THE REGULATION OF UNSOLICITED COMMERCIAL COMMUNICATIONS (SPAM): IS THE OPT-OUT MECHANISM EFFECTIVE?[*]

SEBO TLADI[†]
Senior Lecturer, Department of Mercantile Law, University of South Africa

INTRODUCTION

The success of a company depends on the way they advertise their products or services. Traditionally, consumers were individually informed of products and services by companies with which they had a prior relationship, or because they had requested information from new companies. Alternatively, the products and services were marketed via media such as television, radio, newspapers, magazines and catalogues. Expenses for advertisements, like postage or the airing of advertisements, were incurred by the companies themselves.

The advent of e-commerce has brought with it new electronic delivery systems that offer a wider scope of business for marketing companies — with minimum costs. These marketing strategies utilize the Internet, which is a very effective way of disseminating information, enabling marketing companies to advertise products and services to people all over the world via e-mail and other forms of online advertisements. This method of communication is easy, quick and cost effective.[1] With just a click of a mouse one can buy and sell products or services from different jurisdictions within seconds. However, it also brings with it problems — in particular, that of 'spam', i e unsolicited junk mail.

Although spam is now primarily related to the internet, it is not limited to this medium. One can also receive spam on a mobile telephone via short message services (SMS) or through the post. This contribution is, however, limited to spam in an online environment. The nature of spam will be discussed, as will the methods used to send it and the problems caused by it. At the core of this article is the question whether the use of the 'opt-out' mechanism is effective in limiting spam.

[*] This is a revised version of a paper presented at the Workshop on Consumer Protection in Commercial Law held on 25 August 2005 at Nedcor, Rosebank under the title 'The regulation of unsolicited mail (Spam)'.

[†] B Iuris (Vista) LLB LLM (Pret).

[1] Julien Hofman *Cyberlaw: A Guide For South Africans Doing Business Online* (1999) 21, where the author discusses the concept of e-mail.

THE HISTORY AND NATURE OF SPAM.

The name 'spam' was first used in 1926, when Hormel Foods introduced a brand of tinned lunchmeat by that name.[2] There are various opinions as to when spam was first used to refer to junk mail. It was not yet in use when Jon Postel[3] stated that '[i]t would be useful for a host to decline messages from sources it believes are misbehaving or are simply annoying'.[4] It never occurred to him or others then that unsolicited advertisements would be a plague in the near future and no measures were put in place to limit spam. Some suggest that the origins of the use of 'spam' as synonymous with unwanted communications started with a Monty Python skit in which a group of Vikings sang a chorus of 'Spam SPAM SPAM', with increasing volume in an attempt to drown out the conversation.[5] Spam drowns the conversation on the Internet, making it impossible for anyone to go through his or her e-mails without first reading or otherwise dealing with it.

One of the earliest incidences of electronic spam was the e-mail campaign of the infamous 'green card lawyers' Canter and Siegel.[6] The two attorneys wanted to cash in on the green card scheme that the government of the USA had introduced for the immigrants to that country. The duo sent postings to every newsgroup on Usenet,[7] to promote their law firm's immigration services. After this, thousands of Internet users from across the world showed their displeasure by swamping Canter and Siegel's company with angry warnings not to repeat the mailing.[8]

Spam is generally defined as unsolicited e-mail, or electronic junk mail,[9] but the word 'spam' is used differently in the legislation of various jurisdictions. For instance, in the United States and Australia, spam is referred to as unsolicited commercial electronic mail messages (UCE);[10] in New

[2] See *http://www.hormel.com/templates/knowledge/knowledge.asp?catitemid=16&id=132* (last accessed on 11 April 2006). For a brief history of spam see Adam Mossoff 'Spam-Oy, what a nuisance!' (2004) 19 *Berkeley Technology LJ*
625 at 631–2.

[3] Jon Postel helped launch ARPnet in 1969. He is regarded as one of the internet's pioneers. See *http://www.isoc.org/postel/* (last accessed on 7 September 2006).

[4] Jon Postel 'On the junk mail problem' Request for Comment (RFC 706) published for ARPnet in 1975, available at *http://www.rfc-archive.org/getrfc.php?rfc=706* (last accessed on 7 September 2006).

[5] J A Hitchcock *Net Crimes and Misdemeanors: Outmaneuvering the Spammers, Swindlers, and Stalkers Who Are Targeting You Online* (2002) 30; see also *http://www.templetons.com/brad/spamterm.html* (last accessed on 11 April 2006).

