could then be processed in those countries, frequently called "information havens," without any limitations.[329] It is for this reason that Article 25 of the EU Data Directive imposes an obligation on member states to ensure that any personal information relating to European citizens is protected by law when it is exported to and processed in, countries outside Europe[330]

It is unlikely, that 'data havens' will apply in South Africa.[331] It may be understood that the EU's approach to protection of databases are strict. But that would not be problematic for South Africa once the POPI Bill has been enacted. The POPI Bill allows for South Africa to be able to be a competitive trader in the economic field. South Africa has similar provisions in their domestic laws to the EU, so that, the Safe Harbor Principles will be complied with.

The SALRC suggested that South Africa's local procedures should operate being wary of the problems experienced in the EU with regard to enforcement.[332] It was suggested that a forceful system be put in place to assist data subjects, with the regulatory authority having sufficient power to curtail non-compliance.[333] However, only once the POPI Bill has been enacted will the implications of this apparent robust approach be made clear.

---

[328] SALRC "*Privacy and Data Collection*" 96 5.7.10.
[329] SALRC "*Privacy and Data Collection*"359 7.1.
[330] SALRC "*Privacy and Data Collection*" 359 7.2.
[331] Privacy "*International "Overview.*
[332] SALRC "*Privacy and Data Collection*" 39 5.3.17.
[333] SALRC "*Privacy and Data Collection*" 39 5.3.17.

A general privacy act was proposed to constitute a generic framework to apply across different industries. It was suggested that the overriding legislation should not be too specific and subsequently too restrictive in its impact. For that reason, the definitions in that Act should be wide and generic in nature, and should only contain the general principles. The POPI Bill does contain wide provisions but is not as general as envisaged by some of the members and commentators of the SALRC. This is because the DTI did not want the POPI Bill to be too general that it opens floodgates for unnecessary prosecutions.

4 COMPARATIVE JURISDICTIONS: THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA

In order to comprehend the possible success rate for South Africa's new legislation to protect the consumer's right to privacy, international laws and standards must be considered. As illustrated in previous chapters, the South African legislature has been influenced by international conventions. However, Chapter Four will deal primarily with the EU and the US laws for protection of the consumer's right to privacy. These international laws will be investigated because implementation of the laws plays an influential tool in the world trade economy. As well as the fact that the SALRC made informed decisions about the POPI Bill by taking the EU and the US laws into consideration.

There are various differences between the EU and the US but the main difference is that the US uses a self-regulatory system for protecting privacy of information whereas the EU does not. In theory information protection may be achieved through varying forms of self-regulation, this means that companies and industry bodies will establish codes of conduct and engage in self-policing.[334] However, in many countries, these efforts have been disappointing, as the codes are often unfulfilled.[335] Adequacy and enforcement are major problems with these approaches. Unfortunately most industry codes merely create weak protection and lack solid enforcement.[336]

4.1 Organization for Economic Co-Operation Development (OECD)

In contrast to the EU Data Directive, the OECD Guidelines have little to say about the need for and competence of, national information protection authorities. In fact, the OECD does not require such authorities to be established.

The OECD enacted Security Principles that the EU Data Directive used as the foundation for the principles in the directive. These principles are intended to encourage

---

[334] SALRC "*Privacy and Data Collection*" 3 5.1.6.
[335] SALRC "*Privacy and Data Collection*" 3 5.1.6.
[336] SALRC "*Privacy and Data Collection*"3 5.1.6.

proper application of the security safeguards principles.[337] They are awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and reassessment.[338]

4.2 The European Union

Until the 1980s the European Commission was anxious about impressing maximum obligations on the member states.[339] However, the EU changed their approach in recent years as confidence in their member states grew. The EU has now put forward directives that require the member states to take on more responsibility.

In 1995, the EU enacted the EU Data Directive[340] in order to harmonise member states' laws. This would be possible by supplying consistent levels of protection for citizens and ensuring the 'free flow of personal information' within the EU.[341] The EU Data Directive arose from the sense that European citizens were losing control over their personal information and that they had a fundamental right to privacy which was being infringed.

The EU Data Directive applies to the processing of personal information in electronic and manual files. It provides only a basic framework so that national legislatures may develop the laws to their country's needs.[342] The EU Data Directive also requires all data processing to have a proper basis and identifies the legal grounds for the collection and use of data.

---

[337] Organization for Economic Co-operation and Development *Guidelines for the Security of Information Systems and Networks: Toward as a Culture of Society.* Available at http://www.oecd.org/dataoecd/16/22/15582260.pdf (Accessed 22-01-21) Section III.
[338] OECD *Guidelines* Section III.
[339] Macleod *Consumer Sales Law* 2 ed 2007 87-88.
[340] Data Protection Directive.
[341] SALRC "*Privacy and Data Collection*"i 7.
[342] SALRC "*Privacy and Data Collection*"i 7.

The basic principles[343] that the EU Data Directive establishes are obligations 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. The EU Data Directive establishes a principle of fairness regarding the collection of data under which each individual is provided with the option of whether to supply the information requested or not,[344] this is similar to a type of notice and/or an opt-out procedure.[345]Individuals must also be provided with an opportunity to learn the identity of organisations that are intending to process data about them.[346] In addition, individuals are entitled to know the main purpose for which that information is being collected or will be used.[347]

The EU Data Directive ensures that Member States shall protect the fundamental rights and freedom of natural persons and in particular their right to privacy with respect to the processing of personal data.[348] Personal data' is defined broadly.[349]

The quality of the data is important.[350] To ensure quality, the personal data must be processed in a fair and lawful manner.[351] The data must be collected for a specified purpose[352] and it must be adequate, relevant and not excessive to the reasons behind the specified purpose.[353] In addition the data must also be kept updated, where required, and thus be accurate.[354] And the form in which the data is preserved must be easily identified to the data subject for the purpose of the collection[355] (so that once the data is no longer required, it may be removed with ease.).

