UNIVERSITY OF KWAZULU-NATAL ™

INYUVESI YAKWAZULU-NATALI

ELECTRONIC SPAMMING WITHIN SOUTH AFRICA; A COMPARATIVE ANALYSIS

A DISSERTATION PRESENTED

By

PRISHANI MAHEEPH

TO

THE SCHOOL OF LAW

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

MASTER OF LAWS (LLM)
In
BUSINESS LAW

UNIVERSITY OF KWAZULU NATAL

NOVEMBER 2014

DECLARATION OF ORIGINALITY

I hereby certify that I am the sole author of this dissertation and that no part of this dissertation has been published or submitted for publication.

I declare that this is a true copy of my dissertation including any final revisions and that this dissertation has not been submitted for a higher degree to any other University or Institution.

I declare that this dissertation is my own unaided work. To the best of my knowledge and belief, the dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

This project is an original piece of work which is made available for photocopying and for inter-library loan.

.....

Prishani Maheeph

210528505

ACKNOWLEDGEMENTS

Acknowledgement of my gratitude goes to Ms Devarasi Maduramuthu for supporting my research and providing me with constant guidance, helpful explanations and personal opinion. Furthermore I thank Ms Maduramuthu for sharing a passion in the subject of spamming which provided me with overall encouragement.

I thank my family for the abiding support and for sacrificing noise levels within my home to accommodate my concentration-span. I truly appreciate it.

Finally, I would like to thank the nearest and dearest to me – my four dogs, for reducing my stress levels at times when I needed it the most.

ABSTRACT

In the context of electronic messaging, spam refers to unsolicited bulk messages. Spam creates significant problems for the recipient of these messages, from mere irritation to infringements of constitutionally guaranteed rights. In addition, spam has threatened to undermine the usefulness of email. These abovementioned negative consequences of spam are addressed by technical, legislative and industry self-regulated measures. The primary focus of this research paper is on the legislative measures adopted to combat spamming. The majority of the research will highlight and discuss the South African position and will include an elucidation and critical analysis of the practical difficulties of said legislative means. In particular direct marketing and the enforcement mechanisms designed to implement and accord strength to these measures will be discussed. Thereafter this paper seeks to explore the manner in which the judiciary has interpreted the laws relating to spamming. The South African approach will then be compared to that of the related Canadian position. In conclusion, recommendations and suggestions for improvements will be canvassed.

KEY TERMS

Consumer Protection, Consumer Protection Act, Email, Electronic Communications and Transactions Act, Internet, Internet Service Providers, Opt-in and Opt-out regime, Protection Of Personal Information Act, Spam, Unsolicited Bulk Email, Unsolicited Commercial Email, Unsubscribe Mechanism.

BIBLIOGRAPHY

ADVERTISING STANDARDS AUTHORITY OF SOUTH AFRICA ("ASA")
Code of Advertising Practice (Appendix C) available at
http://www.asasa.org.za/codes/advertising-code-of-practice/appendix-c-direct-marketing-advertising%E2%80%93dmasa

BUYS R CRONJE F
Cyberlaw @SA II: The Law of the Internet in South Africa (2004) 2nd edition Pretoria: Van Schaik (2004)

CUIJPERS C KOOPS B
"How fragmentation in European law Undermines Consumer Protection: the Case of Location-based services" (2008) 33 E.L. Rev. Thomson Reuters (Legal) Limited and Contributors

EBERSOHN G
"An Analysis of Spam Legislation" (2004) 12(3) Juta's Business Law 134

GATES B
"Why I hate spam" The Wall Street Journal (23 June 2003) reprinted at
http://www.microsoft.com/presspass/ofnote/06-23wsjspam.mspx

GEISSLER M L
Bulk Unsolicited Electronic Messages (Spam): a South African Perspective (2004) (LLD thesis, University of South Africa)

GUIDE TO THE CANADIAN HOUSE OF COMMONS
"Making Canada's Laws" Official website of Parliament of Canada at
http://www.parl.gc.ca/About/Parliament/GuideToHoC/making-e.htm

GUIDELINES FOR RECOGNITION OF INDUSTRY REPRESENTATIVE BODIES OF INFORMATION SYSTEM PROVIDERS
"ECT IRB Guidelines" Gazetted under GN 1283 in GG 29474 of 14 December 2006

HOAX-SLAYER
Website available at http://www.hoax-slayer.com/

HUTCHISON D
The Law of Contract in South Africa Cape Town: Oxford University Press (2009)

INTERNATIONAL TELECOMMUNICATION UNION
WSIS Thematic Meeting on Cyber security A Comparative Analysis of Spam Laws: The Quest for a Model Law (10 June 2005) Document CYB/03 Geneva, Switzerland available at http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf

JONES M SCHOEMAN H
"The South African Constitution and Electronic Commerce" ISSA Information Security South Africa 3rd Annual Conference, Sandton (2004) (Unpublished) available at http://eprints.mdx.ac.uk/12693/1/The%20SA%20Constitution%20and%20Electronic%20Commerce.pdf

KASPERSKY LAB
Quarterly Spam Statistics Report Q3 – 2013 available at http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q3-2013#.VBmOuvmSwkO

MCRAE D
The Canadian Yearbook of International Law Volume 47 Toronto: University of British Columbia Press (2009)

MOONEY-COTTER A
Culture clash: An International Legal Perspective on Ethnic Discrimination Farnham, England Ashgate Publishing Ltd (2011)
PAPADOPOULOS S
"Are we about to cure the scourge of spam? A commentary on current and proposed South African legislative intervention" 2012 THRHR 223

PAPADOPOULOS S HAMANN B
"Direct marketing and spam via electronic communications: an analysis of the regulatory framework in South Africa" 2014 (47) 1 De Jure 42

PAULSON D
"Canada Update: A Review of Canada's Recent Holding Regarding the Proposed Securities Act, Canada's Anti-Spam Law that May Soon Take Effect, And the Disciplinary Hearing of Joe Groia" (2012) 18 (4) Law and Business Review of the Americas 615

SIPE M
"The Need for New Federal Anti-Spam Legislation" (2013) Vol. 31:55 Yale Journal on Regulation

SOUTH AFRICAN LAW REFORM COMMISSION
Discussion Paper 109 "Privacy and Data Protection", Project 124 (2005) Pretoria: SALRC

TLADI S
"The Regulation of Unsolicited Commercial Communications (SPAM); Is the Opt-Out Mechanism Effective" (2008) 125(1) SALJ 178-192

VAN DER MERWE D
Information and Communications technology law Durban: LexisNexis (2008) 183

WOKER T
“Why the Need for Consumer Protection Legislation? A Look at Some of the Reasons Behind the Promulgation of the National Credit Act and the Consumer Protection Act” 2010 (31) 2 Obiter 217

TABLE OF STATUTES AND REGULATIONS

CANADA

An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23) (There is no official short title for this Act.)

Charter of Rights and Freedoms, Constitution Act 1982

Electronic Commerce Protection Regulations [Canada Gazette] (Part I, Vol. 145, No. 28 – July 9, 2011]

Interpretation Act R.S.C 1985, c. I-21

NIGERIA

Criminal Code Act of Nigeria (1990)

SOUTH AFRICA

Constitution of the Republic of South Africa, Act 108 of 1996

Consumer Protection Act 68 of 2008

Consumer Protection Act Regulations GN 293 in GG 34180 (1 April 2011)

Electronic Communications and Transactions Act 25 of 2002

Electronic Communications and Transactions Amendment Bill [2012]

National Credit Act 34 of 2005

Promotion of Access to Information Act 2 of 2002

Protection of Personal Information Act 4 of 2013

UNITED STATES OF AMERICA

US Congressional Findings and Policy of the Controlling the Assault of Non-solicited Pornography Act of 2003

TABLE OF REPORTS AND CONVENTIONS

EUROPEAN UNION

European Union Data Protection Directive (95/46/EC)

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT ("OECD")

"Spam Issues in Developing Countries' Organisation for Economic Co-operation and Development" (2005) available at

http://www.oecd.org/internet/ieconomy/34935342.pdf

SOUTH AFRICA

Ad Hoc Joint Committee of South African Parliament Report on the Open Democracy Bill [B67-98] (2000)

South African Law Reform Commission Report Privacy and Data Protection Pretoria: SALRC (2009) ("Report on Privacy and Data Protection")

TABLE OF CASES

SOUTH AFRICA

Children's Resource Centre Trust v Pioneer Food 2013 (2) SA 213 (SCA)

Gaertner and Others v Minister of Finance 2014 (1) BCLR 38 (CC)

Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association 2014 (2) SA 569 (GJ)

North Central Local Council and South Central Local Council v Roundabout Outdoor (Pty) Ltd and Others 2002 (2) SA 625 (D)

UNITED STATES OF AMERICA

Rowan v United States Post Office Department 397 U.S 728 (1970)

TABLE OF CONTENTS

CHAPTER PAGE

CHAPTER 1

INTRODUCTION

"Like almost everyone who uses e-mail, I receive a ton of spam every day. Much of it offers to help me get out of debt or get rich quick. It would be funny if it weren't so irritating."[1]

Bill Gates

1.1 General Introduction

Congratulations, your mobile has been selected in a random draw and you are the lucky winner of one million rand. To claim your prize, please contact Mr Mazibuko on 075 765 8787.[2]

Perhaps if these claims were true, this research paper and what it seeks to achieve would not spark any interest in the reader. Thousands of South Africans would be planning expensive holidays with their winnings claimed from Mr Mazibuko. Alas, this is not the case; messages such as the one above, are almost always false and invariably prejudicial in its intent.

Although most spam messages can be easily distinguished from legitimate messages as fake and a nuisance, others are formulated with more sophisticated language causing the recipient to believe the message to be true. Consider the following real example which has become known as a "Nigerian 419 Scam":[3]

---

[1] B Gates 'Why I hate spam' The Wall Street Journal (23 June 2003) reprinted at http://www.microsoft.com/presspass/ofnote/06-23wsjspam.mspx accessed on 14 October 2014. This article comments on the problems associated with spam and the efforts of Microsoft® in combating spam through technological innovation and cooperation with government and industry leaders.

[2] This is a fictional example of a typical spam message that most consumers receive via SMS often requiring the consumer to deposit money in an account (of which the details are provided) to be able to receive their "winnings".

[3] The quoted spam examples contained in this research paper are direct quotes bearing misspellings that have not been corrected. This specific example can be found on the Hoax-slayer website available at http://www.hoax-slayer.com/engr-david-koni.shtml accessed on 24 September 2014. The number "419" refers to the relevant section of the Criminal Code Act of Nigeria (1990). The section reads: "Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years. If the thing is of the value of one thousand naira or upwards, he is liable to imprisonment for seven years. It is

"Subject: LOOKING FOR PARTNERSHIP IN BUSINESS

Engr David Koni.
(BOARD OF CONTRACT AWARD COMITTEE.)
Cotonou Republic Du Benin.

Sir/Madam,

It is my great pleasure to write to you and present my business proposal for your consideration and possible acceptance which you will find mutually beneficial to both parties.

I am Engr. David Koni, the Chairman of the Contract Award Committee,Cotonou Republic Du Benin W.Africa, We need a trust-worthy partner to assist us in the transfer of (US$11,5M) ELEVEN MILLION, FIVE HUNDRED THOUSAND UNITED STATES DOLLARS.for further investment in your country,

You will be required to:
(1) Assist us in the transfer of this sum to your bank account in your Country.

(2) Advise on areas for potential future investment in your country

(3) Assist us in carrying out the feasibility study before actual investment. If you decide to render your service to us in this regard,you will be paid 20% of the total funds for assistnce.Reply back this email if you are willing to work with us.

Respectfully,
Engr. David Koni.
Chairman Contract Award Committee {BCAC}

In this message the sender undertakes that the recipient will receive a substantial portion of a large sum of money in exchange for the transferring of funds to a bank account and for providing investment advice. Once the recipient shows any interest in the proposal, the fraudster will usually approach the recipient asking him to provide an advanced fee before the funds can be transferred to him. This scam illustrates the more serious consequences of spam.

immaterial that the thing is obtained or its delivery is induced through the medium of a contract induced by the false pretence. The offender cannot be arrested without warrant unless found committing the offence.

Spam is often identifiable (as such) by the layman, however, a legal definition for the term has not yet been settled upon; jurists have varied considerably in this respect.[4] The variations of the definition often relate to whether spam should only encompass commercial communications as opposed to the inclusion of communications of a non-commercial nature. In terms of South African academic writers, Buys has defined "spam" as "unsolicited bulk and/or commercial electronic communications" and Tladi has defined the term as "unsolicited email or electronic junk mail".[5] Geissler submits that a definition of spam should not be solely based on whether the communication is commercial; the volume and indiscriminate nature of the e-mail must also be considered.[6] As will be discussed in terms of the South African approach relating to spam control, there is no protection afforded to the receiver of a spam message of a non-commercial nature. For this reason Geissler's submission seemingly, provides a viable solution to this legislative gap.

Spam takes on many forms, including direct marketing or solicitation for questionable products or services. It can also include hoaxes, urban legends, chain letters, jokes, newsletters, opinion surveys, hate mail and messages containing fraudulent or deceptive content.[7]

Although spam is commonly received via email and short message services (hereafter referred to as SMS's), it may also be received via post and telephonic communication. Abuse is rife with most technology, but particularly with the use of electronic communications, as it has proved to be an inexpensive and quick means of reaching out to a much greater proportion of the public. Furthermore, when a spammer employs email as his mode of spamming, it is a difficult task to trace the spammer to be able to hold him accountable for his actions. For these reasons, this research paper is focused primarily on electronic communications as a means of spamming.

---

[4] The term "spam" originally referred to a canned precooked meat product which is manufactured by Hormel Foods. In 1970 '*Spam*' became the title of a sketch of the famous British comedy group Monty Python. In the sketch, two customers in a café attempt to order a breakfast from a menu that includes the ingredient spam in almost every dish. Whilst attempting to do so, people in the café are continuously chanting 'spam' which overrides the main dialogue. The term, in the context of electronic communications is derived from this sketch.

[5] F Cronje & R Buys *Cyberlaw @SA II: The law of the internet in South Africa* 2 ed Pretoria: Van Schaik (2004) 160; S Tladi 'The Regulation of Unsolicited Commercial Communications (SPAM); Is the Opt-Out Mechanism Effective' (2008) 125(1) *SALJ* 178, 178-179

[6] M L Geissler *Bulk unsolicited electronic messages (spam) : a South African perspective* (LLD thesis, University of South Africa, 2004) 388

[7] Ibid 88-90

1.2 Methods used to spam

Spam is often used as a vehicle for the delivery of other online threats. There are various methods employed to send spam. These methods include but are not limited to:[8]

- *Spyware*

Spyware is a form of computer software that collects information about an individual without their knowledge. It can be installed automatically in several ways. Spyware may be obtained by viewing an unsolicited email message containing a virus as an attachment, or as a result of visiting certain websites. Average internet users are generally unaware that information about their habits online are being monitored without their consent.

