E-mail, Electronic Communications and Transactions Act, Interception of communications, Internet, Internet jurisdiction, Internet Service Providers, Opt-in and Opt-out, Spam, Unsolicited Bulk Email, Unsolicited Commercial E-mail.
SUMMARY

In the context of the Internet, spam generally refers to unsolicited and unwanted electronic messages, usually transmitted to a large number of recipients. The problem with spam is that almost all of the related costs are shifted onto the recipients, and many of the messages contain objectionable content.

Spam has become a significant problem for network administrators, businesses and individual Internet users that threatens to undermine the usefulness of e-mail. Globally, spam spiralled to account for over 60% of all e-mail near the end of 2004. It is a problem that costs the global economy billions of dollars a year in lost productivity, anti-spam measures and computer resources. It has forced governments to enact legislation against the problem and it has prompted the development of numerous technical countermeasures.

Spam can only be defeated by a combination of legal measures, informal measures (including self regulation and social norms), technical measures and consumer education.

Because spam is a relatively recent and evolving problem, the application of various common law mechanisms are explored, including the law of privacy
and the law of nuisance. Various constitutional concerns may also arise in the context of spam, and the right to freedom of expression must be balanced against other competing rights and values, including the right to privacy.

Comparative legislation is examined, because it is important to recognise trends in spam legislation in other jurisdictions so as to ensure a measure of interoperability with those laws. The practical difficulties in identifying spammers, and the lack of jurisdiction over offshore offenders affect the practical implementation of the current protection offered by the ECT Act.

In conclusion, this thesis identifies the need for direct anti-spam legislation in South Africa, and suggests various clauses that will need to be catered for in the legislation. It is submitted that "opt-in" legislation should be preferred over "opt-out" legislation. It is further submitted that a definition of spam should be based on the volume and indiscriminate nature of the email, and not only on whether the communication was commercial. Therefore, a definition of bulk unsolicited e-mail is proposed.
"Wasting somebody else's time strikes me as the height of rudeness. We have only so many hours, and none to waste. That's what makes electronic junk mail and e-mail hoaxes so maddening. The "free" distribution of unwelcome or misleading messages to thousands of people is an annoying and sometimes destructive use of the Internet's unprecedented efficiency. Few tools in history have been as powerful as the Internet. Although still in its infancy, the Internet is beginning to transform the world by making communication and publishing fantastically inexpensive and accessible. But like any powerful tool, it is subject to misuse and abuse".¹

Bill Gates

1. Introduction

The present chapter provides a general introduction to this thesis. Part A gives an overview of the Internet, electronic mail and unsolicited electronic messages, and Part B details the scope and purpose of this study and briefly outlines each chapter included in this thesis.

¹ Gates "On Spam: Wasting Time On The Internet (3/25/98)" available at http://www.microsoft.com/BillGates/columns/1998essay/3-25col.asp (16 May 2003). This article comments that spam is sent to tens of thousands of people because of the fact that the incremental cost of sending a message on the Internet is essentially
PART A: GENERAL INTRODUCTION

2. The Internet

Matthew Burnstein\(^2\) describes the Internet as a “network of networks”\(^3\) that links computers and users worldwide.

The Electronic Communications and Transactions Act\(^4\) ("the ECT Act") defines the Internet as:

"the interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof".

Through the use of the Internet, countries and communities are no longer isolated by physical constraints, such as differences in language, culture, laws and trading methods. This is because the Internet is globally accessible and the mechanics and protocols are universal.

The Internet was created in 1958 by the Advanced Research Projects Agency ("ARPA").\(^5\) It was born out of cold war paranoia as an experiment by zero. This wastes an enormous amount of their collective time, at almost no cost to the senders.


\(^3\) A network is when two or more computers are connected so that they are able to share resources.

the United States Department of Defence to design a communications system that would withstand a Russian nuclear attack. ARPAnet enabled scientists and the military to share computer resources and collaborate on research projects. This was the network that formed the basis for the Internet.