---

[343] Article 6 Data Protection Directive.
[344] Article 7 Data Protection Directive.
[345] SALRC "*Privacy and Data Collection*" 8-9 4.1.23.
[346] Article 19 Data Protection Directive.
[347] Article 12 Data Protection Directive.
[348] Article 1 (1) Data Protection Directive.
[349] Article 2 (a) Data Protection Directive 'personal data 'shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
[350] Section I Data Protection Directive.
[351] Article 6 (1) (a) Data Protection Directive.
[352] Article 6 (1) (b) Data Protection Directive.
[353] Article 6 (1) (c) of Data Protection Directive.
[354] Article 6 (1) (d) Data Protection Directive.
[355] Article 6 (1) (e) Data Protection Directive.

The EU Data Directive also governs the processing of the personal data in section II of the EU Data Directive. The data subject must give clear and complete consent.[356] Processing is required in terms of a contract between the data subject and the controller.[357] The processing of the data requires the controller[358] to be subject to a contractual obligation.[359] The processing is required to protect the data subject's interests.[360] Processing is for public interest or an exercise of official authority that has vested in the controller or a third party to whom the data is disclosed.[361] Processing is required to fulfill legitimate interests.[362]

Subsequently the EU imposed its own standard of protection on any country within which personal information of European citizens might be processed. Articles 25 and 26 of the Directive stipulate that personal information should only flow outside the boundaries of the EU to countries that can guarantee an "adequate level of protection" (the safe-harbour principles, which will be discussed in Chapter Five).

In order for the Member States to transfer personal data to third countries certain requirements must be fulfilled.[363] The transfer must only take place where it will not prejudice national compliance with the EU Data Directive provisions and the third country must provide adequate protection for the transfer to take place.[364] The transfer will be viewed under certain circumstances pertaining to the nature of the data, the purpose and duration of the proposed processing of the data.[365] Also professional rules and security measures must be taken within the third country.[366] The Member States and

---

[356] Article 7 (a) Data Protection Directive.
[357] Article 7 (b) Data Protection Directive.
[358] Article 2 (d) Data Protection Directive. Defined to be "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.".
[359] Article 7 (c) Data Protection Directive.
[360] Article 7 (d) Data Protection Directive.
[361] Article 7 (e) Data Protection Directive.
[362] Article 7 (f) Data Protection Directive.
[363] Chapter IV of Data Protection Directive.
[364] Article 25 (1) Data Protection Directive.
[365] Article 25 (2) Data Protection Directive.
[366] Article 25 (2) Data Protection Directive.

the Commission may inform one another where they believe the third country does provide adequate protection.[367] If there is a finding by the Commission that the third country has inadequate protection, the Member States may attempt to block the transfer.[368] There are ways for the transfer to still take place, subject to the EU Data Directive's derogations.[369] The Commission will make their finding based on the third country's domestic laws and international commitments.[370]

The information that the data subject will be allowed to access is the identity of the controller or his or her representative;[371] the purpose for the processing of the data;[372] the recipients of the data;[373] the data subject may reserve the right to refuse to answer certain questions and accessing the data will allow the data subject an opportunity to rectify the data or not.[374] However, these rights may be restricted by Member States if one or more of the exemptions on the EU Data Directive apply.[375] Any information that may not have been collected from the data subject is also subject to the rules discussed above.[376]

Enforceability is a key concept in the EU Data Directive. Data subjects have rights which are established in explicit rules. Every EU State has a data protection commissioner or agency that enforces the rules.[377] It is expected that the countries which the EU conducts business with will 'provide a similar level of protection.'[378]

The EU Data Directive also provides data subjects with a number of important rights, such as the right to access the data,[379] the right to rectify any inaccurate data,[380] the

---

[367] Article 25 (3) of Data Protection Directive.
[368] Article 25 (4) Data Protection Directive.
[369] Article 26 Data Protection Directive.
[370] Article 25 (6) Data Protection Directive.
[371] Article 10 (a) Data Protection Directive.
[372] Article 10 (b) Data Protection Directive.
[373] Article 10 (c) Data Protection Directive.
[374] Article 10 (c) Data Protection Directive.
[375] Section VI Article 13 Data Protection Directive.
[376] Article 11 Data Protection Directive.
[377] SALRC "*Privacy and Data Collection*" 8 4.1.21.
[378] SALRC "*Privacy and Data Collection*" 8 4.1.21.
[379] Article 12 Data Protection Directive.

right of recourse in the event that unlawful processing of the data occurs[381] and the right to withhold permission to use his or her data in certain circumstances.[382]

The EU and all its trading partners have been required to have adequate information protection regimes, conforming to the EU Data Directive with effect from October 1998. This means that transfer of information from the EU to both private and governmental bodies will normally only be permissible with countries which have acceptable information protection legislation or self-regulation covering the information protection principles.

Where data is transferred from an EU country to a non-EU country, the EU Data Directive establishes a basic rule that the non-EU country receiving the data must provide an "adequate level" of data protection[383]

This requirement has resulted in an increased pressure building outside of Europe for the passage of information privacy laws. Countries which refuse to adopt adequate information privacy laws may be unable to conduct certain types of information transactions with Europe, particularly if they involve sensitive data.[384]

Article 25 should be considered as there is a requirement of an "adequate level" of protection, not "comparable level" or similar level". This relaxes the standard and allows for some leeway when the Commission or the Member State investigates the circumstances affecting adequacy. Also when the determination of "adequate level" is made under Article 25.2, it can be made by the transmitting country, by another EU member nation, or by the EU staff in Brussels. This once again allows for a lot of subjective inspection and decision making. The general rule under the EU Data Directive is that the duty of notification to the competent information protection authority is an obligation for all responsible parties. However, immediately after this general obligation,

---

[380] Article 10 (c) Data Protection Directive.
[381] Recital (55) Data Protection Directive.
[382] Article 10 Data Protection Directive.
[383] Article 25 Data Protection Directive.
[384] SALRC "*Privacy and Data Collection*" 9 4.1.24.

the EU Data Directive sets out extensive exemptions whose application is left to the discretion of the Member States.[385] It is likely that the discretion will be exercised in light of the principles set out in the EU Data Directive.