- *Dictionary attacks*

A dictionary attack is a method employed that systematically enters every possible formulation of an email address into a mail server in the optimistic expectation that some of the addresses will be guessed correctly.

- *Cookies*

Cookies are set on websites in order to profile consumers. A cookie is a piece of data that can be stored temporarily within one's browser. These files contain information about visitors to a site, including the visitor's name and some preferences of the visitor. The web server records the data and during later visits the server searches for a cookie and configures itself based on the provided data.

- *Spoofing*

Spoofing concerns the use of a forged email header to disguise the origin of a message and deceive the recipient into believing that the email comes from a trusted sender. It also describes an attempt to gain access to a system by posing as an authorised user, or the unauthorised use of legitimate identification and authentication data.

[8] Tladi (Note 5 above) 181-183

1.3 Framing the problem

To explore the various forms of spam, one need not travel far. I received the following email from a supposedly prominent bank, which was recognised as spam through Gmail filter protection: [9]

> "Subject: FW: Online service message
>
> Dear Client,
>
> Our system discovered an unusual conflict between your online access details and card number and have therefore set limitations to some online features.
>
> Please follow the link below and you will be guided through the online confirmation process.
>
> Confirm profile records
>
> There could be future problems with your access by failing to attend this matter."

As luck would have it, I am not an account holder with the bank that the email purports as the sender; and so it therefore seems absurd that the message could have any applicability to me. However, this would have serious implications for a recipient who was a legitimate account holder.

This email demonstrates the most stand-out characteristic of spam, namely bulk messaging. It also creates a serious concern that another receiver of the same email may have taken the spammer's bait of luring one to divulge his confidential banking details and as a result suffer losses. Financial loss is surprisingly not the primary concern with this message; consider the scenario where the receiver of the email follows the link that is provided in the email to supposedly update his profile records, and of the information required is a home address. By providing one's home address to a potential criminal, one exposes themselves as well as their family members to countless dangers.

The problems associated with spam are often overlooked which in turn aggravates said problems. The consequences of spam attach to both the receiver and the spammer. Firstly, it is the receiver

[9] Gmail is a free email service provided by Google with internal spam filters.

along with the internet service provider who bears the unwanted financial costs attached to spam, whereas in comparison, any such costs incurred by the spammer is of negligible value. The internet service provider bears the costs of handling, sorting, and delivering the spam to the email user. The receiver bears the financial costs of receiving the unwanted message, and the installation and maintenance costs of filtering software. Spam also causes higher subscription fees due to the increased storage capacity required by unwanted emails received by the internet service provider.[10] In addition to the ordinary email user, the "receiver" may refer to businesses, educational institutions and non-profit organisations. These institutions are at a further disadvantage in that there is a limited amount of mail that such institutions can manage without requiring further spending on infrastructure.

Secondly, the receiver's constitutionally entrenched right to privacy which includes the right not to have the privacy of their communications infringed may potentially be infringed by spam and/or the spammer.[11] Similarly a consumer's right to privacy in terms of Part B of Chapter 2 of the Consumer Protection Act (hereinafter referred to as the "CPA") may potentially be infringed.[12] Part B of Chapter 2 of the CPA encompasses the consumer's right to restrict unwanted direct marketing and provides for regulation of times for contacting consumers.[13]

The constitutional implications of spam are not restricted to the rights of the receiver; the spammer could assert a right to freedom of expression averring that in terms of section 16(1)(*b*) of the Constitution he is free to impart information or ideas. The situation therefore presents itself that the receiver's right to privacy must be weighed against the spammer's right to freedom of expression. Although this paper does not seek to explore in detail the constitutional implications of spam, the issue is briefly discussed in chapter four.

As people across the world become increasingly technologically savvy and join the electronic messaging platform, the volume of spam increases. The third quarterly spam statistics report of

[10] See section 2(3) of the US Congressional Findings and Policy of the Controlling the Assault of Non-solicited Pornography Act of 2003 (hereinafter referred to as the "CAN-SPAM Act")
[11] Section 14(*d*) of the Constitution of the Republic of South Africa, 1996 (hereinafter referred to as the "Constitution")
[12] Consumer Protection Act 68 of 2008
[13] Section 11-12 of the CPA

2013 produced the result that during 2013 spam consisted 68.3 per cent of email traffic. [14] To the email user, the receipt of a large amount of spam creates a risk that legitimate emails will be overlooked or discarded amidst the larger volume of spam. The convenience and efficiency of email has therefore been threatened by the rapid growth in the volume of spam.

In its third quarterly report Kaspersky Lab concluded that in 2013 one of the most common malware distribution tricks used was high-profile news stories and design emails in the form of newsletters. Malware refers to malicious software which is designed to damage a computer system. Interestingly, the report found that events which generated much public interest in 2013 such as the birth of the royal baby in the United Kingdom were used by fraudsters to distribute malware. The interest of a person is often captivated by current events; the spammer uses this information to his advantage and to the detriment of the receiver of the spam.

Countries with legislative measures used to combat spamming would include either an 'opt-out mechanism' or an 'opt-in mechanism' in said legislation. The opt-out mechanism requires the receiver of the spam to take action to be excluded from future mailings. This right is often exercised via the use of an 'unsubscribe' option contained in the message. The unsubscribe option is usually provided by means of a link to follow or contact details to which one would communicate his preference to not receive future mailings. The opt-in mechanism is a method whereby the consumer agrees to receive the spam; the consumer can thereafter limit the intake of messages. Prior to this agreement, the spammer may not send spam to that consumer. With regard to the opt-in mechanism the receiver can be said to have a prior relationship with the marketing company in the course of which he or she receives newsletters or advertisements from that company[15].

Unlike other countries such as Australia, Canada, New Zealand and the United States of America, South Africa has no specific anti-spam legislation. South African legislation with spam as a secondary concern encompasses the opt-out mechanism whereas a new Act which is yet to commence, being the Protection of Personal Information Act (hereinafter referred to as POPI)

[14] For the full report see Kaspersky lab Quarterly Spam Statistics Report Q3 – 2013 at http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q3-2013#.VBmOuvmSwkO accessed on 29 August 2014.
[15] Tladi (Note 5 above) 185

employs the opt-in mechanism.[16] Both mechanisms employed by South African legislation will be critically discussed under chapter two and chapter four.

[16] Protection of Personal Information Act 4 of 2013

CHAPTER 2

THE CURRENT SOUTH AFRICAN POSITION

At the time of writing, a limited amount of sections in POPI have already commenced.[17] These sections are the definitions[18] (this section does not create any laws itself, but is necessary for the application and understanding of other sections in POPI); the establishment of the Information Regulator[19]; the general provisions regarding regulations[20] and the procedure for making regulations[21]. A commencement date for the rest of POPI has not yet been set. A grace period will follow a commencement date. Prior to the commencement of the rest of POPI, the position regarding the regulation of unsolicited communications which is governed by the Electronic Communications and Transactions Act (hereinafter referred to as the ECTA), the Consumer Protection Act (hereinafter referred to as the CPA) and the CPA Regulations will remain in effect. [22]

This chapter explores the current protection afforded to the receiver of unsolicited communications bearing in mind the underlying question of whether change in terms of legislative intervention is warranted. A brief discussion of the Electronic Communications and Transactions Act Amendment Bill[23] will also be embarked upon in this chapter.

2.1 The Electronic Communications and Transactions Act

The ECTA is one of many sources of law which regulate electronic communications and transactions and for this reason the ECTA must not be read in isolation of other relevant statutory and common law. The ECTA was promulgated on 2 August 2002 and came into force on 30 August 2002. The primary objective of this Act is 'to enable and facilitate electronic

[17] Gazette 37544, Regulation Gazette 10173, Proclamation 25 (2014)
[18] Section 1 of POPI
[19] Part A of Chapter 5 of POPI
[20] Section 112 of POPI
[21] Section 113 of POPI
[22] Electronic Communications and Transactions Act 25 of 2002; Consumer Protection Act 68 of 2008
[23] The Electronic Communications and Transactions Amendment Bill [2012]; The Bill was published on the 26th of October 2012.

communications and transactions in the public interest'[24]. For this purpose, it is significant to note that the aims of the ECTA are, inter alia, to 'remove and *prevent* [my emphasis] barriers to electronic communications and transactions...'[25], to 'ensure that electronic transactions in the Republic conform to the *highest international standards* [my emphasis]'[26] and 'develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions'[27].

The ECTA applies to all electronic transactions and data messages except those excluded by the Act itself[28] or its schedules[29]. 'Electronic communications' is defined in this Act as 'a communication by means of data messages'. In addition, 'data' is defined as 'electronic representations of information in any form'. 'Transaction' is defined as 'a transaction of either a commercial or non-commercial nature, and includes the provision of information and e-government services'.[30]

Chapter VII deals with the consumer protection aspects of the ECTA and contains section 45 which represents the starting point in any matter regarding the receipt of unsolicited commercial communications. At the outset it should be stated that the ECTA does not prohibit the act of spamming; it merely attempts to regulate it.

Section 45 of the ECTA is as follows:

> *"(1) Any person who sends unsolicited commercial communications to consumers, must provide the consumer:-*
>
> *(a) with the option to cancel his or her subscription to the mailing list of that person; and*
>
> *(b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on the request of the consumer.*

[24] Section 2(1) of the ECTA
[25] Section 2(1)(d) of the ECTA
[26] Section 2(1)(h) of the ECTA
[27] Section 2(1)(j) of the ECTA
[28] Section 4 of the ECTA
[29] Schedule 1 and 2 of the ECTA
[30] Section 1 of the ECTA

(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.

(3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1).

(4) Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1)." [31]

Section 1 of the ECTA defines personal information as meaning 'information about an identifiable individual, including, but not limited to: information relating to race, gender, sex,... the address, fingerprints; the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about that individual'. The definition of 'personal information' is broad and even extends to 'any identifying number, symbol or other particular assigned to the individual'.[32] This ranges from one's national identification number to one's Twitter™[33] handle.

Section 45 implies that the sending of spam is allowed in South Africa with the exception that once the consumer notifies the sender that he no longer wishes to receive such messages the sender must remove the consumer from his mailing list. In other words, the initial sending of the spam message is allowed in terms of South African law, however once the consumer requests the spammer to stop sending such messages, any further messaging is prohibited. The employment of the opt-out mechanism in section 45 has become the main critique of the ECTA in terms of combating spamming, reason being; spammers are somewhat encouraged by the ECTA's choice to regulate spamming instead of prohibiting it.

2.1.1 Discussion of section 45 of the ECTA

The use of the term 'unsolicited' in section 45 simply implies that no prior relationship between the sender and recipient exists, furthermore the recipient has not consented to receive the

[31] Failure to comply with the requirements contained in section 45 is an offence in terms of section 89(1) of the ECTA with penalties that include fines and imprisonment of up to twelve months.
[32] Section 1(c) of the ECTA
[33] Twitter™ is an online social networking service that allows users to send and read short messages called "tweets". Registered users can read and post tweets. Users mostly access Twitter through the website interface or its mobile application which can be downloaded via the Google Play Store or Apple iStore.

communication or has not previously terminated the relationship by requiring the sender to remove the recipient's details from the database.

Section 45 covers both bulk and individual transmissions. Commerciality of the communication is a prerequisite for the protection afforded under section 45. A commercial communication relates to messages with a primary purpose of advertising or promoting goods or services. Non-commercial communications include religious and political messages, urban legends, chain-letters and news. Therefore, the ECTA affords no protection to the recipient of a non-commercial communication. This has been common practice in many other foreign jurisdictions.[34]

Section 45 will only apply to an electronic transaction where one party is a "consumer". A consumer is defined as "...any natural person who enters or intends entering into an electronic transaction with a supplier, as the *end-user* [my emphasis] of the goods or services offered by that supplier"[35]. This definition would exclude a situation whereby one acquires goods for the purpose of re-selling to another consumer. It should be noted that a consumer will still enjoy protection of section 45 if he merely intends on entering into an electronic transaction with a supplier; this would include a situation whereby a consumer browses weekly Groupon[36] deals.

There is no definition of an "electronic transaction" in the ECTA. After considering the definitions of "electronic communication", "electronic agent" or "electronic signature" Papadopoulos suggests that "electronic transactions" include transactions where the use of data is an integral element of the transaction.[37] The ECTA affords no protection to recipients of unsolicited telephone calls. This will be contrasted with the protection afforded in respect of such communications in terms of the CPA.

With regards to the scope of application of Chapter VII of the ECTA, section 42(3) provides that Chapter VII does not apply to a regulatory authority established in terms of a law if that law prescribes consumer protection provisions in respect of electronic transactions. This has been interpreted to mean that if another Act of Parliament subjects electronic consumer transactions to

[34] See further discussion on this point in Chapter 5.
[35] Section 1 of the ECTA
[36] Groupon is a couponing website where retailers provide discounts available for online orders at www.groupon.co.za accessed on 30 October 2014.
[37] S Papadopoulos "*Are we about to cure the scourge of spam? A commentary on current and proposed South African legislative intervention*" 2012 THRHR 223, 225

alternate and possibly stronger consumer protection laws then Chapter VII of the ECTA will not apply.[38]

With regards to enforcement of Chapter VII, the consumer may in terms of section 49, lodge a complaint with the National Consumer Commission for non-compliance with the consumer protection principles of the ECTA.

2.1.2 Critique and commentary

Tladi points out that the ECTA does not specify the way in which the opt-out option should be provided.[39] This leaves room for abuse of the consumer in that the sender has much freedom in the way he provides the opt-out option. The sender could attempt to draw as little attention as possible to the unsubscribe option. The vagueness of section 45 even extends to a situation whereby the sender is not obliged to provide the opt-out option in the spam message itself or via the means used to send the message and could possibly provide the option in other ways such as via telephonic communication. As has been noted, unsolicited messages via telephonic communication do not amount to spam in terms of the ECTA. Section 45 does not take cognisance of the fact that in reality many spam emails do not contain an opt-out mechanism or even if it does, the mechanism is often dysfunctional.