[6] See *http://lcs.www.media.mit.edu/people/foner/Essays/Civil-Liberties/Project/green-card-lawyers.html* (last accessed on 17 April 2006).

[7] Usenet is the world's largest online conferencing system.

[8] See website supra note 6.

[9] See *http://www.webopedia.com/TERM/s/spam.html* (last accessed on 1 June 2006).

[10] See s 3(2) of the United States Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (henceforth referred to as the CAN-SPAM Act) and s 6 of the Australian Spam Act 129 of 2003.

Zealand it is called unsolicited electronic messages (UEM);[11] in the EU it is referred to as unsolicited bulk or broadcast e-mail (UBE);[12] and in South Africa it is called unsolicited commercial communications (UCC) by the Electronic Communications and Transactions Act ('the ECT Act').[13]

The word 'unsolicited' implies that there is either no prior relationship between the sender of the spam and the recipient, or, at the very least, that the recipient has not consented to receiving a communication.[14] However, the terms used in the different countries emphasize different characteristics of this kind of communication. For example, 'UBE' refers to the volume of the message and not necessarily the content. A 'bulk' message is often sent to a discussion group or to a set of addresses obtained from companies that specialize in creating e-mail distribution lists. There is no indication of how many messages will constitute bulk. Some propose a rule that twenty to fifty messages in a day should constitute bulk.[15] However, in terms of the ECT Act, a single unsolicited commercial message may be defined as spam.[16] In the case of UCE, on the other hand, the definition is essentially based on the commercial nature of the message content, rather than the sender's actual motivation for sending the message.[17] Therefore, scams, viruses, chain letters, hoaxes, and urban legends[18] are not included in UCE because their

[11] See *http://www.ajpark.co.nz/library/2005/03/war_spam.php* (last accessed on 7 September 2006).

[12] See *http://www.euro.cauce.org/en/manifesto.html* (last accessed on 28 August 2006).

[13] Act 25 of 2002, s 45(1).

[14] See Reinhardt Buys *Cyberlaw@SA II: The Law of the Internet in South Africa* 2 ed (2004) at 160.

[15] See *http://www.cauce.org.au/whatis.htm* (last accessed on 5 September 2006).

[16] See Buys op cit note 14 at 161.

[17] With UCE the senders usually hope that consumers/recipients of such e-mails will spend money with them. Products or services that are commonly advertised through UCE include wellness medicines, such as viagra pills, while businesses advertised include gambling sites, lotto draws and 'make money fast' schemes. See Gerrie Ebersöhn 'The unfair business practices of spamming and spoofing' 2003 *De Rebus* (no 424) 25; Shumani Gerada 'The truth about spam' 2003 *De Rebus* (no 426) 51 and Michelle Lara Geissler *Bulk Unsolicited Electronic Messages (SPAM): A South African Perspective* (unpublished LLD thesis, University of South Africa, 2004) 172–3, available at *http://etd.unisa.ac.za/ETD-db/ETD-desc/describe?urn=etd–03312005–104653* (last accessed on 06 February 2008).

[18] A scam is an attempt to intentionally mislead a person or persons (known as the 'mark'), usually with the goal of financial gain. The Nigerian '419' scams and pyramid schemes are included here. (See *http://en.wikipedia.org/wiki/Scam* (last accessed on 15 September 2006)). A virus is a program written to cause mischief or damage to a computer system (see *http://www.ontrack.com/glossary/* (last accessed on 15 September 2006)). A chain letter is a message that attempts to induce the recipient to make a number of copies of this letter and then to pass them on to two or more new recipients (see *http://en.wikipedia.org/wiki/Chain_letters* (last accessed on 15 September 2006)). A hoax is an attempt to trick an audience into believing that something false is real (see *http://en.wikipedia.org/wiki/Hoax* (last accessed on 15 September 2006)). An urban legend is 'a story that appears mysteriously and spreads spontaneously in various

content is not of a commercial nature and hence they are not considered as spam in terms of s 45 of the ECT Act.[19]

The most common understanding of spam is an e-mail message sent to a large number of people without their consent and which constitutes some form of nuisance.[20]

METHODS USED TO SEND SPAM

There are various methods used to send spam and they include the following:

Spyware

Spyware is computer software that collects information about an individual without their knowledge. It can be installed automatically in several ways, e g by viewing an unsolicited e-mail message containing a virus or worm as an attachment, or as a result of visiting certain websites.[21]

Dictionary Attacks

A dictionary attack is 'a program that bombards a mail server with millions of alphabetically generated email addresses in the hope that some addresses will be guessed correctly.'[22] For example, attempting to send a large number of test messages to e-mail addresses within a domain such as @yahoo.com.[23] This is used to compile a list of deliverable e-mail addresses for future spam

forms and is usually false; contains elements of humor or horror and is popularly believed to be true' (Definition per WordNet Search *http://wordnet.princeton.edu/perl/webwn* (last accessed on 15 September 2006)). An example of an urban legend would be a story I was sent recently, which has apparently been circulating since 1993: In it, 'blood gang members' drive at night without their headlights on, and people are warned against flashing their own headlights at such a car, as they would then become a target and be killed by the gang members as part of their 'initiation'. No supporting evidence for this story has been found by police.