There are several principles that need to be followed accordingly. The first principle is that the third country in question which is processing or undergoing processing must ensure that an adequate level of protection for the data is maintained.[386] Secondly, the level of adequacy of protection will be assessed in light of surrounding circumstances of the transfer of data factors such as the nature of the data, purpose of the processing and the duration of the processing to be taken into account to name a few in order to make an informed decision on adequacy.[387] Thirdly, the Member States and the Commission will inform one another if and when any third country is deemed to have inadequate protection in place.[388] The fourth principle applies when a third country is considered to have inadequate protection in place, in terms of Article 25.2. Subsequently the Commission must undertake to prevent any transfer of personal information to the third country.[389] The fifth principle allows for the Commission to remedy principle four but only at the appropriate time.[390] Lastly, the sixth principle allows for the Commission to decide that a third country has an adequate level of protection based upon their own domestic laws or international commitments.[391]

To aid proper implementation of national provisions the EU Data Directive provides for the use of codes of conduct.[392] EU member states are required to approve draft codes and amendments or extensions to existing codes that are prepared by trade associations and other bodies. Organisations representing certain industry sectors may furthermore submit draft Community codes, and amendments or extensions to determine

---

[385] SALRC "*Privacy and Data Collection*" 71 5.5.15.
[386] Art 25.1 Data Protection Directive.
[387] Art 25.2 Data Protection Directive.
[388] Article 25.3 Data Protection Directive.
[389] Article 25.4 Data Protection Directive.
[390] Article 25.5 Data Protection Directive.
[391] Article 25.5 Data Protection Directive.
[392] Article 27 Data Protection Directive.

whether the drafts comply with the EU Data Directive.[393] Codes of conduct are useful to clarify the application of information protection law in a particular sector, and can also be used as 'an alternative to sectoral regulation.'[394] Theoretically the codes should be simpler and more flexible guidelines in order to achieve the same protection, instead of laying down of sector-specific rules applying the more general information protection rules.[395]

The EU Data Directive does make allowance for situations in which an EU Member State can authorise a transfer in the absence of an adequate level of information protection for example, the data subject has unambiguously given consent to the transfer,[396] however, 'it is not clear whether assent is required, or if notice with the opportunity to opt out is sufficient.'[397]

It is therefore possible to protect the privacy of information transferred to countries that do not otherwise provide "adequate protection" by making use of private contract conditions which contain standard information protection clauses.[398] These conditions would bind the data processor to respect fair information practices such as the right to notice, consent, access and legal remedies.[399] The conditions of the contract pertaining to information privacy would be drafted to satisfy the level of adequacy requirement set by the EU.[400]

The EU Data Directive deals with profiling in a limited sense. Article 15(1) states that EU member states shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or her or significantly affects him or her and which is based solely on automated processing of information intended to evaluate

---

[393] SALRC "*Privacy and Data Collection*" 83 5.6.2.
[394] SALRC "*Privacy and Data Collection*"83 5.6.4.
[395] SALRC "*Privacy and Data Collection*"83 5.6.4.
[396] Article 26.1(a) Data Protection Directive.
[397] SALRC "*Privacy and Data Collection*"361 7.6.
[398] SALRC "*Privacy and Data Collection*" 362 7.7.
[399] SALRC "*Privacy and Data Collection*"362 7.7.
[400] SALRC "*Privacy and Data Collection*"362 7.7.

certain personal aspects relating to him or her, such as his or her performance at work, creditworthiness, reliability and conduct.[401]

However, marketing profiles are not regarded as necessarily detrimental to the data subject. In fact, the Commission seems to have been of the opinion that simply sending a commercial brochure to a list of persons selected by a computer does not significantly affect the persons for the purposes of Article 15(1). Also, other commentators view certain forms of advertising as too trivial to be significant.[402]

The EU Data Directive provides that personal information may only be processed if the individual concerned 'has unambiguously given his consent'.[403] The data subject's consent is defined to mean any freely given 'specific and informed indication of his wishes'.[404] This in an unclear definition as it allows for wide interpretation and is capable of creating problems due to the allowance of the responsible party or the data controller to use their subjective views on the data subject's indication.

The EU Data Directive requires that supervising authorities operate with total independence when exercising their functions.[405] Absolute independence requires that great care must be taken in ensuring that authorities do not allow administrative dependence on other bodies to undermine the functional independence they are otherwise supposed to have. 'The role of the Information Protection Authority is therefore that of an ombudsman, auditor, consultant, educator, policy advisor, negotiator, enforcer and international ambassador.'[406]

The EU Data Directive is specific concerning sanctions and remedies. It requires that data subjects be given the right to a "judicial remedy" for "any breach" of their rights

---

[401] Article 15 (1) Data Protection Directive.
[402] SALRC "*Privacy and Data Collection*" 99 5.7.16
[403] Article 7 Data Protection Directive.
[404] Article 2 (h) Data Protection Directive.
[405] SALRC "*Privacy and Data Collection*" 99 5.2.16; Article 28(1) Data Protection Directive.
[406] SALRC "*Privacy and Data Collection*"15 5.2.24.

in order to allow the national data protection law to apply.[407] It also stipulates that decisions by a data protection authority which gives rise to complaints "may be appealed against through the courts."[408]

There are certain problems that countries may face which will affect the implementation of information legislation. Organisations may find that they have a lack of resources in order to adequately conduct protection and enforcement. A reality is for many organisations are that they will only receive help from national budgets years after the information legislation was enacted.[409] And usually when this happens the need for information legislation will have changed, especially upon consideration of the growth rate of e-commerce. Sometimes it becomes increasingly difficult to separate the roles of an ombudsman to that of a parliamentary official.[410] This is due to the fact that South Africa works with checks and balances between the Organs of State (the judiciary, the legislature and the executive) for handling the separation of powers.[411]

In order to achieve acceptance for trade purposes by all the EU Member States, the U.S. Federal Trade Commission (FTC) subsequently announced a major privacy enforcement initiative which 'will increase resources dedicated to protecting consumers.'[412]