The opt-out mechanism requires two things to be effective, namely that the spammer respects the consumer's call to stop the spam messaging and that consumers must have the confidence in the efficacy of the opt-out mechanism.[40] It could be said that these requirements are somewhat ambitious considering the nature of spamming. With regards to consumers having confidence in the efficacy of the opt-out mechanism, consumers are often advised against exercising the unsubscribe option as the sender will not comply with the request and the attempt to unsubscribe will do more harm than good as it seeks to confirm the consumer's email address. The sender is the made aware that the consumer has received and read the message. Such confirmation is harmful to the consumer as the sender may choose to abuse this piece of knowledge in future by

[38] D P Van der Merwe *Information and Communications technology law* Durban: LexisNexis (2008) 183
[39] Tladi (Note 5 above) 186
[40] International Telecommunication Union (ITU) WSIS Thematic Meeting on Cyber security *A Comparative Analysis of Spam Laws: The Quest for a Model Law* (10 June 2005) Document CYB/03 p 20 available at http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf

seeking to evade the consumer's request by using a new email address to continue to send spam messages to the now-confirmed email address. This concern also arises in situations where the consumer requests the spammer to provide him with the identifying particulars of the source from which he obtained the consumer's personal information; such request would also amount to a confirmation of one's email address.

Spammers can evade the aims of section 45 by using false or deceptive email headers. Section 45 does not penalise the forging of email headers. Email headers show the route an email has taken in order to arrive at its destination. They also contain other information about the email including information as to the sender and recipient and the date and time of transmission. Email headers could also be used to trace back the origin of the spam message. Most spammers try to hide their identity by forging email headers or by relaying mail to hide the real source of the message. In this way the consumer cannot properly exercise his right to opt-out of future messaging because he is unable to trace the real identity of the spammer. Other related issues which have an impact on the effectiveness of the opt-out option, such as harvesting of email addresses and dictionary attacks are not addressed by the ECTA.[41]

Another known problematic characteristic of section 45 is that the onus is always placed on the consumer to request the spammer to stop sending spam to the consumer or a request to obtain information to lay a complaint. This means that if the consumer chooses not to exercise her rights then the spammer can continue to send the spam and remain unsanctioned. This in turn places the consumer in a difficult position where the unsubscribe option is dysfunctional. In essence the consumer's ability to exercise her rights in terms of section 45 are at the hands of the spammer.

Section 45 of the ECTA applies to a "consumer" as defined in the Act. A "consumer" in terms of the ECTA refers to a natural person only. In this regard, a juristic person as the receiver of spam enjoys no protection in terms of section 45 of the ECTA.

A further concern is that most spam originates from outside the South African jurisdiction. In 2013 more than half of the world's spam was distributed from three countries, namely China,

[41] Tladi (Note 5 above) 188

USA and South Korea.[42] For this reason, enforcement of the consumer's rights in terms of section 45 is problematic. It is rare that one will take the time, effort or money to find and litigate against an offender for a maximum penalty of twelve months in jail. It is more probable that the consumer would opt for the route of purchasing spam filter software, simply deleting the messages or making use of the various junk mail settings found in email messaging as this would be the more inexpensive and trouble-free option for the consumer.

What would seem to be a more pedantic concern is that section 89 of the ECTA lists a number of sections to which penalties apply, of which section 45 is not listed. It seems as if the Act has created a criminal offence for an act for which a penalty does not exist.

A further critique is that spamming as a general nuisance is not prohibited by the ECTA. Protection is only extended in terms of electronic communications with an end goal of some commercial gain.

For all these reasons it cannot be said that section 45 of the ECTA has been drafted in furtherance of one of the specific aims of the Act namely to "ensure that electronic transactions in the Republic conform to the "*highest international standards*".[43] It is submitted that in this day and age where emphasis is constantly placed on consumer protection, by itself section 45 of the ECTA provides a weak and inadequate standard that spammers are required to comply with. This weak standard is to the detriment of consumer protection.

The opt-out regime as provided for in the ECTA is lacking in many respects.[44] Ebersöhn is of the opinion that section 45 of the ECTA "lags behind corresponding legislation".[45] He proposed recommendations for the amendment of the ECTA. Of these recommendations, he states that the South African government should regularly review the effectiveness of section 45 of the ECTA. This view is supported by the fact that Australian and North American spam legislation mandate the respective legislatures to review the effectiveness of legislation relating to spam within certain periods after it comes into operation.[46] It is submitted that the need to regularly review

[42] Kaspersky lab Quarterly Spam Statistics Report Q3 – 2013 at http://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q3-2013#.VBmOuvmSwkO accessed on 30 August 2014
[43] Section 2(1)(*h*) of the ECTA
[44] As discussed above in paragraph 2.1.2
[45] G Ebersöhn 'An Analysis of Spam Legislation' (2004) 12(3) *Juta's Business Law* 134, 142
[46] Ibid 142

legislation and regulation regarding electronic communications and transactions is derived from the nature of such communications. Technology is fast-paced and ever-changing. To meet the needs of consumers and the economy legislative measures need to keep up with the constant change.

2.2 The Consumer Protection Act and Its Regulations

The CPA came into effect on 31 March 2011. Prior to the commencement of the National Credit Act (hereinafter referred to as the NCA)[47] and the CPA there existed no comprehensive body of law designed specifically to deal with consumer protection. Consumer protection measures and principles existed largely through self-regulation and the common law. In response to the argument that the introduction of the CPA and the NCA will overburden the South African economy and will lead to significant costs for business, Woker has successfully argued that this proposition ignores the lived reality of the South African people and that South Africa has indeed been in dire need of a comprehensive body of law dealing with consumer protection.[48] Predictably the CPA was greatly welcomed by, among others, South African consumers and legal academics.

The CPA's purpose and policy entails the promotion of the social and economic welfare of South African consumers by inter alia promoting fair business practices and protecting consumers from unconscionable, unfair, unreasonable, unjust or otherwise improper trade practices and deceptive, misleading, unfair or fraudulent conduct.[49] The Act introduces many enforceable fundamental consumer rights.[50]

[47] National Credit Act 34 of 2005
[48] T Woker '*Why the need for consumer protection legislation? A look at some of the reasons behind the promulgation of the National Credit Act and the Consumer Protection Act*' 2010 (31) 2 217, 230
[49] Section 3(1)(*c*)-(*d*) of the CPA
[50] Chapter 2, Parts A-I, sections 8-67 of the CPA

The CPA applies to every transaction occurring in South Africa including the promotion, performance or supply of goods or services, the goods and services themselves and the goods that are part of an exempted transaction.[51]

2.2.1 Important definitions used in the CPA

A proper explanation of the application of the Act requires explanation of some key terms:

- "consumer"

The consumer includes both natural person consumers and small to medium-sized juristic person consumers whose asset value or annual turnover at the time of the transaction is less than the monetary threshold of two million rand, to whom goods and services are marketed, who have entered into transactions with suppliers, in the ordinary course of business of the supplier. It may also include a user, recipient or beneficiary of the goods or services and a franchisee.[52]

- "transaction"

Transaction refers to one in respect of a person acting in the ordinary course of business which is an agreement between or among that person and one or more other persons for the supply or potential supply of any goods or services in exchange for consideration; or the supply by that person of any goods to or at the direction of a consumer for consideration; or the performance by, or at the direction of, that person of any services for or at the direction of a consumer for consideration.[53] The definition of "consideration" is broad in that it relates to anything of value, given and accepted, in exchange for the goods and services.[54] In terms of section 5(6) of the CPA certain 'deemed transactions' are regarded as a transaction between a supplier and consumer for the purposes of the Act.

[51] Section 5(1) of the CPA; In terms of section 5(1)(*d*) and section 5(5) if any goods are supplied within the Republic to any person in terms of an exempted transaction (exempted transactions are listed in s 5(2)-(4)), the goods and importer or producer, distributor or retailer are still subject to sections 60 and 61 which relates to safety monitoring, recall and strict product liability
[52] Section 1 of the CPA
[53] Section 1 of the CPA
[54] Section 1 of the CPA

- "goods" and "services"

Goods "…*includes* [my emphasis] anything marketed for human consumption, any tangible object including any medium on which anything is or may be written or encoded, any literature, music, data…or other intangible product written or encoded on any medium, or a licence to use any such intangible product, a legal interest in land or any other immovable property, other than an interest that falls within the definition of 'service'…" Services "…*include* [my emphasis] any work or undertaking performed by one person for the direct or indirect benefit of another, the provision of education, information, advice or consultation…access to electronic communication infrastructure…"[55]

The use of "includes" prefers a situation whereby the concerned provision is not limited to the given examples meaning that a broad interpretation is required.

2.2.2 The implications of the CPA and its Regulations on direct marketing

Section 1 of the CPA defines "direct marketing" as an approach to a person, either in person or by mail or by electronic communication for the direct or indirect purpose of promoting, offering to supply, in the ordinary course of business, any goods or services or to request a donation of any kind. An "electronic communication" is further defined as a communication by means of electronic transmission including telephone, fax, SMS, wireless computer access, email or similar technology or device.[56]

The definition of "electronic communication" is to be contrasted with the definition of the same term in the ECTA.[57] It seems that under the CPA the legislator bore the intention of specifically including regulation of direct marketing via telephonic communications and postal services whilst this type of protection is not afforded in terms of the ECTA. Communications via telephone could be seen as a direct method of communication to which the information theory is applied for the determination of the time and place for the conclusion of the contract.[58] The information theory states that the agreement is concluded when and where the offeror learns or is

[55] Section 1 of the CPA
[56] Section 1 of the CPA
[57] See the discussion of "electronic communication" in the ECTA under paragraph 2.1
[58] Van der Merwe (Note 38 above) 148-150

informed of the acceptance.[59] The ECTA however deals with forms of indirect communication to which the reception theory is applied.[60] In contrast the reception theory provides that agreement is reached when acceptance reaches the address of the offeror.[61]

Section 11 of the CPA provides that a consumer has the right to refuse to accept, require another person to discontinue or in the case of an approach other than in person, to pre-emptively block any approach or communication if the approach or communication is primarily for the purpose of direct marketing.[62] Any opt-out request or pre-emptive block must be respected by the direct marketer[63] and confirmed in writing on receipt.[64] Furthermore the exercise of these rights must be performed free of charge.[65]

To facilitate section 11 of the CPA, the National Consumer Commission (hereinafter referred to as the Commission)[66] *may* establish a registry where a person may register a pre-emptive block against direct marketing communications and appropriate procedures must be implemented to facilitate demands to stop future communications.[67] To build on the striking feature of a pre-emptive block schedule 4 (3)(*g*) of the CPA Regulations provides that a direct marketer must, without exception assume that a comprehensive pre-emptive block has been registered by a consumer unless the administrator of the registry has in writing confirmed that the pre-emptive block has not been registered.[68] This will be discussed further below.

2.2.3 Critique and commentary

Application of the CPA is not limited to natural persons; it includes certain juristic persons. As a result, the application of the CPA is wider than that of the consumer protection provisions found

[59] Hutchison et al *The law of contract in South Africa* Cape Town: Oxford University Press (2009) 57
[60] Section 22(2) of the ECTA
[61] Hutchison et al (Note 59 above) 57
[62] Section 11(1)(*a*)-(*c*) of the CPA
[63] Section 11(4) of the CPA, the "direct marketer" in this respect refers to a person authorising, directing or conducting any direct marketing.
[64] Schedule 4(1)(a)-(b) of CPA Regulations GN 293 in GG 34180 (1 April 2011) (CPA Regulations)
[65] Schedule 4(3)(b) of CPA Regulations
[66] Established by section 85 of the CPA
[67] Section 11(3)-(4)(*a*) of the CPA
[68] Schedule 4(3)(g) of CPA Regulations

in Chapter VII of the ECTA. Unfortunately, like the ECTA the CPA does not address the problems associated with misleading or false email headers.[69]

With regards to the establishment of a registry where a consumer may register a pre-emptive block against direct marketing communications, the wording of the CPA and its Regulations creates the impression that establishment of such an institution is not definite nor is there any obligation to establish such an institution found in the Act. Section 11(3) of the CPA simply states that the Commission "may" establish such a registry. Furthermore schedule 4(5) of the CPA Regulations provides that "*In the event that* [my own emphasis] the Commission recognises a registry as authoritative as contemplated in section 11(3) of the Act…" this wording connotes a possibility that the registry *could* be established rather than a definite obligation on the part of the Commission. At the time of writing the registry as contemplated in section 11(3) of the CPA has not been formed. This in turn creates an issue relating to the lack of enforcement of the consumer's rights in terms of section 11. Although the Commission has not established a national opt-out registry, other registries including the Direct Marketing Association of South Africa (DMA)[70] are currently in existence. Members of the DMA are required to consult the DMA database. Non-members are not bound by the rules of the DMA therefore the registry's effectiveness is not all-encompassing.

Papadopoulos and Hamann argue that the scope of protection afforded by the CPA differs from the protection afforded in terms of section 45 of the ECTA, since in terms of the CPA, protection is granted for "direct marketing" via an electronic communication as well as requests for donations of any kind whereas the ECTA relates only to unsolicited commercial electronic communications. "Unsolicited commercial electronic communications" is wider than a "direct marketing communication".[71] Herein lays a further critique; in terms of the CPA, protection is limited to the narrower, non-preferred concept of direct marketing.

[69] See critique and commentary of section 45 of the ECTA above at paragraph 2.1.2
[70] Some key members of the association which are also founding members of the association include ABSA and Nedbank Ltd. For more information about the Direct Marketing Association of South Africa see http://www.dmasa.org/home/about-us/ accessed on 13 October 2014.
[71] B Hamann; S Papadopoulos *'Direct marketing and spam via electronic communications: an analysis of the regulatory framework in South Africa'* 2014 (47) 1 De Jure 42, 54

2.3 The ECT Act Amendment Bill

Despite the intention that POPI will repeal section 45 of the ECTA, the Department of Communications published the proposed Electronic Communications and Transactions Act Amendment Bill (hereinafter referred to as the ECT Amendment Bill) wherein it is suggested that section 45 be retained or re-enacted, although in an amended form.[72]

The ECT Amendment Bill brings about a new definition of "consumer" to include natural and certain juristic persons. These persons will enjoy the protection of Chapter VII of the ECTA.[73] A definition of "electronic transaction" is introduced and refers to a transaction conducted using electronic communications. Furthermore, an unsolicited communication in relation to a data message regarding goods or services has been defined as a data message that is transmitted to a consumer by or on behalf of a supplier without the consumer having expressly or implicitly requested that data message.