[19] See Buys op cit note 14 at 160. See also Geissler op cit note 17 at 88–111 where the author discusses these types of spam.

[20] At the very least, it is not considered good netiquette to send spam. The term 'netiquette' means 'network etiquette'. Netiquette constitutes an informal code of good manners governing online conduct. It can be as simple as not typing a message in all upper-case letters (This is commonly interpreted as representing SHOUTING). For the core rules of netiquette see *http://albion.com/netiquette* (last accessed on 3 August 2006).

[21] See Brad Slutsky & Sheila Baran 'Spyware and the internet: A cyberspace odyssey' (2005) 10 *Georgia Bar Journal* 22 at 23, where the authors elaborate on the origins of spyware.

[22] See *http://www.sophos.com/security/spam-glossary.html* (last accessed on 6 February 2008).

[23] The target e-mail addresses are generated based on words from a dictionary of possible or likely words, combined with the name of the domain being attacked.

communications. This method is also used as a means of obtaining passwords to gain unauthorized access to computer systems.[24]

Cookies

A cookie is a small piece of information that a web server can store temporarily within one's browser.[25] These files contain information about visitors to a site. This can include the visitor's name, and certain preferences. The information is obtained during the first visit to a website. The server records the information in a text file and stores it on the visitor's hard drive.[26] At the beginning of later visits, the server looks for a cookie and configures itself based on the information provided.[27] Cookies are set on websites in order to profile consumers.[28]

Spoofing

This is the use of a forged header[29] to disguise the origin of a message and fool the recipient into believing it comes from a trusted sender. It also describes an attempt to gain access to a system by posing as an authorized user, or the unauthorized use of legitimate identification and authentication data.[30]

[24] See Shirley Quo 'Spam: Private and legislative responses to unsolicited electronic mail in Australia and the United States' (2004) 1 *Murdoch University Electronic Journal of Law*. Article available at *http://www.murdoch.edu.au/elaw/issues/v11n1/quo111.html* (last accessed 12 April 2005).

[25] See Ian King 'On-line privacy in Europe — New regulation for cookies' (2003) 12 *Information and Communications Technology Law* 225 at 229.

[26] See the sources quoted in the previous note.

[27] See *http://sharepoint.agriculture.purdue.edu/agit/webtrends_glossary.aspx* (last accessed on 3 August 2006). See also Philippe Suchet 'Real time online profiling' (2004), available at *http://www.clickz.com/experts/crm/actionable_analysis/article.php/3359121* (last accessed on 20 September 2006), where the author gives a list of elements which help to build a good profile of the consumer online. These include knowing the referral sources (how the consumer arrived at a website), tracking their behaviour on the site and frequency of online visits, maintaining a full online purchase history, etc. See further Henry H Perritt, Jr *Law and the Information Superhighway* 2 ed (2001) 186.

[28] King op cit note 25 at 228–9; See also Gerrie Ebersöhn 'Internet law: Cookies, traffic data, and direct advertising practices' (2004) 16 *SA Merc LJ* 741 at 742–6.

[29] 'A header is a part of the e-mail message that precedes the message. It contains information such as the originator ('from'), recipients ('to') and the subject of the message.' See *http://www.eudora.com/techsupport/kb/2148hq.html* (last accessed on 19 September 2006). See also s 3(8) of the CAN-SPAM Act.