The EU Data Directive concerning unfair commercial business practices in the internal market and the Unfair Commercial Practices Directive[413] has become a technology-neutral and comprehensive EU framework.[414] It does not override practices

---

[407] Article 22 Data Protection Directive.
[408] Section 28(3) Data Protection Directive.
[409] SALRC "*Privacy and Data Collection*" 18 5.2.30.
[410] SALRC "*Privacy and Data Collection*" 18 5.2.
[411] Section 2 (1) Constitution of the Republic of South Africa.
[412] SALRC "*Privacy and Data Collection*" 49 5.3.43.
[413] Directive2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive').
[414] De Groote & De Vuldes "The Unfair Consumer Practice Directive" in Howells (et al) *The Yearbook of the Consumer* 2007 349 358.

where cross-border restrictions are identified and which fall outside of the co-ordinated fields of the sector-specific directives.[415]

4.3 The United States of America

The SALRC was referred to the position in the US, where an assortment of privacy laws are found in the individual States and at the federal level, but no national general privacy law has been enacted for the private sector.[416]

Information protection is rather a question of economic power opposed to a political right.[417]

US industries in the private sector are encouraged to self- regulate. The law will rarely intervene – usually only on targeted basis to solve specific issues where the marketplace has failed to handle the situation appropriately.[418]

Sector divided laws can be regarded as a mélange of laws that regulate the collection and dissemination of different types of personal information in different ways, depending on how it is acquired, by whom, and how it will be used.[419] Although these laws provide a degree of privacy protection, they are not comprehensive. This is because they do not apply uniformly to all service providers. There are few meaningful legal privacy protections which exist for some important categories of records, for example, marketing information.[420] 'Sectoral regulations are often unconsidered and inconsistent compared to what is required of them.'[421]

---

[415] De Groote & De Vuldes "Unfair Consumer Practice" in *The Yearbook 2007* 358.
[416] SALRC "*Privacy and Data Collection*" 13 3.4.21.
[417] SALRC "*Privacy and Data Collection*" 3 5.1.2.
[418] SALRC "*Privacy and Data Collection*"21 5.2.35.
[419] SALRC "*Privacy and Data Collection*"21 5.2.37.
[420] SALRC "*Privacy and Data Collection*" 22 5.2.39.
[421] SALRC "*Privacy and Data Collection*" 22 5.2.39.

It is often overlooked that self-regulation is nothing new, but actually nothing more or less than the default position of the way in which most problems are solved in society.

Self-regulation is often complex due to the need for experimenting in order to prepare for more effective regulation.[422] Self-regulation may also serve as a sector specific way to implement legislation and to avoid too much detail in the legislation itself. A last option is that self-regulation can serve as a way to provide solutions beyond the scope of the existing legislation, which may or may not lead to a new cycle of policy making.[423]

In 1998 the US Department of Commerce was requested to provide the President with a report on industry efforts which were being made to establish self-regulating regimes to ensure online privacy and to develop technological solutions to guard privacy.[424] Self-regulation must be meaningful and consumer-friendly. Also self-regulation must be 'more than articulate broad policies or guidelines'.[425]

Effective self-regulation also involves substantive rules, as well as ensuring that consumers know the rules, that companies comply with them, and that consumers have appropriate recourse when grievances occur due to non-compliance.[426] Ensuring that consumers are informed about the rules is problematic to implement. This is because consumer types range from young, old, poor, wealthy, educated and uneducated and therefore in order to effectively inform all consumers becomes challenging.

The US Constitution does not explicitly mention a right to privacy. The Supreme Court has, however, ruled in favour of a limited constitutional right to privacy based on a number of provisions in the Bill of Rights.[427] This includes a right to privacy from

---

[422] SALRC "*Privacy and Data Collection*" 23 5.2.46.
[423] SALRC "*Privacy and Data Collection*" 23 5.2.46.
[424] SALRC "*Privacy and Data Collection*"28 5.2.64.
[425] SALRC "*Privacy and Data Collection*"28 5.2.64.
[426] SALRC "*Privacy and Data Collection*" 29 5.2.64.
[427] SALRC "*Privacy and Data Collection*" 377 8.3.1.

government surveillance into an area where a person has a "reasonable expectation of privacy".[428]

The US Constitution only applies where a "state action" may be found. Therefore the rights which the individual has in the US Constitution are only enforceable against the State. In addition, the US Constitution is a provider of "negative rights". This means that the individual may protect themselves from State abuse but places no affirmative duties on the state to protect the constitutional rights of individuals by actions such as the 'adoption of legislation.'[429] Subsequently there is no duty placed on the government to play an active role in protecting the individual against the invasion of his or her informational privacy rights.[430]

In *Doe v Chao*[431] the Court held that a plaintiff in a privacy act[432] suit must demonstrate actual damages to qualify for the Act's minimum statutory award.[433]

Various federal laws cover some specific categories of personal information but there are no comprehensive privacy protection laws which are available for the individual to depend upon.[434] There is no independent information protection agency in the US.[435]

4.4 The Safe Harbor Agreement

Articles 25 and 26 of the EU Data Directive as discussed above stipulates that personal data should only flow outside the boundaries of the EU to countries which can guarantee an "adequate level of protection".[436] This brought about fears in the US that the free flow of information between the US and Europe would be hampered.

---

[428] *Katz v United States* 386 U.S. 954 (1967).
[429] SALRC "*Privacy and Data Collection*"377 8.3.1.
[430] SALRC "*Privacy and Data Collection*"377 .3.1.
[431] Doe v Chao 540 U.S. 614 (2004).
[432] Privacy Act of 1974.
[433] SALRC "*Privacy and Data Collection*" 378 8.3.4.
[434] SALRC "*Privacy and Data Collection*"378 8.3.6.
[435] SALRC "*Privacy and Data Collection*"379 8.3.7.
[436] SALRC "*Privacy and Data Collection*" 374 8.2.8.