The ECT Amendment Bill proposes that section 45 be amended to be read as follows:

> *"(1) No person may send unsolicited communications without the permission of the consumer to whom those unsolicited communications are to be sent or are in fact sent.*
>
> *(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.*
>
> *(3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence, and liable, on conviction, to a fine not exceeding R1 million or imprisonment for a period not exceeding 1 year."*

As will be seen under the discussion of POPI in chapter 4, the ECT Amendment Bill does not materially alter the position; the proposed amendment encompasses an opt-in regime in terms of data messages regarding goods and services which is essentially the same as unsolicited commercial emails.

[72] The ECT Amendment Bill (Note 23 above)
[73] See definition of "consumer" under paragraph 2.2.1

CHAPTER 3

JUDICIAL INTERPRETATION OF THE CURRENT LAWS RELATING TO SPAMMING; THE *KETLER* CASE

Legal disputes relating to spam issues rarely reach the courts for binding decisions. In weighing up the advantages and disadvantages of instituting an action of this matter, one is often inclined to lean towards more practical solutions such as purchasing and installing spam filter software. For this reason, legal academics are deprived of judicial interpretations of the various laws relating to spam. This creates the difficult task of lending our own interpretations to the laws relating to spam until they are built upon through case law and setting of precedents.

Recently the South Gauteng High Court shone light on this area of law through what has been described as a "landmark spam court case"[74] in South African law, namely *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association* (hereinafter referred to as the "Ketler case").[75] A thorough discussion of this case is therefore warranted. The discussion of this case will be limited to the applicable issues set out and addressed in this research paper.

3.1 The Facts

The applicant ("Ketler") utilised an independent internet service provider to send bulk emails to recipients. The respondent (Internet Service Providers' Association) hereinafter referred to as the "ISPA", has a website containing a webpage titled "*Hall of Shame*" listing those whom it claims are spammers. Ketler's name appeared on the list. Ketler brought an application for the removal of its name from the webpage and an application to interdict its relisting. Ketler contended that

[74] The Internet Service Providers' Association has described the case as such on its website at http://ispa.org.za/press-release/ispa-concludes-landmark-spam-court-case/ accessed on 29 August 2014. Interesting to note is that this very association was the respondent in the case.
[75] *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association* 2014 (2) SA 569 (GJ)

placing its name as a spammer on the respondent's "Hall of Shame" webpage was defamatory. On this basis Ketler relied on three submissions:[76]

a) Spamming is not prohibited in South Africa; it is merely regulated by section 45 of the ECTA and Ketler had fully complied with this section;

b) Ketler was not a member of the ISPA and was therefore not subject to the latter's code of conduct in so far as the code may allow the respondent to list spammers on its Hall of Shame. Furthermore it submitted that, on the facts, even if it was a member of the ISPA, the ISPA would not have been entitled to list the applicant as a spammer.

c) Although it had signed an undertaking required by the ISPA not to spam, the undertaking was not legally binding and in any event it was withdrawn.

In response, the respondent relied on the defences of consent, qualified privilege and truth and public interest.

3.2 Commentary

The respondent presented uncontradicted evidence that several consumers had made written requests to the applicant under section 45(1)(*b*) of ECTA, for the identifying particulars of the source from which the applicant had obtained the recipient's personal information. These details were not provided.

Undisputed evidence was presented to court in relation to the applicant's activities of sending unsolicited advertising emails to at least;

a) a "*spamtrap* address"; and

b) a "role email account".[77]

[76] Ibid para 7; Ketler also contended that it was entitled to procedural regularity before being relisted on the Hall of Shame and that the ISPA failed to follow its own complaint procedure laid out in its Code of Conduct (para 8).
[77]Ketler (Note 75 above); these terms are defined at paragraph 57 of the judgment.

A "*spamtrap* address" as it suggests, is used to lure spam. It is an address without a user. A spammer could not successfully argue that he obtained such an address from a person who requested such emails or that a prior relationship existed between the spammer and the user of the "*spamtrap"* email address.

Undisputed evidence showed that the applicant had sent bulk unsolicited emails to a role email account which was set up for the sole purpose of soliciting public comment regarding the re-delegation of the ".za" country code top-level domain to the ".za *Domain Name Authority"*. The characteristic of this type of email address is that it is used for a specific function. A common example is an email address which begins with "info@". This would imply that the address is not associated with a particular person; it is usually associated with a company. As with the "*spamtrap*", this email address could not have been harvested by the applicant in any lawful manner.

In his judgment Spilg J goes into great detail of the effects of spamming on internet service providers, consumers as well as the internet industry as a whole.[78] Emphasis is placed on the costs and inconvenience borne by the recipient of spam.

The learned judge observes that the ECTA recognises both the advantages and pitfalls of electronic communications. This recognition is implicitly expressed in the objects of the ECTA where it is stated that investment and innovation in the field of electronic transactions is encouraged while at the same time promoting the industry's development in a manner that is not only effective for consumers but responds to the needs of users and consumers.[79] The learned judge further states that there is no reason to believe that our legislature would not have been cognisant of these advantages and pitfalls of electronic communications when considering the drafting of the ECTA.[80] Perhaps this statement connotes an underlying assumption that Spilg J considers the provisions of the ECTA to be properly effective in dealing with issues such as those before the court in this case.

Of significant relevance to this discussion is the fact that the ECTA provides not only a legislative framework but also establishes a self-regulatory framework for information system

[78] Ketler (Note 75 above) para 26-29; 65-66
[79] Section 2(1)(*i*) and section 2(1)(*k*) of the ECTA
[80] Ketler (Note 75 above) para 30

service providers. In terms of section 71 of Chapter XI of the ECTA (titled "*Limitation of Liability of Service Providers*") an industry representative body for service providers may be recognised as such by the Minister of Communications provided, inter alia, membership of the body is subject to adequate criteria, members are subject to a code which provides for adequate standards of conduct and the representative body is capable of monitoring and enforcing its code of conduct adequately.[81] The ISPA has been recognised as such a representative body under section 71 of the ECTA.

The Guidelines for Recognition of Industry Representative Bodies of Information System Providers[82] (hereinafter referred to as the ECT IRB Guidelines) places emphasis on control for self-regulation by the industry rather than government regulation and intervention.[83] Spilg J recognises that the focus on self-regulation is consistent with the intention of the legislature as expressed in the body of the ECTA.[84] It is submitted that this statement is made in view of Chapter XI of the ECTA; namely the provisions relating to the recognition of representative bodies within the industry.

It is important to note that the provisions of Chapter XI or any other provisions of the ECTA are not to be construed as prohibiting a person from establishing requirements in respect of the manner in which that person will accept data messages.[85] This is consistent with the large emphasis that has been placed on self-regulation. A service provider would not be able to successfully argue that section 45 of the ECTA is only the standard that the service provider is to be held to and nothing more; the ECTA clearly allows a self-regulatory regime to co-exist alongside legislative sanctions.

Section 5 of Part 1 of the ECT IRB Guidelines provides the minimum requirement that members of an industry representative body such as the ISPA "...shall not send or promote the sending of spam and will take reasonable measures to ensure that their networks are not used by others for this purpose. Members must also provide a facility for dealing with complaints about spam

[81] Section 71 of the ECTA is to be read with the definition of "service provider" in section 70.
[82] Gazetted under GN 1283 in GG 29474 of 14 December 2006 (ECT IRB Guidelines)
[83] Ibid Part 1 paragraph 1.2
[84] Ketler (Note 75 above) para 75
[85] Section 4(2) of the ECTA

originating from their networks and must react expeditiously to complaints received."[86] It is also provided that members "...shall follow best industry practice in providing anti-spam software to recipients of the service in order that they can elect to minimise the amount of spam received on their email accounts."[87] The use of "shall" as opposed to "may" connotes wording of a peremptory obligation.

Spilg J states that as a result of the industry representative bodies' obligation to provide anti-spam software, the Ketler judgment, regarding the defamatory nature of the applicant's listing on the Hall of Shame, should not be construed as relevant to cases where internet service providers may utilise spam software or adopt spam countermeasures.[88]

Section 2 of Part 1 of the ECT IRB Guidelines further provides that the industry rather than the State should regulate and control both illegal and unacceptable conduct and content [my emphasis] by internet service providers. "Unacceptable conduct and content" is independent of illegal conduct and content; it is thus capable of a broad interpretation extending industry regulation and control over a number of acts or omissions. In this way a consumer is given extensive protection (by legislation and industry-regulation). However, the problem often lies in the fact that the associations of the industry which regulate and control such conduct and content are only able to exercise control over members of said associations and not non-members. The control is therefore exercised on a voluntary basis.

Industry players are somewhat persuaded to become members of these types of associations to maintain goodwill with its customers. Also, industry players such as Ketler would only be able to rely on the limitation of liability provisions in terms of Chapter XI of the ECTA if it was a member of a representative body referred to in section 71 (such as the ISPA). In addition it would be required to adopt and implement the code of that representative body.

Spilg J finds that the ISPA's Code of Conduct will apply until such time as an industry code is prescribed under the CPA to deal with matters arising from the CPA.[89] If there is an overlapping

[86] ECT IRB Guidelines (Note 82 above) para 5.8.1 - 5.8.2
[87] ECT IRB Guidelines (Note 82 above) para 6.8
[88] Ketler (Note 75 above) para 53
[89] On 9 May 2013 a proposed Industry Code was published for comment by the National Consumer Commission (Notice 451 of 2013; No. 36439). The Code provides an elaborate complaint process in section F.

between the CPA and the ECTA, the code of conduct provided for in the ECTA "is intended to serve the same purpose as contemplated in the CPA until amended..."[90]

In terms of the ISPA's Code of Conduct, members are not to send or promote the sending of unsolicited bulk email and must take reasonable measures to ensure that their networks are not used by others for this purpose.[91] It is further provided that members must provide a complaint facility regarding unsolicited bulk email and unsolicited email communications that do not comply with the provisions of section 45(1) of the ECTA originating from their networks and must react expeditiously to complaints received.[92] In essence the ISPA's Code of Conduct largely encompasses the ECT IRB Guidelines.

It is submitted that the ISPA's Code of Conduct has taken up adequate measures in contributing towards eliminating spam. For example, the requirement that the members of the association are not to promote the sending of unsolicited bulk email goes beyond section 45 of the ECTA. This is an illustration that self-regulation of the internet industry could prove to be more successful in certain respects of combating spamming than the legislative measures held in place to regulate spamming. For a successful fight against spam, regulation needs to be afforded to the promotion and facilitation of spamming. Facilitation of spamming has been addressed by Canadian anti-spam legislation.[93]

3.3 The Court's Findings

Spilg J found that in the circumstances, listing a sender of unsolicited bulk commercial email on a webpage titled "Hall of Shame" by a recognised representative body in the internet industry such as the ISPA was defamatory in its secondary meaning.[94] The word "spammer" by itself will not constitute defamatory matter; the context is essential in making a determination.

[90] Ketler (Note 75 above) para 79
[91] Section 14 of Part E of the ISPA's Code of Conduct
[92] Section 15 of Part E of the ISPA's Code of Conduct
[93] Canada's Anti Spam law S.C. 2010, c. 23; this will be discussed further in terms of a comparative analysis under chapter 5.
[94] Ketler (Note 75 above) para 55

However, it was found that Ketler's failure to adhere to requests for the particulars of the source from which it had obtained recipients' personal information amounted to a contravention of section 45(3) of the ECTA.

The learned judge further found that the defence of truth and public benefit/interest to be successful in the circumstances on the following bases:

- the respondent was able to demonstrate truth of content both under ECTA and the broader industry definition of spamming as applied in its code of conduct[95];
- the respondent's code of conduct is part of the self-regulatory framework sanctioned under the ECT IRB Guidelines; and
- 'public benefit' was demonstrated by reference to the respondent's status as an industry self-regulatory under ECTA and the public interest it serves in dealing with spam.[96]

The defence of consent was also upheld.[97] The defence of qualified privilege was not considered.

3.4 Concluding remarks

In the Ketler case there was no appearance for the applicant when the matter was set-down for hearing. As a result the judgment does not have the benefit of full argument. Spilg J recognises that this very situation may have possibly produced a judgment of "diluted value".[98] For this reason the judgment should not be considered as the final say on future cases with similar issues. Future parties could raise other applicable arguments. For example, in this case, Ketler could have raised the defence of improper motive (in the form of malice or otherwise).

The judgment is nevertheless of significant value as it has created a starting point in the formation of spam law jurisprudence. We are no longer deprived of judicial interpretation of section 45 of the ECTA and of the overall issues associated with spam in the South African

[95] Ketler (Note 75 above) para 61
[96] Ketler (Note 75 above) para 71-83
[97] Ketler (Note 75 above) para 98; the defence of consent was upheld on the basis that the applicant's purported withdrawal of consent only after the defamatory matter was published was irrelevant, as long as the consent remained extant, the respondent was entitled to rely on it in order to relist the applicant's name.
[98] Ketler (Note 75 above) para 6

context. The judgment has shed light on concepts such as "*spamtraps*" and role-based email addresses.

Allowing for a self-regulatory regime to co-exist alongside legislative measures and government intervention is a step in the right direction towards combating the issue of spamming. Self-regulatory measures have the potential to seep into problematic areas which would ordinarily be out of reach for government. Government may also lack the funds to initiate and maintain comprehensive combative measures aimed at spamming. Furthermore, regulatory bodies such as the ISPA have the potential to influence telecommunications policy in South Africa.

If a complainant approaches a regulatory body wishing to file a complaint against a non-member of that body, the complainant will have no recourse because the service provider is not a member of the regulatory body. It is possible that the complainant would choose to move their business to a member of the body as such member is required to comply with a higher standard of practice as evidenced in the regulatory body's code of conduct. In this way, the internet industry players are held to a higher standard of practice which over time benefits South African consumers.

CHAPTER 4

THE DAWNING OF THE PROTECTION OF PERSONAL INFORMATION ACT

This chapter seeks to discuss the newly enacted POPI in relation to spamming and the protection it affords to the consumer or the data subject. Focus will be placed on a comparison of POPI and the current position in our law which was discussed in chapter two. To understand the importance of the emergence of POPI, one needs to set out key background information as to how POPI came about.

4.1 Background information

At its 89th meeting held on 17 November 2000 the South African Law Commission (hereinafter referred to as the "Commission") approved the inclusion in its programme the investigation entitled "Privacy and Data Protection". The inclusion of the investigation was thereafter confirmed by the Minister for Justice and Constitutional Development.[99]

The reason behind the decision to embark on an investigation into privacy and data protection stemmed from the Report of the Ad Hoc Joint Committee on the Open Democracy Bill[100] (the Open Democracy Bill became the Promotion of Access to Information Act).[101] This report which is referred to as the "Report on the Open Democracy Bill" stated that the Open Democracy Bill did not regulate all aspects of the right to privacy such as the correction, control and dissemination of personal information; instead it dealt with the aspect of access to private information of an individual. It further stated that other countries have enacted both access to information legislation and separate privacy and data protection legislation.