[30] See *http://imms.com/cyberglos/* (last accessed on 19 May 2006, but was no longer available at the time of going to press). This also includes instances where spam is sent via the ISP's website without the ISP's knowledge or consent. See *also http://www.sophos.com/security/spam-glossary.html#spoofing* (last accessed on 26 January 2008), where spoofing is defined as follows: 'When spammers forge an email address to hide the origin of a spam message. Email scammers and virus writers also use this trick. Scammers spoof address lines to fool people into thinking an email has arrived from a legitimate source, such as an online bank. Similarly, virus writers have passed

Harvesting

E-mail address harvesting is a general term covering the methods spammers use to find new e-mail addresses via legitimate websites. Besides buying lists from other spammers, the most common method is the use of harvesting (or snidding) software. This works by scanning web pages, Usenet postings, online profiles, mailing lists and chat rooms for obvious signs of addresses like '@' followed by 'com'.[31]

PROBLEMS CAUSED BY SPAM

The nature of spam, and the methods used to send it cause the recipients to encounter a variety of problems. These include the flooding of the recipient's mailbox, making it difficult for him or her to go through legitimate e-mails without reading the spam. It also leads to employees spending time online reading and discarding unwanted messages while they should be working. The Spam Summit reported that spam costs South African businesses between R7 billion and R13 billion per annum in terms of lost productivity.[32] Furthermore, recipients also bear the installation costs of filtering software or any other software that can assist in eliminating the spam.[33] Spam also causes higher subscription fees due to the increased storage capacity required by unwanted e-mails received by the Internet service provider ('ISP').[34] The volume of the messages received can also result in the server slowing down or crashing as a result of spam messages that are undeliverable to their destination bouncing back to the ISP's server.[35] Consequently, the ISP can incur revenue loss and loss of business opportunities,[36] as well as damage to computer equipment.

off viruses as security patches by spoofing their origin as being, for example, from Microsoft technical support.'

[31] See *http://en.wikipedia.org/wiki/Email_harvesting* (last accessed on 26 May 2006). See also Uri Raz 'How do spammers harvest email addresses?' available at *http://www.private.org.il/harvest.html* (last accessed on 06 February 2008).

[32] The Spam Summit was held in October 2003. See also Geissler op cit note 17 at 39–46, where the author discusses the issue of cost shifting; Jörg Walter Haase, Nicolas Grimm & Eva Versfeld *International Commercial Law from a South African Perspective* (2003) at 134–6; and Elizabeth A Alongi 'Has the US canned the spam?' (2004) 46 *Arizona LR* 263 at 263–5.

[33] Eric Goldman 'Where's the beef? Dissecting spam's purported harms' (2003) 22 *John Marshall Journal of Computer and Information Law* 13 at 20–2; also see Haase et al op cit note 32 at 134–6.

[34] See Simmons & Simmons Communication Practice *E-Commerce Law: Doing Business Online* (2001) at 131; and also Stephen D York & Ken Chia *e-Commerce: A Guide to the Law of Electronic Business* (1999) at 24, where the authors list problems that are caused by spamming. See further s 2(2)-(6) of the CAN-SPAM Act where the findings of the US Congress on attempting to regulate spam are stated.

[35] See York & Chia op cit note 34 at 24.

[36] Loss of business opportunities occurs when the consumer moves to a different ISP, to avoid the inconvenience. Damage to computer equipment results from the overload of messages coming into the ISP's server.

The problems highlighted in this section point to the serious consequences of spam and the need for the issues surrounding this phenomenon to be addressed by all that are affected by it. Certain technical and legislative measures have been put in place in order to limit spam, but the question arises whether these mechanisms are effective. In the discussion below the focus will be, first, on the technical measures used to limit spam and, secondly, on the opt-out mechanism and its effectiveness (or lack thereof) as a legal tool to limit spam.

TECHNICAL MEASURES USED TO COMBAT SPAM

As spam threatens the way business is conducted, certain technical regulatory measures have been developed that are helpful in limiting spam. These measures include the use of filters. Various filter-software applications are installed by ISPs in order to prevent third-party spam from reaching their subscribers' e-mail addresses and also to filter their subscribers' out-going messages in order to inhibit spamming activities. This filtering software normally recognizes spam when certain words that have been identified as indicating potential spam messages — such as 'viagra' or 'free' — appear within the text of an e-mail.[37] However, filters on servers may not be an efficient method of limiting spam as they can indiscriminately filter out even legitimate e-mails that a recipient would expect to receive.[38]

Another method that mail users employ to protect themselves from receiving spam is the use of spam fighters. These include the organization called the Coalition Against Commercial e-Mail ('CAUCE'). CAUCE is an NGO dedicated to fighting spam. Its contribution to eliminating spam is educating consumers on the do's and dont's of surfing the net, and the organization also offers software packages to help eliminate spam.[39]

Consumers can also download software to eliminate spam on their computers or to prevent themselves from receiving spam, for example from companies such as Peterman Circle and E-Technik in South Africa.[40]

These technical measures are of some use in helping to combat spam, but their effectiveness is limited and for that reason the focus of this article is, as already mentioned, on the legal tools used in the fight against spam.