The US does have a great respect for privacy; however they tend to favor protecting the home of an individual more than the integrity of personal information.[437] There is a requirement for the individual to be able to protect him or herself from any intrusion of privacy by means of personal information for compiling databases.[438]

Although the EU Commission never issued a formal opinion on the adequacy of privacy protection in the US, there were serious doubts whether the US self-regulatory approach to privacy protection would pass the adequacy standard set out in the EU Data Directive.[439]

The US was correct to be concerned over their adequacy of their protective levels. This is the reason the safe-harbor agreement (the principles) were negotiated in 2002. The safe-harbor agreement consists of a set of information principles agreed upon by the US and the European Commission with which all parties have to comply voluntarily.[440]

The US strongly petitioned the EU and its member countries to find their system adequate. In 1998, the US began negotiating a "Safe Harbor" agreement with the EU in order to ensure the continued transborder flow of personal information. The idea of the "Safe Harbor" was that US companies could voluntarily adhere to a set of privacy principles worked out by the US Department of Commerce and the Internal Market Directorate of the European Commission. These companies would then have a presumption of adequacy and they could continue to receive personal information from within the EU.

The EU commissioned two prominent US law professors, who wrote a detailed report on the state of US privacy protections and 'pointed out the many possible cracks in US protection.'[441] On conclusion of the negotiations, which lasted nearly two years, over

---

[437] Keller et al *USA* 2001 in Edited Henry International Privacy, Publicity and Personality Laws 2001 461.
[438] Keller et al *USA* in *International Privacy* 2001 385.
[439] SALRC "*Privacy and Data Collection*" 362 7.9.
[440] Safe Harbor Available at https://www.export.gov/safehrbr.aspx (Accessed 20-01-2010).
[441] SALRC "*Privacy and Data Collection*" 362 7.10.

the drafting of the principles, they were still subjected to bitter criticism by privacy and consumer advocates.[442]

The US Department of Commerce and the European Commission in June 2000 announced that they had reached an agreement on the Safe Harbor negotiations that would subsequently allow US companies to continue to receive information from Europe. In July, 2000, the Commission approved the agreement. Since the approval over 200 companies have joined the Safe Harbor.[443]

The Principles aim to prevent accidental information disclosure or loss of the personal information. 'Personal information' is worded in such a way that it falls back on the EU Data Directive's definition.[444] The Principles are not mandatory to US companies; however, if such companies wish to trade easily with EU Member States, they will need this agreement to uphold these principles.[445]

The principles are easily understandable for US Companies and all fall back on the EU Data Directive.[446] The first safe harbor principle is notice, which links back to the purpose of the collection[447] and to whom the data may be disclosed to. The second principle is choice, this means that the data subject needs to be able to choose whether the information must be released to third parties or not. If the data subject would prefer to opt out of the collection, the choice needs to be available to him or her.[448] Thirdly, the onward transfer principle requires that the transfers of personal data will only be done to third parties whom have adequate protection of personal data.[449] The fourth principle is security which requires reasonable steps taken to be taken to protect the data.[450] Another principle is to control the integrity of the data: this requires that the data must be

---

[442] SALRC "*Privacy and Data Collection*" 362-363 7.11.
[443] Safe Harbor "*List* " Available at https://www.export.gov/safehrbr/list.aspx (Accessed 20-01-2010).
[444] Section I (c) of the Policy.
[445] Privacy "*International "Overview.*
[446] Safe Harbor "*Safe Harbor Privacy Principles*" Available at http://www.export.gov/safeharbor/eu/eg_main_018475.asp (Accessed 20 01 2010)
[447] Article 6 (1) (b) Data Protection Directive.
[448] Section VII Article 14 Data Protection Directive.
[449] Chapter IV of Data Protection Directive.
[450] Section VIII Data Protection Directive.

adequate, reliable and relevant to the purpose of collection.[451] There is also a principle which governs the access to the information. The data subject needs to be able to access their personal information for reasons ranging from correction to deletion.[452] The final principle is the enforcement principle which requires that the data protection principles must be capable of being enforced.[453]

Individuals must be given the option to opt out of the collection of information where the information is either going to be disclosed to a third party or used for an incompatible purpose. When information contains sensitive details, individuals must expressly consent to the collection. Organisations wishing to transfer information to a third party may do so if the third party subscribes to Safe Harbor or if that third party signs an agreement to protect the information.[454] Organisations must take reasonable steps to secure information against loss, misuse and unauthorized access, disclosure, alteration and destruction. Organisations must provide individuals with access to any personal information held about them, and provide consumers with the opportunity to correct, amend, or delete that information where it is inaccurate.[455]

4.5 Comments on the Safe Harbor Agreement

Privacy advocates and consumer groups both in the US and in Europe are skeptical of the European Commission's decision to approve the agreement, which they predict will fail to provide European citizens with adequate protection for their personal information.[456] The agreement rests on a self-regulatory system whereby companies merely promise not to violate their declared privacy practices. There is little enforcement or systematic review of compliance. The Safe Harbor status is granted at the time of self-certification. There is no individual right to appeal or right to compensation for privacy infringements.

---

[451] Article 6 (1) (c) Data Protection Directive.
[452] Article 6 (1) (d) and (e) Data Protection Directive.
[453] Article 32 (1) Data Protection Directive.
[454] SALRC "*Privacy and Data Collection*"364 7.13.
[455] SALRC "*Privacy and Data Collection*"364 7.13.
[456] SALRC "*Privacy and Data Collection*" 364-365 7.14.

There is an open-ended grace period for US signatory companies to implement the principles.[457]

In February 2002 the European Commission issued a report on the practical operation of the EU-US Safe Harbor Agreement. This was the first report to evaluate the success of the agreement. It concluded that all the essential elements of the agreement are in place and that a structure exists for individuals to lodge complaints if they feel their rights have been infringed. It did find, however, that there is not sufficient transparency among the organisations that have signed up to Safe Harbor and that not all dispute resolution providers relied on to enforce Safe Harbor actually comply with the privacy principles in the agreement itself.[458]

[457] SALRC "*Privacy and Data Collection*" 364-365 7.14.
[458] SALRC "*Privacy and Data Collection*"365 7.15.