[99] This confirmation was given on 8 December 2000. The members of the Project Committee for this investigation included among others The Honourable Mr Justice CT Howie, Prof J Neethling and Prof I Currie.
[100] Ad Hoc Joint Committee of South African Parliament *Report of the Ad Hoc Joint Committee on the Open Democracy Bill* [B67-98], 24 January 2000, as published in the Announcements, Tablings and Committee Reports of Parliament (Report on the Open Democracy Bill)
[101] Promotion of Access to Information Act 2 of 2002

The Ad Hoc Joint Committee requested the Minister to introduce privacy and data protection legislation in Parliament "after thorough research of the matter and as soon as reasonably possible".[102] Thereafter the Minister approached the Commission to consider the inclusion of such an investigation in its programme. The Commission produced Discussion Paper 109 which included preliminary findings of the investigation and called upon parties to deliver comment with respect to said findings.[103] In 2009, a report of the Commission's final findings and recommendations, including draft legislation was submitted to the Minister of Justice and Constitutional development.[104] This will be discussed below.

4.2 The Report on Privacy and Data Protection

The report begins by emphasising the importance of the right to privacy in South Africa by highlighting the fact that the right enjoys common law protection and significant constitutional protection. It is further stated that data or information protection forms an element of safeguarding a person's right to privacy.[105]

The investigation into information protection legislation in South Africa is, according to the Commission, in line with international standards as more than fifty countries (at the time the report was drafted) have enacted information protection statutes and the number of such countries has been gradually increasing.

The Commission makes the significant finding that even though information protection laws of foreign jurisdictions vary; the common denominator among the differing legislative regulations is a reliance on Principles of Information Protection. This common reliance can be translated into POPI's eight conditions to be met for the lawful processing of personal information found in chapter three.[106]

---

[102] Report on the Open Democracy Bill (Note 100 above) para 4, page 17

[103] SA Law Reform Commission Discussion Paper 109, Project 124 *Privacy and Data Protection* Pretoria: SALRC, (2005)

[104] SA Law Reform Commission Report *Privacy and Data Protection* Pretoria: SALRC (2009) ("Report on Privacy and Data Protection")

[105] Ibid Page vi

[106] These principles are: accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation. These principles will be discussed further below at paragraphs 4.8.1 – 4.8.8

Another reason given for legislative reform is that South Africa's inability to provide adequate information protection of international standards could create barriers to international trade.[107] This was a significant consideration at the time the report was compiled by the Commission as South Africa anticipated the 2010 FIFA World Cup.

4.2.1 Summary of the Report's recommendations which are relevant to this research paper: [108]

- A general information protection statute will regulate privacy and information protection. This will be supplemented by codes of conduct for the various sectors and will be applicable to both the public and private sector. Both automatic and manual processing will be covered. Identifiable natural and juristic persons will enjoy protection.

- General principles of information protection have been incorporated in the legislation; these are eight core information protection principles. Provision is made for exceptions to the principles and exemptions are possible in certain circumstances. Special provision has been made for the protection of sensitive personal information.

- A statutory regulatory agency namely an independent Information Protection Regulator is to be established.

- A flexible approach should be followed in which industries will develop codes of conduct in accordance with the core principles set out in the legislation. This will be overseen by the Information Protection Regulator.

- The legislation makes provision for the protection of data subjects' rights in terms of unsolicited electronic communications and automated decision making.

[107] Report on Privacy and Data Protection (Note 104 above) Page vii; For example, article 25 and 26 of the European Union Data Protection Directive (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) ("EU Data Protection Directive"), provides that personal data should only flow outside the boundaries of the European Union to countries that can guarantee an "adequate level of protection".
[108] Report on Privacy and Data Protection (Note 104 above) Page viii

- The legislation prohibits the transfer of personal information to countries that do not ensure an adequate level of information protection.

The Commission's recommendations are largely in keeping with international trends with regards to information protection legislation. For example, the notion of prohibiting the transfer of personal information to countries that do not ensure an adequate level of information protection is a key feature of the EU Data Protection Directive.[109] Also, as it has been mentioned above, the establishment of information protection principles has become a trite trait of foreign information protection legislation.

The South African approach to information protection is also evident in the recommendations; the recommendation for 'a flexible approach' is in line with the ECTA's emphasis placed on self regulation of the internet industry. The Commission's recommendations which make provision for the protection of data subjects' rights in terms of unsolicited electronic communications is not by itself seen as an advancement in terms of data protection laws as it has been provided for previously. However, the specific sections regarding spam in POPI and what it seeks to provide will be considered an *improvement* on the current South African position.

4.3 Preliminary Observations of POPI:

As it has been mentioned above, POPI has been passed into law and a limited amount of sections have already commenced.

In its preamble, POPI explicitly states that one of its objectives is to provide for rights of persons regarding unsolicited electronic communications and automated decision making. Neither the ECTA nor the CPA in its respective preambles *explicitly* recognises an aim or object to provide rights in terms of unsolicited electronic communications and/or automated decision making. I believe that this explicit recognition in POPI's preamble is significant because at the very outset POPI recognises the growing problems associated with spamming and seeks to provide adequate protection to data subjects whereas previously spamming was seen as more of a 'by-the-way' problem and it was addressed in a 'by-the-way' fashion.

[109] EU Data Protection Directive (Note 107 above)

It is clear that POPI has been formulated, inter alia, to give effect to the constitutionally entrenched right to privacy[110] and it recognises such an aim in its preamble. POPI's preamble states that "…the need for economic and social progress, *within the framework of the information society* [my own emphasis] requires the removal of *unnecessary impediments* [own emphasis] to the free flow of information, including personal information. It is commendable that the legislator has recognised that we live in a technological age and that it is essential to bring legislation in line with this age of technology.

It is my submission that spam can be seen as one of the unnecessary impediments to the free flow of information (which POPI seeks to remove), which could in the long term hamper economic progress. A report endorsed by the Organisation for Economic Co-operation and Development found that the effects of spam are felt much more strongly in developing countries by internet service providers, businesses and email users than in developed countries.[111] High volumes of spam are a severe drain on the limited availability of bandwidth in developing countries. Most small and medium-sized businesses of the South African economy are unable to make provision for the ongoing costs associated with controlling and combating spam.

Notably POPI seeks to regulate the processing of personal information in harmony with international standards. This paper will explore legislation of the Canadian jurisdiction which has become prominent in the area of protection of personal information regulation, and compare this position to the provisions relating to spam in POPI.

4.4 Application of POPI

POPI sets out various conditions for the processing of personal information to be complied with. As a result of POPI personal information can only be obtained legally under strict conditions for a lawful purpose. POPI applies to public and private bodies which are referred to as "responsible parties"[112] where the processing of personal information is entered into a record by or for a responsible party by making use of automated or non-automated means; provided that when the

[110] Section 14 of the Constitution
[111] See generally S Ramasubramanian 'Spam Issues in Developing Countries' *Organisation for Economic Co-operation and Development* (2005) available at *http://www.oecd.org/internet/ieconomy/34935342.pdf* accessed on 13 May 2014
[112] Section 3(1) read with section 1 of POPI

recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof.[113] This provision easily accommodates acts of employees of direct marketing companies.

4.4.1 Important definitions used in POPI

To fully understand the scope of application of POPI, one needs to refer to some key definitions:[114]

- "Data subject" refers to the person to whom personal information relates. In the context of spamming the recipient of the spam would be regarded as the "data subject" whereas the spammer would be regarded as the "responsible party".

- "Direct marketing" means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –
  promoting or offering to supply, in the ordinary course of business any goods or services to the data subject; or
  requesting the data subject to make a donation of any kind for any reason.

The definition of "direct marketing" is identical to the definition of the same term found in the CPA with the exception that POPI refers to a data subject.[115] The definition concerns commercial communications; however the inclusion of "or to request a donation of any kind" extends protection to situations which were not covered by the ECTA. A recipient of a non-commercial communication such as a religious and political message, without the request of a donation of any kind will not enjoy protection of POPI in terms of the rights afforded to data subjects regarding direct marketing. However, it is my submission that much room is left for affording protection in this instance by the use of "*or* to request a donation of any kind". For example, protection could possibly extend to a situation where one receives an unsolicited email

[113] Section 3(1)(*a*) of POPI
[114] Section 1 of POPI
[115] See Chapter 2 at paragraph 2.2.1 'The Implications of the CPA and its Regulations on Direct Marketing'

communication with a religious message requesting one to donate a number of hours of service to a religious organisation over the weekends.

- "Electronic Communication" means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

This simplistic definition of "electronic communication" differs from the definitions of the same term in the CPA as well as the ECTA. It has been noted that the CPA provides protection in terms of telephonic direct marketing. On the other hand, the ECTA's definition of electronic communication includes voice where it is used in an automated transaction only. The position of telephonic direct marketing under POPI is not clear because of the requirement that the communication must be stored until collected. This would mean that if telephonic direct marketing is covered by POPI, protection will fall away where the telephonic call was merely relayed to the consumer and not stored in the network or in the consumer's terminal equipment as required by POPI. POPI's definition of "electronic communication" has been criticised as being too restrictive compared to the wider definitions found in the CPA or ECTA. [116]

- "Personal Information"

POPI encompasses the wide definition of "personal information" found in the ECTA except POPI refers to "a person" which means a natural or juristic person, whereas section 45 of the ECTA refers to a "consumer". A "consumer" in terms of the ECTA refers to a natural person only. This is significant because protection in terms of POPI extends to juristic persons where it is applicable. The CPA only refers to a specific type of juristic person considering its annual turnover and not juristic persons in general. It has been recently confirmed by the Constitutional Court that businesses do indeed possess a right to privacy, although it may be a more attenuated right to privacy as compared to natural persons, more so if the business is public.[117]

[116] This will be discussed further below at paragraph 4.7 under "Critique and Commentary of Chapter 8 of POPI"
[117] *Gaertner and Others v Minister of Finance* 2014 (1) BCLR 38 (CC) para 36

- "Processing"

The term "processing" is defined as "any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including the collection, receipt, recording, organisation, collation, storage…erasure or destruction of information." Notwithstanding the exclusions from the applicability of the Act for the processing of personal information, it is clear that, read with the definition of "personal information", the widely defined term "processing" would not present a difficult task in extending POPI's protection to most instances of handling, usage or even destruction of one's personal information.

4.5 Noteworthy exclusions in POPI

The exclusions in terms of POPI include the processing of personal information in the course of a purely personal or household activity, by or on behalf a public body which involves national security or public safety, by the Cabinet and its committees or the Executive Council of a province or relating to the judicial functions of a court referred to in section 166 of the Constitution.[118]

There is a further exclusion for the processing of personal of information where it is solely for the purpose of journalistic, literary or artistic expression to the extent that such exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression.[119] This exclusion provides a test which will be employed by courts where a dispute of this nature arises. In its context this provision highlights the constitutional implications of spam. In a legal dispute the recipient of a spam message would assert the constitutional right to privacy and possibly the right to privacy by virtue of being a consumer in terms of the CPA whereas the spammer could possibly rely on a right to freedom of expression.

Jones and Schoeman contend that spam can be regarded as a subspecies of advertising.[120] They further contend that spam constitutes commercial expression therefore enjoying protection in

[118] Section 6 of POPI
[119] Section 7 of POPI
[120] M Jones; H Schoeman '*The South African Constitution and Electronic Commerce' ISSA Information Security South Africa 3rd Annual Conference,* Sandton (2004) (Unpublished) available at

terms of one's right to freedom of expression as contained in section 16 of the Constitution. However, Jones and Schoeman pose the question of how far the protection can extend; whether protection can extend to a situation whereby spammers have the right to express themselves on private property without the consent of the owner. They submit that when the two rights (the right to privacy and freedom of expression) are pitted against each other, precedence suggests that the right to privacy would be accorded the higher importance because courts have generally accorded more importance to the right to privacy than the right to commercial expression as a form of freedom of expression[121]. Commercial expression is clearly not excluded in terms of POPI's applicability and will not fall under the exclusion relating to processing of personal information for the sole purpose of literary or artistic expression. POPI makes specific provision for messages of a commercial nature.

POPI is a new piece of legislation that has not yet had the opportunity of judicial interpretation. For these reasons concepts such as "literary or artistic expression" and "purely personal or household activity" as well as the provisions of POPI in general will be built up over time through case law, academic research, agreements and policy statements.

Two further exemptions relating to the powers of the Information Regulator and in respect of certain functions are created in chapter four of POPI. Firstly, the Information Regulator may exempt a responsible party from the application of POPI if satisfied that the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing, or the processing involves a clear benefit to the data subject or a third party that outweighs to a substantial degree any privacy interference of the

---

http://eprints.mdx.ac.uk/12693/1/The%20SA%20Constitution%20and%20Electronic%20Commerce.pdf accessed on 13 May 2014, at page 6. On this point it is important to note that the Advertising Standards Authority of South Africa (commonly known as the ASA) provides a Code of Advertising Practice which members are required to adhere to. The Code makes provision for direct marketing principles encompassing the privacy principles found in POPI. For more information on this see Appendix C of the Code of Advertising Practice available at http://www.asasa.org.za/codes/advertising-code-of-practice/appendix-c-direct-marketing-advertising%E2%80%93dmasa accessed on 19 October 2014.

[121] *North Central Local Council and South Central Local Council v Roundabout Outdoor (Pty) Ltd and Others* 2002 (2) SA 625 (D) at 635 D – E. This argument is given support by a statement of the Supreme Court of the United States in *Rowan v United States Post Office Department* 397 U.S 728 (1970) 735-738 in which the court found that a vendor does not have a constitutional right to send unwanted material into someone's home, and a mailer's right to communicate must stop at the mailbox of an unreceptive addressee.

data subject or a third party.[122] It is clear that any decision relating to the granting of an exemption by the Information Regulator will be preceded with a test of weighing up various interests in the matter. In this regard the legislator is commended for providing an unambiguous method for the Information Regulator to employ when it exercises its discretion in matters relating to the granting of exemptions.

What is important to note is that although the Information Regulator may grant such an exemption, it may also impose conditions on such exemption.[123] The way in which the exemptions (encompassing a strict test to be satisfied and allowing the Regulator to impose conditions on an exemption) are formulated ensures that possible abuse by the grantee of an exemption is constricted.