[37] See Gerrie Ebersöhn 'Is your e-mail being rejected?' (2004) 14 *Computers and Law* at 21 where the author discusses the pros and cons of filtering software. and Geissler op cit note 17 at 349–56.

[38] See Ebersöhn op cit note 37, Haase op cit note 32 at 151–3, and also Mossoff op cit note 2 at 632–4, where the author discusses the folly of filters.

[39] CAUCE has branches in the following countries: India, Canada, Australia and Europe. See, for instance *http://www.caube.org.au* (last accessed on 5 September 2006)) and *http://www.euro.cauce.org/en/index.html* (last accessed on 8 September 2006).

[40] See *http://peterman.co.za/spam/html* (last accessed on 25 May 2005, but at the time of going to press the site was no longer available; and *www.e-technik.com* (last accessed on 8 September 2006). E-Technik offers anti-spam tools for Outlook. This tool is downloaded free of charge from their website.

LEGISLATIVE MEASURES TO COMBAT SPAM

In countries that have anti-spam legislation, one of the options used to limit spam is the 'opt-out' mechanism. This method requires the consumer to take action in order to be excluded from future mailings. While countries such as the USA and South Africa are in favour of this mechanism,[41] others prefer the 'opt-in' mechanism.[42] The latter is a method whereby the consumer agrees to receive the spam. Once on the list, consumers can limit the intake of messages, meaning that if they do not want to receive further advertisements they can choose to opt-out. In this scenario, 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. Although this paper is concerned with the opt-out mechanism, keeping in mind this alternative will assist in evaluating the merits of the opt-out mechanism. I will now discuss the opt-out mechanism in light of s 45 of the South African ECT Act[43] and in terms of the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the 'CAN-SPAM Act') in the United States.[44]

The ECT Act

The ECT Act came into operation in August 2002. The object of the Act is to facilitate electronic communications and transactions. Its objects include developing a 'safe, secure, and effective environment for the consumer . . . to conduct and use electronic transactions'.[45] In South Africa there is no specific anti-spam legislation, but the issue of spam is addressed in s 45 of the ECT Act, which deals with unsolicited goods, services or communications, and provides 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.
>
> (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,

[41] See below the discussion on the opt-out mechanisms under the ECT Act and CAN-SPAM Act.

[42] These countries include, among others, the EU and Australia.

[43] See note 13 above.

[44] See note 10 above.

[45] See s 2*(j)* of the ECT Act.

> is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1).'

Section 45 places the primary obligation on the sender (spammer), and some burden or responsibility is also placed on the consumer. An important aspect of this provision is that if the spam message contains an offer, an agreement would only be reached once the consumer responds to the senders' e-mail.[46] A further important feature of the section is that it states that the consumer must be provided with the particulars of the source from which the sender of spam obtained the personal information of the consumer.[47] The Act gives the consumer an opportunity to cancel his or her subscription to the mailing list of the spammer — that is, opt-out from receiving unwanted e-mail.[48] The sender must then refrain from sending further spam to the consumer or face penalties.[49] Note must be taken of the fact that the Act does not state how the opt-out facility should be provided.[50] The unsubscribe facility requires two things to be effective namely: the sender to honour the request, and that the recipients must have the confidence in the efficacy of the unsubscribe method in order to use it.[51] Therefore, s 45 implies that the sending of spam is allowed in South Africa. The only time when the sender is not allowed to send spam to the consumer is when the consumer has notified the sender of his or her lack of interest in receiving further e-mails from the spammer. At first glance, this seems like a plausible attempt to limit spam. However, there are various problems that arise from the use of the opt-out mechanism and they need to be addressed.

The first problem is that the Act does not prohibit spam.[52] Only messages sent to the receiver after they have opted out are prohibited. This increases the problem of spam as it encourages spammers to send spam. The second problem relates to the cancellation of the subscription by the consumer. Although the ECT Act specifically states that the consumer should be afforded a chance to unsubscribe from the unwanted e-mail, there is nothing in the provisions of s 45 that compels the sender to honour the opt-out mechanism. Unfortunately most spam e-mails do not have an unsubscribe link, or if they do, that facility will be inoperative. This is aggravated by the

[46] Section 45(2) of the ECT Act.

[47] Section 45(1)*(b)* of the ECT Act. Section 1 of the ECT Act 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'.

[48] Section 45(1)*(a)* of the ECT Act.

[49] Section 45(4) of the ECT Act.

[50] Ibid.