5 SOUTH AFRICAN IMPLEMENTATION OF THE CONSUMER'S INFORMATION PRIVACY

5.1 South Africa's Implementation

Dean has stated that the creation of effective legislation in order to protect the individual's right to privacy is a necessity.[459] Any misuse of personal information in a database can amount to an unlawful invasion of privacy.[460]

It is important for consumers to be able to help themselves.[461] The DTI has to bear in mind that the South African Legislature is not dealing with the same type of consumer as in the EU member states and the US citizens. In fact, many South African consumers are uninformed, uneducated and reasonably observant of his or her rights. [462]

Also it is important to remember that all consumers do not share equal knowledge.[463] This is the reason the DTI is pressured to ensure that the consumer is educated on their consumer rights. However the DTI needs to be careful that the consumer is not bombarded with the too much information too quickly.[464]

South Africa's international trade aspirations would be adversely affected by the adoption of a privacy model that is considered inadequate by international and EU standards. This impact would not only be felt on a bilateral basis, but on the multilateral level. It would result in lost opportunities for database warehousing, and possible cross border trade in financial and telecommunications services. South African international trade will be negatively impacted if South Africa does not meet the standard of the EU Data Directive.[465]

---

[459] Dean et al *South Africa* in *International Privacy* 2001 385.
[460] Dean et al *South Africa* in *International Privacy* 2001 385.
[461] Rinkes "*European Consumer*" in *Yearbook* 2008 18.
[462] Wilhelmsson "*The Informed Consumer v the Vulnerable Consumer in European Unfair Commercial Practices Law – A Comment*" 2007 in Howells *Yearbook* 2007 211.
[463] Macleod "*Consumer Sales*" 71.
[464] Macleod "*Consumer Sales*" 71.
[465] Article 25 Data Protection Directive.

Although the international community (as well as the EU Data Directive) is not prescriptive as to the way in which these standards are to be met, it is safe to say that having an appropriate comprehensive statute that meets the requirements of Article 25 of the EU Data Directive, with an independent regulatory authority to support this cause, will be a big step in the right direction.

The fact that the EU Data Directive makes provision for other ways in which to acquire adequacy contradicts the argument that South Africa will be adversely affected, in so far as its trade with African countries are concerned, should it comply with Article 25. Trade with African countries will be more difficult than with Europe since adequacy will have to be established in each particular transfer. This is, however, the status quo at the moment and this position cannot be credited to the effects of the information protection legislation.

It is also important to consider that the transfer of information to South Africa from Europe is governed from the European side by the directive or country's legislation which has been enacted to conform to the EU Data Directive.[466]

It is the South African Law Commission's objective to ensure that the legislation provides an adequate level of information protection in terms of the EU Data Directive. In this regard a provision has been included in the POPI Bill that prohibits the transfer of personal information to countries that do not ensure an adequate level of information protection.[467]

Should these proposals be adopted, the protection of information privacy in South Africa will be brought in line with international requirements and developments.[468]

Even though South Africa is a young democratic country it is still up to date with international standards. South Africa's IP Principles will provide adequate protection for

---

[466] SALRC "*Privacy and Data Collection*" 365 7.17.
[467] Section 69 Protection of Personal Information Bill.
[468] SALRC "*Privacy and Data Collection*"406 9.15.

South Africa to receive personal data from any of the EU Member States. Notice, choice, onward transfer, security, data integrity, access and enforcement are all in the POPI Bill in the form of accountability, openness, processing limitation, further processing limitation, specification of the purpose of collection, information quality, security safeguards and data subject participation. This is an illustration of how South Africa is developing and is capable of being an authentic participant in the international market of trade and commerce.

A suggestion about South Africa and the US working together on approaches for addressing legitimate concerns about privacy protection and relevant trans-border issues was conducted by the SALRC.[469] The initiatives used in the US are thought to be useful alternatives to "one-size-fits-all" legislative approaches to privacy protection. It appears that due to South Africa still being young, in comparison to the member states of the EU and the US, self-regulation does not seem like a viable option for South Africa.

However, it may be advantageous for South Africa to have sector-specific regulatory authorities (similar to the US) as this would ensure that information protection policies and legislation are adequate and compliant with international practice.[470] This will also ensure that there is proper and adequate policing of issues around privacy protection. However, the existing regulatory bodies, which oversee the various industries, have adequate systems and insight to properly ensure compliance which subsequently makes the need for an independent regulatory agency or authority unnecessary.[471] This is more sensible as having sector-specific regulatory bodies will create more expenses for the government and subsequently the consumer.

---

[469] SALRC "*Privacy and Data Collection*" 52 5.3.45.
[470] SALRC "*Privacy and Data Collection*" 46 5.3.36.
[471] SALRC "*Privacy and Data Collection*" 46 5.3.36.

5.2 Concluding Remarks

When the EU Data Directive was enacted, it was done so with the aspiration of harmonising the member states' laws in providing consistent levels of protection for citizens and ensuring the free flow of personal data within the EU.[472] The EU Data Directive has a great ambition to tackle cross-border pressure of goods and services that the consumer encounters.[473]

Given the growing number of cross-border information transfers, the idea of relying on global rules for all cross-border information transfers is attractive. The code of conduct concept is a simple one. Related companies doing business in multiple countries would apply just one set of rules to govern their information transfers from within the EU to outside the EU rather than having to comply with the specific requirements of each of the countries in which they operate. Companies could also draft these codes so that they comply with the privacy laws in non-EU states.[474]

5.2.1 The EU Data Directive

Bainbridge states that the processing limitation principle is the crux of the EU Data Directive and in fact the other principles just help to express the processing limitation principle.[475] This opinion is logical as the entire EU Data Directive is aimed at regulating the processing of personal information

The fact that the DTI has used the EU Data Directive as the foundation of the POPI Bill means that South Africa will avoid the use of the Safe Harbor Principles. This is a more feasible option for South African businesses and their consumers.