The processing of personal information for the purpose of discharging a "relevant function" is exempt from certain provisions of POPI to the extent that application of those provisions will prejudice the proper discharge of that function.[124] "Relevant functions" relates to those of public bodies or those conferred in terms of law which is performed for the purpose of protecting members of the public against, inter alia, dishonesty or seriously improper conduct by persons authorised to carry on a profession or other activity. An obvious example would be the processing of personal information by the Public Protector.[125] If the Public Protector, in every instance, were to be held accountable to meeting the conditions for the processing of personal information found in POPI, then it would not be able to discharge its duties in a complete and proper manner.

The ECTA and CPA must be consistent with POPI. If any provision of these Acts or any other legislation which regulates the processing of personal information is materially inconsistent with POPI, then POPI will prevail. However, if other legislation provides for more extensive conditions for the lawful processing of personal information then those conditions prevail.[126]

[122] Section 37(1) of POPI
[123] Section 37(3) of POPI
[124] Section 38 of POPI
[125] The Public Protector is established in terms of section 181 of the Constitution.
[126] Section 3(2) of POPI

What will be considered "materially inconsistent with POPI" is open to interpretation by the courts. It is clear that the interests of the data subject hold priority in this respect.

4.6 Transforming the Regulatory Framework of Direct Marketing and Spam; Employing the Opt-in Regime

The conditions for the lawful processing of personal information by or for a responsible party for the purpose of direct marketing by any means are reflected in Chapter three, read with section 69 of POPI insofar as it relates to direct marketing by means of unsolicited electronic communications.[127] Chapter 8 of POPI sets out the rights of data subjects regarding direct marketing by means of unsolicited electronic communications, directories and automated decision making.[128] POPI will repeal and replace amongst others, section 45 of the ECTA.

Section 69 of POPI refers to "electronic communications" as *including* facsimile machines, SMS's, automatic calling machines and emails. The use of "including" infers that application of the section is not limited to the given examples and protection will extend to situations where spam is received through other electronic means.

The major change that POPI brings to the laws relating to spam is the employment of the opt-in system. POPI's opt-in system prohibits the processing of personal information for direct marketing purposes unless the data subject has given prior consent to the processing, or is subject to section 69(3), a customer of the responsible party.[129] Immediately one can infer that spamming is no longer allowed until the recipient requests to opt-out; spamming is now an unlawful act. This will be discussed further, below at "Critique and Commentary".

There is no longer a burden on the recipient of the spam to stop future communications. In contrast, the recipient is to consent to direct marketing communications. The employment of the opt-in system has been considered an improvement on section 45 of the ECTA.[130] It is the opinion of many academics in the field, that preferring the opt-in regime over the opt-out regime

[127] Section 4(6) of POPI
[128] For a full understanding of the provisions discussed under this section, reference must be made to the key definitions which were discussed above at paragraph 4.4.1 "Important Definitions of POPI".
[129] Section 69(1) of POPI
[130] Hamann & Papadopoulos (Note 71 above) p 57 para 3.3.2

is a step in the right direction when looking towards minimizing spam and overall removing the abuses that attach to the act of spamming, namely the recipient bearing the cost, irritation, time loss and possible infringement of privacy.[131]

The consent of the data subject that is required for the lawfulness of the processing of personal information for direct marketing purposes is defined by POPI as any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.[132] Consent for this purpose can only be requested once provided that the data subject has not withheld such consent previously.[133] The "once-off request for consent" is welcomed as it bears in mind the consumer's interests and avoids the constant irritation that the consumer is often subject to when he/she is constantly approached by marketers.

A responsible party may process the personal information of a data subject who is a customer of that responsible party; however a number of qualifications exist.[134] This encompasses an existing relationship between data subject and responsible party. Of the qualifications to meet the responsible party must have obtained the contact details of the data subject in the context of the sale of a product or service for the purpose of direct marketing of the responsible party's own similar products or service. A simplistic example is a scenario where a customer receives a haircut at a salon. He then proceeds to pay for the service at the front desk of the salon. Whilst paying he is asked if he would like to be contacted by the salon for future "giveaways or specials". He agrees and provides his contact details. Collection of the customer's email address in this way ensures that the responsible party or the salon will not fall foul of section 69. However, it is important to note that in terms of POPI the data subject must have been given a reasonable opportunity to object to such use of his electronic details.[135]

---

[131] See generally Sipe M 'The Need for New Federal Anti-Spam Legislation' (2013) Vol. 31:55 *Yale Journal on Regulation* and Tladi (Note 5 above)

[132] Section 1 of POPI

[133] Section 69(2) of POPI; Furthermore consent must be requested in the prescribed manner and form meaning that the responsible party must adhere to the conditions for the processing of information referred to in chapter 3. One must be mindful of the fact that "processing" in terms of POPI includes collection of personal information. In turn "personal information" would include an email address or contact number or any identifying number or symbol.

[134] Section 69(3) of POPI

[135] Section 69(3) of POPI; this reasonable opportunity to object must be free of charge and in a manner free of unnecessary formality. It must also exist at the time when the information was collected and on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such

Section 69(4) of POPI also requires any communication for direct marketing to contain the details of the identity of the sender or the person on whose behalf the communication has been sent, and an address or other contact details to which the recipient may send a request for communications to cease.

4.7 Directories and Automated Decision-making

Section 70 of POPI requires that the data subject who is a subscriber to a printed or electronic directory of subscribers (available to the public or which could be obtained through directory enquiry services) in which his personal information is included must be informed, free of charge and before the information is included, about the purpose of the directory and any further uses to which the directory may possibly be put based on search functions embedded in electronic versions of the directory.[136] In addition, a reasonable opportunity to object to the use of the personal information must be afforded to the data subject. Also, he must be able to request verification, confirmation or withdrawal of such information if he has not initially refused.[137]

In terms of POPI, no one may be subject to a decision that has legal consequences, or which affects them to a substantial degree, if it is taken solely on the basis of automated processing of personal information intended to provide a profile of certain aspects of the subject's personality, personal habits such as performance at work, credit worthiness and reliability.[138] This will not apply if the decision has been taken in connection with the conclusion or execution of a contract and the data subject's request in terms of the contract has been met; appropriate measures[139] have been taken to protect the data subject's legitimate interests; or the decision is governed by a

---

use. This provision can be considered 'user friendly' as it considers every day practicalities and it ensures that a data subject's exercise of choice is not hampered by unfair expense or difficulties.

[136] In terms of section 70(5) of POPI a subscriber is any person who is party to a contract with the provider of publicly available electronic communications services for the supply of such services.

[137] Section 70(2) of POPI; however exceptions exist in sections 70(3)-(4) which concern certain directories which existed prior to the commencement of section 70.

[138] Section 71 of POPI

[139] In terms of section 71(3) of POPI "appropriate measures" must allow for an opportunity for a data subject to make representations about such a decision and require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him so that representations in this respect can be made.

law or code in which appropriate measures are specified for protecting the subject's legitimate interests.[140]

4.8 Critique and commentary of Chapter 8 of POPI

Section 69 is largely modelled on Chapter II of the EU Data Protection Directive.[141] Section 69 of POPI addresses spam in a way that requires some form of prior relationship to exist between the sender and recipient of the spam or some other adequate nexus and is therefore more restrictive on spam activities than section 45 of the ECTA.[142] For this reason, as noted above, POPI's provisions can be regarded as a significant improvement on the ECTA.

A considerable critique of section 69 is the fact that it allows for a responsible party to approach a data subject once, to request consent for the sending of direct marketing material, provided that consent has not previously been withheld. Hamann and Papadopoulos argue that by allowing the responsible party to do so, in essence POPI reverts to an opt-out regime and causes the prohibition in section 69(1) to be reduced to a "second level protection mechanism", meaning that section 69(1) only becomes relevant after the initial approach has been made.[143] Further criticisms of section 69(2) are that it is open to abuse and is contrary to the CPA Regulations which provides for a pre-emptive block.

POPI's definition of "electronic communication" has also been criticised as being too restrictive compared to the wider definitions found in the CPA or ECTA. Hamann and Papadopoulos point out that POPI extends protection to electronic communications for direct marketing in the form of text, voice, sound or image that is sent over an electronic communications network. However, direct marketing online also includes collecting data through software and cookies which are data files. This type of processing is not protected under the automated decision making provisions of POPI. For this reason the authors suggest that the definitions of "electronic communication" in the CPA and ECTA, which would be sufficiently wide to include actions

[140] Section 71(2) of POPI
[141] See generally EU Data Protection Directive (Note 107 above) Chapter II – General Rules on the Lawfulness of the Processing of Personal Data
[142] *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association* (Note 75 above) para 80
[143] Hamann & Papadopoulos (Note 71 above) 59

such as data collection via software and the communication of data files, should be employed instead.[144]

The problems attached to the use of false or misleading email headers by spammers has been discussed previously.[145] POPI, like the ECTA and the CPA does not address issues associated with the disguising of email headers.

Section 69(4) of POPI provides that the direct marketing communication must contain, inter alia, details of the identity of the sender and an address to which the recipient may send a request to stop further communications. However, similar to the ECTA, POPI does not provide specifications as to how or where the details should be displayed.

Another concern, which has been discussed as a criticism of section 45 of the ECTA, is that POPI does not provide for measures in consideration of the fact that most spam originates outside the South African jurisdiction. Consideration needs to be given to the extraterritorial reach of national laws such as POPI. In chapter five it will be shown that Canadian laws have not shied away from implementing an extraterritorial reach of its spam laws.

4.9 The Eight Conditions for the Lawful Processing of Personal Information

The conditions for the lawful processing of personal information for the purpose of direct marketing are reflected in Chapter 3. The provisions in terms of the conditions are extensive and this paper does not serve to provide these provisions verbatim; the following discussion will as far as possible be limited to the issues relating to spamming.

4.9.1 Condition 1: Accountability[146]

In essence, to meet this condition the responsible party must ensure compliance with all the conditions contained in POPI and the measures that give effect to those conditions.

---

[144] Ibid 59
[145] See chapter 2 at paragraph 2.1.2 'Critique and Commentary of section 45 of the ECTA'
[146] Section 8 of POPI

4.9.2 Condition 2: Processing limitation[147]

Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.[148] Section 11 of POPI provides certain "defences" for the processing of personal information. For example, the responsible party may rely on the defence that the processing was necessary for pursuing its own legitimate interests or a legitimate interest of the data subject.[149]

With regards to the consent that must be obtained from the data subject for the purposes of commercial communications referred to in section 69, the burden of proof of such consent is born by the responsible party.[150] The data subject is also entitled to withdraw his consent at any time.[151]

In terms of direct marketing which is not covered by section 69, the data subject may object at any time to the processing of personal information.[152] If he has objected to such then the responsible party may no longer process the personal information.[153] It is submitted that these sections relate to direct marketing through means other than electronic communication. It is not revolutionary to provide a consumer with a right to object to the processing of his personal information once he has already been approached by a direct marketer. It would however be seen as a more sophisticated right of a consumer where it is required that the direct marketer does not approach the consumer in the first place.

Ordinarily personal information must be collected from the data subject; however an exception exists where the information is made public by the data subject.[154] Consider the situation where one provides his cellular number on his Facebook™ page which is made public. [155] A direct marketer would be able to collect such information and although he will not be able to add the

[147] Section 9-12 of POPI
[148] Section 9(a)-(b) of POPI
[149] Section 11(1) of POPI
[150] Section 11(2)(a) of POPI
[151] This is subject to section 11 of POPI.
[152] Section 11(3)(b) of POPI
[153] Section 11(4) of POPI
[154] Section 12(2)(*a*) of POPI
[155] Facebook™ is an online social networking service.

number to his list for the purposes of commercial communications, he would be implicitly allowed to initially spam the data subject requesting his consent for future communications. The direct marketer might also unlawfully provide another marketer with the same phone number.[156] This is to be contrasted with section 69 which provides precise situations in which a direct marketer might process the personal information of a data subject in the context of electronic communications.

4.9.3 Condition 3: Purpose specification[157]

Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.[158] A direct marketer would therefore not be able to obtain a data subject's personal information for his own private reasons. The data subject must also be made aware of that purpose.[159] This condition also provides for certain requirements for the retention of the personal information and the restriction of processing of personal information.

4.9.4 Condition 4: Further processing limitation[160]

There are certain limitations for the further processing of personal information. However it has been noted that once a data subject requests that he no longer wishes to receive future communications from a direct marketer, then that request must be honoured.

4.9.5 Condition 5: Information quality[161]

In terms of this condition, the responsible party must take reasonably practicable steps to ensure that the personal information is, inter alia, complete and accurate and he/she/it must have regard to the purpose for which the information was collected when taking said steps.[162]

---

[156] If the marketer engages in such unlawful activity, he will be in contravention of section 19(1)(*b*) of POPI which provides that a responsible party must secure the confidentiality of personal information in its possession or under its control by taking appropriate measures to prevent unlawful access to or processing of personal information. This will be further discussed at paragraph 4.8.7 under 'Condition 7: Security safeguards; considering the issues relating to enforcement of POPI'

[157] Section 13-14 of POPI

[158] Section 13(1) of POPI

[159] Section 13(2) of POPI

[160] Section 15 of POPI

[161] Section 16 of POPI

[162] Section 16(1)-(2) of POPI

4.9.6 Condition 6: Openness[163]

If personal information is collected, the responsible party is under a duty to take reasonably practicable steps to ensure that the data subject is made aware of, inter alia, the right to lodge a complaint to the Information Regulator.[164] This is significant because an ordinary consumer may not be fully aware of the laws relating to personal information protection and any recourse that he may have in terms of any breach of said laws. This duty on the responsible party is therefore welcomed.

4.9.7 Condition 7: Security safeguards[165]*; considering the issues relating to enforcement of POPI*

There is often a concern relating to the enforcement of protection of personal information legislation, especially in terms of possible threats to privacy which have been detected via the internet. The accepted opinion is that it is difficult to track and hold a person responsible for actions committed over the internet because the internet is a vast series of networks and a limitless platform of communications. Although this may be somewhat true, it is probably worth stating that the barriers created by the internet between an offender and prosecutor may be brought down through legislation and improvement on relations between countries.

Section 19(1)(*b*) of POPI provides that a responsible party must secure the integrity and confidentiality of personal information by taking appropriate, reasonable, technical and organisational measures to prevent unlawful access to or processing of personal information. Furthermore where there are reasonable grounds to believe that the information of a data subject has been accessed or acquired by an unauthorised person, the responsible party must notify the Information Regulator and the data subject of such knowledge.[166] Such compromises would include hacking incidents, stolen electronic devices containing personal information, paper records discarded without being disseminated, persons inappropriately accessing information for personal reasons or with ill intentions. When organisations notify the Information Regulator or

[163] Section 17-18 of POPI
[164] Section 18(1)(*h*)(v) of POPI
[165] Section 19-22 of POPI
[166] Section 22(1) of POPI

data subjects of such compromises, as required by POPI, it is likely that an investigation will be initiated.