[51] International Telecommunication Union (ITU) WSIS Thematic Meeting on Cybersecurity *A Comparative Analysis of Spam Laws: The Quest for a Model Law* (10 June 2005) Document CYB/03 at 22.

[52] See Buys op cit note 14.

fact that spammers disguise their headers, and as such the consumer will not succeed in cancelling their subscription because he or she will be able to trace the spammer. Moreover, the forging of headers is not penalized in the ECT Act.[53] In cases where the consumer succeeds in being taken off the list of the spammer, it confirms that his or her e-mail address is 'live' and thus the consumer often ends up receiving more spam from new sources.[54]

The third problem concerns the requirement that the sender of spam must furnish the consumer with the identifying particulars of the source from which the spammer obtained the consumers' personal information. This will only be possible in cases where the spammer has given their correct e-mail address. The nature of spam is such that the spammer would wish to remain anonymous, thus they disguise their headers when sending the spam. The purpose of this subsection is thus defeated, since spammers falsify their headers.

It is clear, therefore, that it will be hard for the recipient to get information from the spammer, especially in cases where the unsubscribe facility is inoperative. Even if the sender discloses where they have obtained the personal particulars of the consumer, the consumer might have difficulties in having recourse against those sources, as data controllers may have divulged such information to the spammers.[55] There is also a possibility that the spammer might have obtained the recipient's personal information via public sites where cookies might have been set. If that is the case, consumers will also have no recourse against the source from which the address or personal information was received.

The fourth problem is that the onus to put an end to the spamming is on the consumer. If the consumer does not opt out of the unsolicited e-mail, there is no obligation on the spammer to stop sending spam. This places the consumer in a difficult position, especially where the opt-out link is inoperative.

The fifth problem concerns the penalties meted out to those who continue to send spam after the consumer has requested that they be removed from the mailing list of the unsolicited e-mail. Most spam in South Africa originates from outside the Republic and therefore the chances of prosecuting and convicting spammers are slim. Furthermore, the efficacy of s 89 in respect of spam may be questionable. Section 89 of the ECT Act contains a list of sections to which penalties apply and s 45 is not included in that list. The ECT Act has thus created a criminal offence for which no penalty exists.

The sixth problem relates to the lack of definition of spam. The Spam

[53] Ibid and Ebersöhn op cit note 17 at 26.

[54] See Gerada op cit note 17 at 52.

[55] The term data controller means any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject. The principles on the protection of personal information are dealt with under s 50–51 of the ECT Act. The list comprises nine items that are not compulsory.

Summit reported that, although the issue of spam is covered by s 45 of the ECT Act, there are certain loopholes in the section arising largely from the fact that spam is not defined adequately.[56] The definition of spam in the ECT Act should be broadened to include at least chain letters, hoaxes, and the like.[57]

Lastly, problematic aspects of the ECT Act include issues such as harvesting of e-mails addresses, dictionary attacks, false headers, and use of misleading or deceptive subject lines. These matters are not addressed in the Act but they have an impact on the effectiveness of the opt-out facility. Of course, dealing with these issues in the ECT Act will not of itself eliminate spam, but it would be a good start in the efforts to deal more effectively with the problem. In fact, some of these issues are dealt with under the CAN-SPAM Act in the USA, the discussion of which follows below.

The CAN-SPAM Act

In the United States the CAN-SPAM Act came into operation on 1 January 2004.[58] Before this act came into operation, most states had their own legislation dealing with spam. Only twelve states did not have such legislation.[59] States that legislated spam adopted either opt-out or opt-in mechanisms, with most states favouring the opt-out mechanism.[60] In addition, provisions were included in these statutes prohibiting the falsifying of routing information or the use of misleading subject lines in all commercial e-mails,[61] or the use of third-party Internet addresses or domain names without consent.[62] The statutes also required that where sexually explicit or unsolicited commercial e-mails were sent, they had to include the label 'ADV' (meaning advertisement) at the beginning of the subject lines and also the sender's name, physical address and domain name or e-mail

[56] The Spam Summit op cit note 32; see also Buys op cit note 14 at 160–1.

[57] See Buys supra note 14 at 160.

[58] Section 16 of the CAN-SPAM Act.

[59] States that had not enacted legislation relating to unsolicited bulk or commercial e-mail included: Alabama, Hawaii, Kentucky, Massachusetts, Mississippi, Montana, Nebraska, New Hampshire, New Jersey, New York, South Carolina and Vermont.