---

[472] SALRC "*Privacy and Data Collection*"374 8.2.7.
[473] De Groote & De Vuldes "Unfair Consumer Practice" in *The Yearbook 2007.*
[474] SALRC "*Privacy and Data Collection*"371 7.22.
[475] Bainbridge *Data Protection* 70.

5.2.2. The Safe Harbor Principles

Effectively by signing up to the Safe Harbor each US company agrees to adhere to respecting the privacy of the personal data.[476] This illustrates a leap of faith and a willingness on behalf of the company to adhere to the EU Data Directive.

5.2.3 South Africa

There are few concerns that have been brought to light in this paper. It appears that the DTI is clear on the fact that they want to ensure that the consumer is protected. And after an analysis of the EU Data Directive throughout this paper it is clear that the EU Data Directive is a good model to base South Africa's consumer privacy protection on.

5.2.3.1 Opt In versus Opt Out

A concern that has been noted is that the CPA institutes the opt out approach for situations in which the consumer is dealing with spam and other unsolicited communications. On the other hand the POPI Bill institutes the opt in approach to spam. However it is likely that once the Protection of Personal Information Act is enacted the Act will repeal the CPA's provisions relating to unwanted direct marketing. This is unlikely to become a major concern for the State as both the CPA and the POPI Bill are attempting to achieve the same result but by different methods. This is illustrated by DMASA which has already begun to offer an opt in list.

The fact that the DMASA has already begun to control the opt in and opt out lists is a positive move for the CPA and the POPI Bill to be implemented. The only concern is that the DMASA will be carrying all the costs of these lists. This may be extremely difficult for the DMASA to do, especially considering that the opt out list will be banished once the POPI Bill is enacted as an act of Parliament.

Also Section 21 (1) of the CPA is especially important for the South African consumer. However, there is a possibility that with the introduction of the POPI Bill this section may become redundant. This is because the POPI Bill requires the direct marketer

[476] Bainbridge *Data Protection* 71.

to make use of the opt in list which means that people who have opted in to receive direct marketing materials want to receive those details. Perhaps 'redundant' is too strong after all section 21 (1) may be used by the consumer once the consumer has decided he or she no longer wishes to receive information.

5.2.3.2 Consumer Education

Perhaps it is necessary for the Minister of Finance to make provisions in the budget for a percentage of the cost of implementation that the DMASA will in incur. Also the consumer receiving education about his or her consumer rights and responsibilities need to be considered in the National Budget. The SALRC is clear on their position that the consumer has to be educated. It would be difficult to disagree that consumer education is not a necessity.

As mentioned in Chapter One, the right to education is applicable to the consumer's privacy protection laws. This was mentioned by the SALRC, as discussed in Chapter Three. The fact that South Africa has such a wide-reaching Constitution will only be completely beneficial to the consumer if the consumer is educated about these rights. There is a great responsibility bestowed upon the DTI to ensure that all the different types of consumers need to be a) aware of their rights; b) understand their rights and c) be capable of enforcing their rights.

5.2.3.3 Unwanted Direct Marketing Due to Privacy Concerns

The consumer's right to restrict unwanted direct marketing is an important right for the consumer. This is because the consumer needs to be able to control the amount information that he or she makes available to third parties. There is room for a lot of personal damage if a consumer's personal particulars are abused. Although identity theft has not been the focus of this paper, it must not be forgotten.

Nevertheless, the consumer needs to have the knowledge about which persons have access to their personal information. The fact that PAIA has been enacted helps the

much needed transparency between organizations and their consumers. Bearing this in mind, the consumer needs more than just access to information. The consumer needs to be able to alter and delete certain particulars of their information held by a third party.

5.3 Closing remarks

The cooling-off periods instituted in the CPA are necessary as the pressure of purchasing goods or services by way of direct marketing needs to be alleviated from the consumer. This is especially the case when the consumer receives the direct marketing in their home. This is because in the home, the consumer may feel compelled to make a purchase.

The ultimate goal of consumer protection and consumer law is to contribute to a better society.[477] Consumer law is primarily focused on restoring the balance between the strong and the weak market players.[478] The CPA appears, at face value, to achieve this goal. However, only time will tell as to whether the CPA will be successful or not. The POPI Bill contains many promises but due to the fact that it is still a Bill it is subject to change. Although it is unlikely that the IP principles will be changed once the POPI Bill is enacted.

The sections in the CPA which govern the protection of consumer privacy is not the most convincing legislation and does pose minor issues but with the implementation of the POPI Bill – the CPA's intentions may be accomplished. Therefore the consumer's protection of personal information in relation to direct marketing will be made possible.

---

[477] Rinkes "*European Consumer Law: Making Sense*" 2008 in Twigg-Flesner *Yearbook of the Consumer* 2008 3 15.
[478] Rinkes "*European Consumer*" in *Yearbook* 2008 15.

BIBLIOGRAPHY

Primary Sources

Cases

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

O'Keeffe v Argus Printing and Publishing Co Ltd 1954 (3) SA 244 (CC)

American Online Inc v National Health Care Discount, Incorporated 121 F. Supp.2d 1255 (ND Iowa)

http://homepages.law.asu.edu

Crawley v Rex (1909 TS 1105)

S v Pepsi-Cola (Pty) Ltd 1985 (3) SA 141 (C)

National Media Ltd 90 v Jooste 1996 (3) SA 262 (A)

Campbell (Appellant) v MGN Ltd (Respondant) [2004] UKHL 22

http://www.publications.parliament.uk

Mistry v Interim Medical and Dental Council of South Africa 1998 (4) SA 1127 (C); 1998 (7) BCLR 880 (CC)

Stoffberg v Elliot 1923 CPS 148

Lymberg v Jefferies 1925 AD 235

Lampert v Hefer 1955 (2) SA 597 (A)

Esterhuizen v Administrator, Transvaal 1957 (3) SA 710 (T)

Bernstein v Bester NO 1996 (2) SA 751 (CC) ; BCLR 449 (CC)

Statutes

South Africa

Bantu Education Act 47 of 1953

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Electronic Communication and Transactions Act 25 of 2002

Gambling Act 51 of 1965

Group Areas Act 41 of 1950

Interim Constitution of the Republic South Africa Act 2 of 1994

National Credit Act 34 of 2005

Natives (Abolition of Passes and Co-ordinated Documents) Act 67 of 1952

Promotion of Access to Information Act 2 of 2000

Regulation and Interception of Communications and Provisions of Communication-Related Information Act 70 of 2002

The Protection of Personal Information Bill [B9-2009]

United States

The Privacy Act of 1974

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

International Conventions

1948, Universal Declaration of Human Rights

United Nations Guidelines for Consumer Protection (as expanded in 1999)

United Nations Guidelines Concerning Computerised Personal Data Doc E/CN.4/1990/72, 20.3.1990

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector

Secondary Resources

About.com African History *Apartheid Legislation in South Africa* http://africanhistory.about.com.