Violations of the POPI may therefore be discovered through various means. Firstly it may be discovered through the responsible party's obligation in terms of POPI to disclose compromises of personal information and secondly, the most likely source would be the individual data subjects themselves, via an investigation following the lodging of a complaint to the Information Regulator. Another means by which non-compliance might be discovered is if the Information Regulator spontaneously initiated a review or investigation of an organization's compliance as it is empowered to do in terms of POPI; the Information Regulator will likely identify high-risk or high-profile organisations and initiate reviews of their practices to ensure compliance. This is an effective enforcement mechanism but its effectiveness is dependent on how often the Information Regulator will conduct such reviews and which organisations is likely to be reviewed.

Proper enforcement of POPI is also dependent on whether the public is made aware that they are able to exercise and enforce their rights as data subjects in terms of the Act. The public must be made aware that complaints may be formally lodged with the Information Regulator.

Enforcement is further influenced by penalties held in place for non-compliance with POPI:-[167]

a) The Regulator is empowered to levy administrative fines on organisations of up to ten million rand.

b) The Regulator may choose to pursue criminal prosecution, which could result in fines of up to ten million rand, as per above, and/or prison terms of up to twelve months. In the event that a natural or juristic person wilfully obstructs an investigation, prison terms can be up to ten years.

c) A further enforcement power of the Information Regulator which is potentially the most threatening to organisations concerns the issuing of an "enforcement notice". The notice will

[167] Chapter 11 of POPI

require the organisation to stop processing personal information. The scope of the order can vary from one individual's information to the processing of all personal information. It can be restricted to a division or cover an entire business. Such an order has the potential for immense disruption and possibly forced closure of a business.

d) The fourth power of the Information Regulator is to initiate a civil action on behalf of an individual or group of individuals. While many class-action lawsuits have been initiated in the USA in reaction to data breaches, they have not succeeded due to the inability of the plaintiffs to prove financial harm. South African law provides for damages for pecuniary loss and damages for non-pecuniary loss, opening the door to claims for Pain and Suffering. Although the right to privacy enjoys constitutional protection, it is worthy to note that the Supreme Court of Appeal has recently confirmed that class actions are not limited to cases where a constitutional right is invoked; a cause of action may be made without invoking such a right.[168]

4.9.8 Condition 8: Data subject participation[169]

In terms of section 24(1) of POPI a data subject may request a responsible party to correct or delete information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully or destroy or delete a record that the responsible party is no longer allowed to retain. Notwithstanding the exclusions in terms of POPI, the data subject's right to require the responsible party to delete information which has been obtained unlawfully is a logical response to such disputes and strengthens the position of said subject in terms of POPI.

An additional noteworthy point is that in terms of POPI, the Information Regulator must have regard to certain matters in the performance of its functions and exercise of its powers.[170] Of these considerations is "any developing general international guidelines relevant to the better protection of individual privacy".[171] This essentially gives authority to the proposition that if more extensive privacy protection exists, then that should prevail. It will be shown that the

[168] *Children's Resource Centre Trust v Pioneer Food* 2013 (2) SA 213 (SCA) par 21
[169] Section 23-25 of POPI
[170] Section 44 of POPI
[171] Section 44(1)(*d*) of POPI

current international trend is to lend more extensive privacy protection to data subjects and the employment of the opt-in regime has been recently favoured as the starting point in providing more widespread protection.

4.10 Concluding Remarks

Overall POPI seeks to achieve an adequate balance between providing protection to a person's right to privacy and ensuring that such protection accommodates the proper functioning of various institutions and professionals of which, the proper functioning of those institutions and professionals are also necessary for the best interests of the same persons requiring privacy protection. For example, the South African government is accountable to the general public and journalism has created an informal means of communication for the public for such government accountability. POPI creates an exclusion from the conditions relating to processing of personal information where it is solely for the purpose of journalistic expression.

More specifically to the issues of spamming, POPI's employment of the opt-in mechanism is a response to a goal to put an end to 'mindless spamming', that is, the sending of bulk mail to everyone in the optimistic expectation that someone might be interested. The employment of this mechanism is a definite improvement on the current provisions relating to direct marketing in the ECTA. The ECTA was undoubtedly lacking in many respects and did not address consumer protection in relation to spamming adequately.

Although similar to the approach of the ECTA, the CPA and its regulations are distinguishable on many points. As a result, these two Acts have produced a fragmented approach to spam and direct marketing. Hamann and Papadopoulos submit that spam and direct marketing online has not been given 'holistic attention'.[172] The terminology employed in the ECTA, CPA and POPI as well as the fields of applications for each of the Acts lack a common understanding. A lack of common understanding amongst the Acts creates legal uncertainty, confusion and ignorance of legal rights and obligations resulting in inadequate consumer protection. These Acts fail to live up to its aims or objectives in the context of spam.

[172] Hamann & Papadopoulos (Note 71 above) 61

An approach to data protection with similar characteristics of a lack of common understanding amongst legislation and regulations has been observed in European consumer protection law.[173] Papadopoulos suggests that the legislature obtain a comprehensive, holistic and comparative overview of current trends in legislative interventions or at least a proper effort should be made to harmonise POPI and the CPA.[174]

As with the ECTA, POPI does not address legal issues arising out of spam in general; its application is limited to commercial communications. For this reason, no protection is afforded to a data subject who receives spam containing newsletters, religious messages, political messages, newsletters, urban legends, chain letters, virus warnings and virus hoaxes and other carefully formulated communications with fraudulent or deceptive content.[175] These types of non-commercial communications are equally, if not more common than spam with commercial content.

The Information Regulator will play an important role in determining the success of POPI's aims to give effect to the constitutional right to privacy by ensuring respect for and to promote, enforce and fulfil the rights protected in POPI. The unsympathetic penalties provided for in POPI will act as a deterrent to those contemplating committing acts inconsistent with POPI.

[173] See generally C Cuijpers; B Koops "*How fragmentation in European law undermines consumer protection: the case of location-based services"* (2008) 33 E.L. Rev. Thomson Reuters (Legal) Limited and Contributors
[174] Papadopoulos (Note 37 above) 240
[175]Hamann & Papadopoulos (Note 71 above) 61

CHAPTER 5

CANADIAN INSPIRATION; WHY SPAMMERS SHOULD REMOVE CANADIANS OFF THEIR MAILING LISTS

This chapter seeks to critically analyse and compare the Canadian approach to spamming to the newly enacted POPI. Since POPI explicitly provides that it seeks to harmonise with international standards, the processing of personal information by public and private bodies, it bears merit to explore this international standard.[176]

5.1 Background Information

Canada has the highest per capita immigration rate in the world, and is often depicted as being incredibly progressive, diverse and multicultural. Multiculturalism has a direct effect on Canadian law: it includes an express policy of bilingualism.[177]

In terms of the country's legal system, like South Africa, Canada uses the adversarial legal system. In terms of legislation, all Acts of Parliament are enacted, printed and published in both official languages (English and French). The primary sources of law are statutes passed by the Parliament of Canada. Bills of the federal government are initially announced in the Canadian Gazette. The bill is subject to three 'readings'. Should a federal bill receive Royal Assent, it is subsequently published in the Annual Statutes of Canada.[178]

[176] The Preamble of POPI
[177] A Mooney-Cotter *Culture clash: an international legal perspective on ethnic discrimination* Ashgate Publishing Ltd (2011) 176
[178] 'Guide to the Canadian House of Commons' Official website of Parliament of Canada at http://www.parl.gc.ca/About/Parliament/GuideToHoC/making-e.htm accessed on 29 July 2014

5.2 Introducing Canada's Approach to Spam

On 15 December 2010 Canada's new anti-spam law was enacted.[179] Although there is no official short title for the Act, it is commonly known as 'Canada's anti-spam law' (hereinafter referred to as CASL). CASL came into force on 1 July 2014. Similarly to POPI, CASL is a new piece of legislation which is open to a number of interpretations and has not yet been subject to judicial interpretation.

The purpose of CASL is to deter spamming and other deceptive and harmful online threats. CASL regulates a range of activities including spam emails or messages via other electronic medium, spyware, phishing, fraudulent or deceptive practices.

It will come to light that CASL can probably be described as the most stringent anti-spam law in the world, which would likely have a great impact on reducing spam. It would therefore be interesting to note how POPI compares to CASL in these respects.

5.3 Preliminary Observations of CASL

At the outset it is observed that, in Canada, spam is dealt with by a specific statute which was created for this purpose and not by a limited amount of provisions which is secondary to the aims of a statute that it is contained in. Granted, when a legal issue is addressed in a chapter of a statute, which is connected to the overall theme of the statute, the effectiveness of those provisions contained in the chapter is not necessarily hampered. However, when a legal issue is given holistic attention, better understandings of the manner in which the legislature chooses to address that issue, ensues. To put it differently, not every foot should be forced into Cinderella's glass slipper; a glass slipper should be tailored to meet the needs of the individual (or the legal issue, in this case).

[179] An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act (S.C. 2010, c. 23) There is no official short title for this Act. The full text of the Act can be accessed at http://lois-laws.justice.gc.ca/eng/AnnualStatutes/2010_23/FullText.html retrieved on 1 June 2014.

CASL aims to regulate certain activities of the Canadian economy in a manner that discourages reliance on electronic means of carrying out commercial activities.[180] This stated purpose of CASL immediately puts into focus what CASL seeks to achieve, namely to combat spamming.

Under the Interpretation Act, CASL will be deemed to be remedial legislation and will "be given such fair, large and liberal construction and interpretation as best ensures the attainment of its objects".[181] CASL's preamble including its objectives and the constitutional limitations on how freedom of commercial speech can be impinged upon under the Canadian Charter of Rights and Freedoms of the Canada Act, play essential roles in determining how CASL will be construed.[182]

The driving force of the anti-spam provisions centres on an opt-in regime prohibiting commercial electronic messages to be sent to a person, unless that person has previously consented to receiving the message.[183]

5.4 Application of CASL

CASL provides a broad scope of applicability; CASL will apply to electronic spam communications if the communication is sent or accessed by a computer system in Canada.[184] This means that CASL's application extends to foreign messages and messages stored on foreign servers accessed from Canada. CASL includes a three year grace period allowing organisations to bring their businesses in line with CASL.

5.4.1 Important definitions used in CASL

Some key definitions in CASL include:

[180] Section 3 of CASL
[181] Section 12 of the Interpretation Act R.S.C., 1985, c. I-21
[182] Schedule B to the Canada Act 1982, c. 11 (U.K.)
[183] Section 6(1) of CASL
[184] D Paulson '*Canada Update: A Review of Canada's Recent Holding Regarding the Proposed Securities Act, Canada's Anti-Spam Law that May Soon Take Effect, And the Disciplinary Hearing of Joe Groia*' (2012) 18 (4) Law and Business Review of the Americas 615, 618. Further authority for this point can be found in section 12(1) of the CASL.

- "Commercial activity" means any particular transaction, act or conduct that is of a commercial character, whether or not the person who carries it out does so in the expectation of profit.

This definition does not apply to acts that are carried out for the purpose of law enforcement, public safety and the protection of Canada, the conduct of international affairs or the defence of Canada. Although POPI provides a definition specifically for "direct marketing", it fails to provide any clarity as to what constitutes "commercial activity".

- "Electronic message" means a message sent by any means of telecommunication, including a text, sound, voice or image message.

This definition differs from the definition of "electronic communication" used in POPI insofar as the latter requires storage of the communication either on the network or in the recipient's terminal equipment until it is collected by the recipient.

- "Person"

"Person" is defined similarly in POPI as it refers to either natural or juristic persons. The difference between the two Acts relates to the specific mention of the type of juristic persons to which CASL will apply to. "Person" in CASL will therefore be strictly restricted to the types of persons listed as the definition omits any use of "includes" to render it inclusive as opposed to restrictive.[185]

- "Commercial electronic message" is an electronic message, having regard to the content of the message, the hyperlinks in the message to content on a website or other database, or the contact information contained in the message, it would be reasonable to conclude has as its purpose, or one of its purposes, to encourage participation in a commercial activity.

It is submitted that a form of guidance in determining commerciality of a message is welcomed. POPI provides no guidance as to how one is to determine whether a spam message bears commercial content. Such guidance is important because the anti-spam provisions of POPI will not apply to non-commercial messages; it is therefore essential to make this distinction with precision.

[185]In terms of section 1 of CASL, CASL applies to an individual, partnership, corporation, organisation, association, trustee, administrator, executor, liquidator of a succession, receiver or legal representative.

5.5 Noteworthy exceptions and exclusions in CASL

There are several exceptions to the opt-in rule, such as product recall information or information related to confirming a transaction that was previously entered into.[186] It is submitted that such exceptions are necessary to allow for *bona fide* communications which have the consumer's interests borne in mind.

Typical exclusions from CASL's applicability include messages sent for the purposes of law enforcement or "public safety".[187] Unlike POPI, there is no requirement in terms of CASL that a message relating to public safety be a message by or on behalf of a public body, to be excluded from CASL's applicability. The resultant problem from the way this exclusion is formulated is that it may prove to be a difficult task to distinguish a *bona fide* message regarding public safety from a hoax. For example, I received the following email, which supposedly contained a message concerning public safety:

> "Subject: FW: Public service announcement
>
> Dear Reader,
>
> Please be warned that there are several vehicles travelling in the Durban area at night with their headlights switched off. As a mark of friendliness one would usually "flash bright lights" at the other car to warn the driver that his headlights are not switched on.
>
> If you come across such a scenario, DO NOT "FLASH" YOUR LIGHTS AT THE DRIVER. This antic is seen as an "initiation hurdle" for new members of the "3-6 Boys" gang. The new member would be required to kill the one who flashes their bright lights.
>
> Please pass this message on to all loved ones."

This message raised genuine concern among members of the public. The content of the message was not proved to be true. This email could have been a vehicle for the distribution of malware to the recipient's device. It is therefore wise to exclude from CASL's applicability messages of public safety from public bodies only.