[60] Of the states that have anti-spam legislations or provisions towards eliminating spam, only two states adopted the opt-in mechanism, namely California and Delaware. See *http://www.spamlaws.com* (last accessed on 18 September 2006) and also David E Sorkin 'Spam legislation in the United States' (2003) 22 *John Marshall Journal of Computer and Information Law* 3 at 6. (The favouring of the opt-out mechanism by most states is in all probability the reason why the CAN-SPAM Act adopted this mechanism.)

[61] These include the following state legislation: Arizona Revised Statutes Title 44 (Trade and Commerce) 1372–01; Florida Statutes Title 39 (Commercial Relations) 668.603; State of Colorado, Sixty Second General Assembly, House Bill 1309 Title 6–2.5–103; and Illinois Compiled Statutes Chapter 815 (Business Transactions Deceptive Practices) 815 ILCS 511/10. These statutes are available at *http://www.spamlaws.com* (last accessed on 22 September 2006).

[62] Ibid.

address.[63] The coming into operation of the CAN-SPAM Act has the effect that the individual provisions of many states have been superseded.[64]

The CAN-SPAM Act establishes requirements that must be met by those who send commercial e-mail and it spells out penalties for senders and companies whose products are advertised in spam in violation of the law.[65] As with the ECT Act, CAN-SPAM gives consumers the right to ask the senders of spam to stop sending it.[66]

This Act covers commercial e-mail messages, the primary purpose of which is the advertisement or promotion of a commercial product or service, including content on an Internet website operated for a commercial purpose.[67] It provides protective measures for users of commercial e-mail and these include the following prohibitions:

First, the transmission of false or misleading information is banned. The Act states that the senders' e-mails 'From' and 'To' and routing information, including the originating domain name and e-mail address, must be accurate. Furthermore, the e-mail must identify the person who initiated the e-mail.[68] In terms of the Act, header information will be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message (e g because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin).[69]

Secondly, the Act prohibits deceptive subject lines.[70]

Thirdly, the sender must provide the recipient with an opt-out method. The sender must provide a functioning return e-mail address or another Internet-based response mechanism that allows a recipient to request the sender not to send future e-mail messages to that e-mail address, and the sender must honour that request.[71] This Internet-based mechanism must be displayed clearly and conspicuously so that the recipient may use it to reply to that email in order to inform the sender that her or she does not desire

[63] These include the following states: Arkansas Code Title 4 Chapter 88 (Deceptive Trade Practices) 4–88–602; Kansas Statutes Chapter 50 (Unfair Trade and Consumer Protection) Article 6 (Consumer Protection) 50–6,107; Louisiana Revised Statutes Title 14 (Criminal Law) Section 106; Pennsylvania Consolidated Statutes, Title 18 (Crimes and Offences Chapter 59) Public Indecency 5903; Utah Code Title 13 (Commerce and Trade Chapter 36) Unsolicited Commercial and Sexually Explicit Email Act 13–36–103; and Wisconsin Statutes Criminal Code Chapter 944 (Crimes Against Sexual Morality) 944.25.

[64] See s 8*(b)* of the CAN-SPAM Act.

[65] Sections 4–6 of the CAN-SPAM Act.

[66] Section 5(5) of the CAN-SPAM Act.

[67] Section 3(2)(A) of the CAN-SPAM Act.

[68] Section 5*(a)*(1) of the CAN-SPAM Act.

[69] Section 5*(a)*(1)(C) of the CAN-SPAM Act.

[70] Section 5*(a)*(2) of the CAN-SPAM Act. The Act provides that the subject line may not mislead the recipient about the contents or subject of the message.

[71] Section 5*(a)*(3)(A) of the CAN-SPAM Act.

future mailings from the sender.[72] The sender can also create a menu of choices to allow the recipient to opt-out of certain types of messages, but one must include the option to end any commercial message from the sender.[73] According to the Act any opt-out mechanism that is offered must be able to process opt-out requests for at least thirty days after the sender has sent commercial e-mail.[74] When the sender receives an opt-out request, the Act gives the sender ten business days to stop sending e-mail to the consumer's e-mail address. Furthermore, the transfer of e-mail addresses to other entities may only be done in such a way that those entities are able to comply with the law.[75]

Fourthly, the Act prohibits the transmission of commercial e-mail after objection. Address harvesting and dictionary attacks from public sites such as Usenet and chat forums are considered as aggravated violations relating to commercial e-mail and are thus prohibited by the CAN-SPAM Act.[76] The Act also requires e-mails containing sexually-oriented material to place warning labels on those e-mails.[77]