Advertising Standards Authority of South Africa http://asasa.org.za.

Bainbridge D *Data Protection Law* 2 Edition (2005) XPL Publishing , United Kingdom.

Bortz T and Ginsburg J *Object of the Bill* http://www.rhp.co.za/protection_bill.html.

Buys R *New Laws to Restrict Marketing Activities* Journal of Marketing volume December/November 2009.

De Jager C & Smith E *Advertising and the Law* (1995) Butterworths, Durban.

Deneys Reitz Attorneys *Protection of Personal Information* 2009 http://www.deneysreitz.co.za/index.

Dicey L *Marketing vs Advertising* Journal of Marketing 2008.

Direct Marketing Association of South Africa *Opt In* http://www.dmasa.org/core.

Edmonds D Commentary *No: 44: South Africa: The Real Threat to Sustainable Democracy* May 1994.

Epstein D & Nickles S *Consumer Law in a Nutshell* 2 Edition (1981) West Publishing, United States of America.

European Advertising Standards Alliance *The EASA Advertising Self-Regulatory Charter* http://www.easa-alliance.org

Federation of European and Direct Marketing http://www.fedma.org

Henry M (edited) International Privacy, Publicity & Personality Laws (2001) Butterworths, Durban.

Howells G, Nordhausen A, Parry D & Twigg-Flesner C *The Yearbook of Consumer Law* (2007) Ashgate, England.

Jazzbhay A *Corporate Social Responsibility and the Consumer Protection Act* 2009 http://www.law24.com/blogs.

Jeloschek C *Examination and Notification Duties in Consumer Sales Law: How far Should we go in Protecting the Consumer* 3 rd Edition (2006) Sellier, England.

Jordaan Y *Information Privacy Issues: Implications for Direct Marketing* 2007 in International Retail and Marketing Review Volume 3 Issue 1 May.

Kenyon A & Richardson M (edited) *New Dimensions in Privacy Law International and Comparative Perspectives* (2007) Cambridge University Press, Cambridge.

Kevan T & McGrath P *E-mail, the Internet and the Law: Essential Knowledge for Safe Surfing* (2001) EMIS Professional Publishing, Hertforshire.

Lee A & Du Plesis E *The Consumer Protection Bill: Kill it Says New Marketing Body* Journal of Marketing June/July 3 2006.

Laubser and Reid *Liability for the Production in the Consumer Protection Bill 2006: A Comparative Critique* Stellenbosch Law Review 2006 (17) (3).

Lim Y *Cyberspace Law: Commentaries and Materials* 2 nd Edition (2007) Oxford University Press, Australia.

Macleod J *Consumer Sales Law* 2 Edition (2007) Routledge Cavendish, London.

McQuoid-Mason PJ *The Law of Privacy in South Africa* (1978) Juta & Company, Johannesburg.

Michalson L *Protection of Personal Information Bill – The Implications for you* Online Legal http://www.michalsons.co.za/protection-of-personal-information-bill-the-implications-for-you/3041?gclid=CMO8ucWqq58CFY8A4wodpQxw1g.

Organization for Economic Co-operation and Development *Guidelines for the Security of Information Systems and Networks: Toward as a Culture of Society* http://www.oecd.org/dataoecd.

Parfit D *Reasons and Persons* 2 Edition (1987) Oxford University Press, New York.

Privacy International *Overview of Privacy* 2007 http://www.privacyinternational.org/article.shtml.

Ramsey I *Consumer Law* (1992) Dartmouth Press, New York.

Rawls J *Theory of Justice* (1971) Harvard City Press, United States of America,

Rule JB *Global Privacy Protection The First Generation (*2008) Edgar Elgar Publishing, United Kingdom.

Samuel GH *Cases in Consumer Law* (1979) Macdonald & Evans Limited, Great Britain.

Safe Harbor *List*
https://www.export.gov/safehrbr/list.

Shimmel G *In The Beginning : Advertising* Without Prejudice Volume 1 Issue 1 Feb 2009.

Snail S *The Rights of the e-Commerce: Consumer Law* Without Prejudice Volume 7 Issue 6 July 2007.

South African Law Reform Commission Discussion Paper 109 Project 124 October 2005 *Privacy and Data Collection*
http://salawreform.justice.gov.za/dpapaers/dp109.pdf.

The Department of Trade and Industry *What are a Consumer's Rights and Responsibilities?*
http://www.dti.gov.za/protectingconsumers/consumerrights.htm.

Twigg-Flesner C; Parry D; Howells and Nordhausen A *The Yearbook of Consumer Law 2008* (2007) Ashgate, England.

Van Eeden E *A Guide to the Consumer Protection Act* (2009) LexisNexis, Durban.

Van Wyk E and Botes R *Misleading Advertising* Without Prejudice Volume 8 Issue 10 November 2009

Varney H *Protection of Personal Information Bill Briefing*
http://pmg.org.za/report/20080611

Wacks R *Personal Information Privacy and the Law* (1989) Oxford University Press, Oxford.

Weatherill S *EU Consumer Law and Policy* (2005) Edward Elgar, Cheltenham.

Webber Wentzel *Consumer Protection Bill 2007*
http://www.webberwentzel.com/wwb

Woker T *Advertising Law in South Africa* (1999) Juta & Company, Johannesburg.