[186] Section 6(6)(a)-(g) of CASL
[187] Section 1(1) of CASL

5.6 CASL's Opt-in Mechanism

In terms of section 6(1) of CASL, it is prohibited to send or *cause or permit to be sent* [own emphasis] to an electronic address a commercial electronic message unless the person to whom the message is sent has consented to receiving it, whether the consent is express or implied. It is further provided that the message must set out prescribed information that identifies the person who sent the message, and the person – if different, on whose behalf it is sent and the message must also set out information enabling the recipient to readily contact the sender or the person on whose behalf the message was sent.[188] The message must also set out an unsubscribe mechanism in accordance with CASL.[189] Furthermore the sender of the message must ensure that the contact information provided in the message is valid for a minimum of sixty days after the message has been sent.[190]

CASL, like POPI employs an "opt-in regime" in response to the need to discourage spam. The benefits of employing the opt-in mechanism have been discussed throughout this research paper. Regardless of this similarity, CASL differs greatly from POPI.

The wording of section 6(1) of CASL, namely the excerpt "it is prohibited to send or *cause or permit to be sent*" makes provision for the unlawfulness of facilitation of spamming. Section 6(1) is to be read in conjunction with section 9 of CASL which provides that it is prohibited to aid, induce, procure, or cause to be procured the doing of any act contrary to section 6.

Prohibiting the facilitation of spamming is a novel concept to spamming legislation and regulation and may prove to be the key to adding to the prospect of legislative success in combating spamming. An example of facilitation of spamming exists where an employee of a direct marketing company approaches her employer with a mailing list for the purposes of sending commercial communications, to which the employer approves regardless of the fact that the employer is aware that certain holders of email addresses on the mailing list did not provide the company with express or implied consent to receive any commercial communications. The employer's act of approving the list will be regarded as an unlawful act in terms of section 6(1) and section 9 of CASL as it seeks to facilitate spamming.

[188] Section 6(2)(*a*)-(*b*) of CASL
[189] Section 6(2)(*c*) of CASL
[190] Section 6(3) of CASL

Section 6(1) of CASL would then create a concern that internet service providers may be in contravention of said section since internet service providers "facilitate" the sending of emails. CASL has addressed this concern in section 6(7) which provides that section 6 does not apply to a telecommunications service provider merely because the service provider provides telecommunication services that enables the transmission of the message (being the electronic commercial communication). More so, there is no sufficient nexus between the internet service provider and the spammer to hold the provider liable for the spammer's unlawful acts.

A further novel concept of CASL is the requirement that the sender of the communication is to ensure that the contact information provided in the message is valid for a minimum of sixty days after it has been sent. This requirement provides the recipient with assurance that should he decide to no longer receive commercial communications from the sender of such messages, his request will be honoured as he is in some way guaranteed of the accuracy of the sender's provided contact details.

5.7 Express or Implied Consent

A person who seeks express consent for the purposes of section 6 of CASL must, when requesting consent, set out clearly and simply the purpose or purposes for which consent is being sought, prescribed information that identifies the person seeking consent and any other prescribed information.[191] If the person seeks the consent of a person whose identity is unknown, then the only information required is the prescribed information that identifies the person seeking consent and compliance with the Electronic Commerce Protection Regulations (hereinafter referred to as the "ECP Regulations") in respect of that consent.[192]

For the purposes of section 6 of CASL, consent is implied where:[193]

a) the sender, or the person who causes or permits the message to be sent has an existing business relationship or an existing non-business relationship with the receiver of the message;

[191] Section 10(1)(*a*)-(*c*) of CASL
[192] Section 10(2)(a)-(b) of CASL, ECP Regulations [Canada Gazette] (Part I, Vol. 145, No. 28 – July 9, 2011] Pursuant to CASL, the Canadian Radio-Television and Telecommunications Commission published its regulation in the Canada Gazette which later became known as the Electronic Commerce Protection Regulations.
[193] Section 9 of CASL

b) the receiver of the message has conspicuously published, or has caused to be conspicuously published, the electronic address to which the message is sent;[194]

c) the receiver of the message has disclosed to the sender or the person who causes or permits the message to be sent, the electronic address to which the message is sent without indicating a wish not to receive unsolicited commercial electronic messages at that address, and the message is relevant to the person's business, role, functions or duties in a business or official capacity; or

d) the message is sent in circumstances set out in the ECP Regulations.

CASL provides a detailed definition of what constitutes an existing business relationship and an existing non-business relationship. Similarly POPI allows a responsible party to send a commercial communication to a data subject where there is an existing relationship between both parties but provides for a number of qualifications before the responsible party may invoke this section.[195]

Examples of an existing business relationship in terms of CASL include a relationship between the receiver and sender of the message arising from the purchase of a product, goods or services and a written contract between the receiver and sender of the message. Examples of an existing non-business relationship include a relationship between the sender and receiver of the message arising from the receiver having membership in the sender, namely a voluntary organisation, club or association. The ECP Regulations clearly define the terms "club," "association" or "voluntary organisation" as a non-profit organisation operated exclusively for any purpose other than profit.[196] The clearly defined terms in the ECP Regulations establish limits and avoid ambiguity when interpreting the provisions relating to implied consent in CASL. This clarity is necessary to prevent spammers from exploiting said provisions in order to send communications without the recipient's consent and to come to the assistance of legitimate businesses which are willing to comply with the law.

[194] As per section 10(9)(*b*) of CASL to constitute implied consent in this situation, the publication of the electronic address must not be accompanied by a statement that the person does not wish to receive unsolicited commercial electronic messages at that address and the message must be relevant to the person's business, role, functions or duties in a business or official capacity.
[195] Section 69(2) of POPI
[196] ECP Regulations (Note 192 above) section 7

5.8 The Unsubscribe Mechanism

In addition to employment of the opt-in mechanism CASL requires the communication to include an unsubscribe mechanism which must enable the receiver to communicate to the sender that he no longer wishes to receive such communications.[197] In doing so the receiver must bear no costs and must be able to use the same electronic means that was used to send the message to unsubscribe or if not practicable, other means may be used.[198] This can be contrasted with the unsubscribe mechanism provided for in section 45 of the ECTA.[199] As was discussed in Chapter two, the ECTA mentions no guidance as to how the opt-out mechanism should be provided for or through what means the consumer may unsubscribe from the communications, which leaves room for abuse. Unlike the ECTA, the CASL specifically requires that the unsubscribe link must be valid for a minimum of sixty days after the message has been sent.[200]

If the recipient indicates that he no longer wishes to receive such communications from the sender then effect must be given to that indication no later than ten business days after the indication has been sent and without requiring any further action on the recipient.[201] Again the ECTA is lacking in these many respects; the ECTA does not provide a specific time period for which the recipient's request must be honoured – if the spammer chooses to honour the request at all.

5.9 Noteworthy Enforcement Measures

CASL provides for administrative monetary penalties and damages in terms of a private right of action. Only one action may be made, either the administrative or the private right of action.[202] In the case of a company or any person not to be considered an individual, the administrative monetary penalties are capped at ten million Canadian dollars.[203] In terms of compensatory damages, one may receive a maximum of two-hundred Canadian dollars for each violation of

[197] Section 11(1)(*a*) of CASL
[198] Section 11(1)(*a*)(i)-(ii) of CASL
[199] This mechanism was discussed under Chapter 2 "The Current South African Position".
[200] Section 11(2) of CASL
[201] Section 11(3) of CASL
[202] Section 48(1)-(3) of CASL
[203] Section 20 (4) of CASL

sending an electronic message without consent, not to exceed one million Canadian dollars for each day of occurrence.[204] Paulson points out that the measure for damages may not seem overwhelming in the case of a single plaintiff but a class action may cause much more serious consequences for defendant companies.[205] The maximum penalties are therefore significant and the legislator has recognised this significance and in response, created an internal measure to ensure that the penalties are not disproportionate to the spammer's act or ability to pay the damages. A court will be required to exercise discretion when determining the amount payable for a contravention of CASL and will be required to consider a number of factors including the purpose of the order and the person's ability to pay the amount.[206]

5.10 Critique and Commentary of CASL

The noteworthy change that CASL has brought to Canadian legislation is the requirement of express consent. Many consumers are often unaware that their information is used for commercial purposes. For example when an agreement is presented to you, your "consensus" may already be expressed in a pre-checked in box regardless of the fact that you were unaware of the checked box. Businesses will often rely on those tactics as the consumer's valid consent. Express consent is therefore a step in the right direction towards consumer protection.

CASL does present certain exceptions and makes provision for implied consent. Canadian businesses will most likely invoke these exceptions instead of obtaining one's express consent. Reliance on these exceptions could create internal business complications which can be simply avoided by seeking the express consent of the consumer.

Although commendable for its forceful approach against spamming, CASL is not without its ugly side. CASL's approach encompasses what one would call "jurisdictional overreach". Foreign spammers will not be easily intimidated by the penalties imposed by CASL for the simple reason that it is difficult to fathom that the Canadian government will physically track and

[204] Section 51 (1)(b)(i) of CASL
[205] Paulson (Note 184 above) 618
[206] Section 51(3) of CASL

bring to justice a spammer who is outside Canadian borders. Instead the Canadian government would rather impose the law on organisations operating within Canada.

CASL places online marketing in Canada in an uneven playing field. Direct marketers are required to jump through many hoops created by the legislation. In effect CASL will require direct marketing companies to completely re-evaluate their marketing communications strategy. In this sense CASL may become a marketer's nightmare.

Perhaps a forceful approach to spamming is required because of the ease in which spammers are able to avoid prosecution and the fact that spamming is often taken lightly and not regarded as a "real crime". The significant penalties in CASL are to likely act as a somewhat successful deterrent to spamming.

Regardless of the prospect of success of CASL, if one were to adopt a legislative route in combating spamming then CASL provides great guidance in the drafting of the provisions that would be required. The provisions with specific application to the commercial communication of the spam message are non-ambiguous. Non-ambiguous legislation leads to clear and coherent judgments which in turn make the status quo plain and understandable.

CHAPTER 6

CONCLUDING REMARKS AND SOME SUGGESTIONS

This research paper begun by seeking to bring the reader's attention to the more serious consequences derived from spam. It must be emphasised that spam should no longer be seen as only an everyday nuisance; spamming should be considered an act which is able to infringe a person's right to privacy, create a number of dangers to the recipient and substantial costs to the recipient, internet service provider and the internet infrastructure as a whole.

Prior to the commencement of POPI, a litigant has recourse to section 45 of the ECTA and section 11 of the CPA. The ECTA provides inadequate and limited protection to the recipient of spam. The ECTA fails to live up to its objective of ensuring that electronic transactions conform to the highest international standards. It seems as if the ECTA was drafted during a time when spam did not represent a current challenge. Unlike the ECTA, the CPA does not limit protection to instances of direct marketing via electronic communications. The CPA also provides for a pre-emptive block against communications primarily for the purpose of direct marketing; however this provision has not seen successful enforcement. The approach of ECTA and the CPA seem disjointed and require harmonisation bearing in mind the consumer's interests.

POPI represents a significant step towards the right direction in creating much improved consumer protection with regards to spam and has produced the secondary effect of creating awareness of the issues relating to spam.

Geissler points out that legislative effort to reduce spam within South Africa could bring about a considerable difference in the volume of spam globally. She further submits that we often look to foreign jurisdictions to seek guidance on legal issues; similarly those jurisdictions will also look to South African law for such guidance.[207] The introduction of anti-spam legislative protection allows South Africa to influence the international arena to encourage other countries to follow suit thereby working towards a global solution as spam is considered a global problem.

[207] Geissler (Note 6 above) 386

Spam can be defeated through a combination of measures and not only through the use of legislative measures.

6.1 Industry Self-Regulated Regime

The Ketler case provides a wise sentiment that the light of solution should not be only shone on statutes; rather we should also implement an industry self-regulated regime. The problem with self-regulatory measures stems from the fact that compliance with an association's code of conduct can only be asked of a member of such an association. However, it is true that industry players are somewhat pressured into becoming members of such associations by the consumer's preference of members over non-members as consumers become more aware that a member of an association will be held to a higher standard of practice which in turn benefits the consumer. This shows that a further worthy approach to combating spam largely lies in the need for consumer awareness.

6.2 Anti-Spam Awareness Campaigns

In 2003 Australia introduced anti-spam legislation and simultaneously embarked upon a public awareness campaign. At the time, Australia was listed as one of the top ten countries of spam origination. By 2005 the country dropped off the list.[208] This shows us that spam can be defeated through effective anti-spam legislation and an elaborate public awareness campaign.

Countries such as Mauritius, Canada, Hong Kong and Australia have all recognised the importance of consumer awareness in the fight against spam. Awareness campaigns inform end-users about what they are able to do to limit the amount of spam that they receive. Consumers must be made aware of practices to reduce spam including spam reporting and the use of internet security and filtering tools.

[208] D M McRae *The Canadian Yearbook of International Law* Vol 47 Toronto: University of British Columbia Press (2009) 475

6.3 Employ A Task Force On Spam

A task force on spam should be employed to identify user practices and behaviours relating to spam. Such an approach has been implemented by the Canadian government and has proved to be successful in many respects. The Canadian task force which is named the Working Group on Public Education and Awareness was formed in 2004. It has placed focus on engaging with stakeholders in the public and private sphere to implement an awareness initiative to combat spam. The task force submits comprehensive reports to the Minister of Industry making recommendations of *inter alia* best practices for internet service providers and end-users.

6.4 The Definition Of Spam

What can be seen as a common theme throughout this research paper is the emphasis placed on the lack of protection afforded to the recipient of a non-commercial communication. There is simply no protection afforded to the recipient when the message bears religious or political content, hoaxes, chain letters and other similar content. This is worrisome as most spam bears non-commercial content. The definition of spam should therefore be extended to non-commercial communications.

6.5 Regular Review Of Anti-Spam Measures

Ebersöhn recommended that the South African government should regularly review section 45 of the ECTA.[209] I similarly submit that POPI as well as related enforcement mechanisms should be regularly reviewed to consider its effectiveness in defeating spam. The reason being is that technology is fast-paced and ever-changing; measures which are considered suitable in the present may not be considered so in five years time. Regular review is therefore warranted.

[209] Ebersöhn (Note 45 above) 142

6.6 The Unsubscribe Mechanism In Conjunction With The Opt-In Mechanism

CASL employs the opt-in regime but also requires a functional unsubscribe mechanism in each communication. CASL has also provided specifications as to how the unsubscribe mechanism is to be provided and how the recipient is to exercise his option to no longer receive future communications.[210] It is submitted that this approach should be adopted by the South African legislator as it removes the ambiguity that attaches to section 45 of the ECTA and provides a more coherent approach notwithstanding the added consumer protection.

The fight against spam requires effective legislative and consumer intervention and simultaneous implementation of industry self-regulated measures. A more creative way of describing what is needed to combat spam is as follows: a single digit on a hand will not make an impact, but if you bring them together it forms a fist and you are able to strike a mighty blow.

[210] These specifications have been discussed in chapter 5 at paragraph 5.7