The CAN-SPAM Act has created penalties for different unlawful acts committed while spamming. The Act establishes the Commission whose duty it is to prevent any person from violating the provisions of the Act.[78] Additional fines are provided for commercial e-mail senders who not only violate the rules described above, but also the harvesting of e-mail addresses from websites or web services that have published a notice prohibiting the transfer of e-mail addresses for the purpose of sending e-mail. State officials may also institute civil actions against the perpetrator(s) on behalf of the recipients, and claim damages from them of up to $2 million for any violation of s 5.[79]

It would seem that the CAN-SPAM Act protects consumers against spam more effectively than the ECT Act. However, although the CAN-SPAM Act will serve to deter spammers to some extent,[80] there are also criticisms levelled against it. First, it is said that the CAN-SPAM Act limits the role of the individual states in combating spam, and that enforcement actions lie primarily in the hands of the Federal Trade Commission (FTC).[81] Secondly,

[72] Section 5*(a)*(3) of the CAN-SPAM Act.

[73] Section 5*(a)*(3)(A)*(i)* of the CAN-SPAM Act.

[74] Section 5*(a)*(3)(A)(ii) of the CAN-SPAM Act.

[75] Section 5*(a)*(4) of the CAN-SPAM Act.

[76] Section 5*(b)*(1) of the CAN-SPAM Act.

[77] Section 5*(d)* of the CAN-SPAM Act.

[78] Section 7*(a)* & *(d)* of the CAN-SPAM Act.

[79] Section 7*(f)*(1)–(3). Section 5 deals with protections for users of commercial e-mail.

[80] Erin Elizabeth Marks 'Spammers clog in-boxes everywhere: Will the CAN-SPAM Act of 2003 halt the invasion?' (2004) 54 *Case Western Reserve LR* 943 at 952, where the author discusses the strengths and weaknesses of the CAN-SPAM Act.

[81] Marks op cit note 80; See also s 8*(b)* of the CAN-SPAM Act, which states that the Act has the effect of pre-empting other state laws.

it is also said that the CAN SPAM Act under-protects consumers and does not solve the spam problem.[82] Thirdly, it is averred that the Act does not create an effective solution because it allows the sender to invade in-boxes and forces spam recipients to take positive action to curtail future invasions.[83] Fourthly, it has been pointed out that the CAN-SPAM Act supersedes state laws, some of which had more stringent requirements and heavier penalties.[84] Fifthly, the critics cite as a problem the fact that the Act allows spammers to send messages as long as each message offers a legitimate link from which one can request that the spammer refrains from sending future e-mails.[85]

In light of these concerns, it is clear that this measure is not as effective as it might have been. However, some provisions of this Act can be helpful in developing our law in respect of the limitation of spam.

CONCLUSION

Spam is threatening the way we communicate. It is a booming business negatively affecting consumers. The fact that many countries have legislation in place shows that the world is serious about eliminating, or at least limiting, spam. However, measures such as the opt-out mechanism under s 45 of the ECT Act have proven to be ineffective, especially in light of the absence of a procedure on how the opt-out mechanism has to be administered and the lack of a proper definition of what constitutes unsolicited commercial communications.

Perhaps some of the steps that are laid out in the CAN-SPAM Act may shed light on how to limit spam. For instance, note should be taken of its measures in respect of the falsification or disguising of headers, address harvesting, as well as its procedure on how to administer opt-out mechanisms. Some authors are of the opinion that South Africa should rather make use of the opt-in mechanism like the EU and Australia, thus making it illegal to send spam.[86] This would be a good starting point, but legislation on its own will not eliminate spam, since spammers will continue to develop new technologies to evade the law.[87]

Considering that spam is a global problem, global measures need to be put in place. All stakeholders must combine to conduct more research and

[82] Mossoff op cit note 2 at 637

[83] Marks op cit note 80 at 953; See also Daniel L Mayer 'Attacking a windmill: Why the CAN-SPAM Act is a futile waste of time and money' (2004) 31 *Journal of Legislation* 177 at 189; and Sorkin op cit note 60 at 11.

[84] See Alongi op cit note 32 at 287.

[85] Marks op cit note 80 at 953 and Alongi op cit note 32 at 288.

[86] See Geissler op cit note 17 at 303; Haase op cit note 32 at 157; and Marks op cit note 80 at 953–4.

[87] Mayer op cit 83 at 189–90 and Goldman op cit note 33 at 27.

resolve this pressing issue. What is needed is a multi-layered approach, which will include legislation, technical solutions and also consumer education.[88]

[88] Marks op cit note 80 at 963 and Haase op cit 32 at 163.