The nature of the Internet was such that it was "user unfriendly" and it remained primarily in the domain of academics for a number of years. The Internet became more "user friendly" in the early 1990's, with the development of the World Wide Web, and this led to its rapid commercialisation. 6

A user must access the Internet through an Internet Service Provider ("ISP") using a browser, such as Microsoft's Internet Explorer. In simplistic terms, a user logs onto the Internet from a computer, requests information, and a computer somewhere on the globe serves the requested information up to their computer. Information can be in text, graphical or multimedia formats. There are also a number of other services available such as electronic-mail

---

5 ARPA, the Advanced Research Projects Agency, was created in 1958 as part of the United States Department of Defense. ARPAnet enabled scientists and the military to share computer resources and collaborate on research projects. It was the network that formed the basis for the Internet. See Street and Grant Law of the Internet (2000) at page xxxi. See also NOIE "Spam" available at http://www.noie.gov.au/publications/noie/spam/final_report/what.htm (15 May 2003).

(e-mail), File Transfer Protocol ("FTP"), Internet Relay Chats ("IRC"), List
servers (e-mail mailing lists) and Newsgroups.\(^7\)

The ISP is connected to regional networks, that are in turn connected to
"backbones" (high capacity networks). Each network is separately
administered, maintained and paid for. As such, there is no central
ownership or management of the Internet. There are, however, various
groups who influence the direction the Internet takes including private
companies, Governments and organisations such as the "Internet Society".

3. **Electronic Mail (E-mail)**

While technological progress has opened numerous new opportunities in
online services, one of the oldest and most basic Internet applications,
electronic mail, remains the most widely used. It is estimated that some 31
billion email messages were sent over the Internet in 2002, and that this
number will reach 60 billion in 2006.\(^8\) For millions of people around the world

---

\(^7\) See Street and Grant *Law of the Internet* (2000) at page xxx. See also Burnstein
"A Global Network In A Compartmentalised Legal Environment" *Law and Electronic

\(^8\) At the end of 2000 there were 891.1 million electronic mailboxes in the world. In
1985 there were fewer than 2 million e-mail accounts in the world. By 1995 there
were 98.6 million e-mail accounts, and 85 percent were at-work accounts. Webmail
services such as Hotmail attracted millions of new users to the extent that
consumers now own 60 percent of e-mail accounts. The spread of wireless devices
continues to drive the growth of e-mail. Even though many of the world's e-mail
accounts are inactive or act solely as spam receptacles, and many e-mail users
have more than one account, it is estimated that one in 13 people in the world have
an e-mail account. See further Foley "E-Mail: The Wonder Tool" available at
e-mail has become a convenient way to communicate and exchange information.

E-mail has transformed the way companies and other organisations conduct their business. It provides a quick and efficient tool for communications and information sharing. E-mail has also dramatically changed the relationship between consumers and suppliers of products and services. It allows companies to quickly inform their customers of new products and services. It has also become one of the most cost efficient ways of providing customer support and assistance.

E-mail is an extremely important and effective means of communication and is used by millions of people on a daily basis for personal and commercial purposes. Its convenience and efficiency, however, are increasingly being threatened by the rise in spam.9

4. Unsolicited Electronic Messages

As is often the case when a new technology appears, abuse is not far behind. Unsolicited electronic messages, or "spam", has become a significant problem for network administrators, businesses and individual Internet users that threatens to undermine the usefulness of email.10 It is

---

9 For the purposes of this thesis, spam is defined as unsolicited bulk e-mail. See further Chapter 2 below for the history of the term "spam".
10 See further Chapter 2 below.
eroding trust in technology, costing business billions of Rands a year,\textsuperscript{11} and decreasing our ability to realise technology's full potential. It has been described as being "the mosquitoes of the Internet – numerous, annoying and often carrying objectionable content and nasty viruses".\textsuperscript{12}

After large-scale commercial spam made its public debut on Usenet in the infamous Canter and Siegel "green card lawyers" incident in 1994,\textsuperscript{13} the proliferation of spam has rapidly increased. The use of the Internet to send large volumes of e-mail to promote products and services has infuriated many consumers, forced employees in organisations to waste time identifying and deleting junk e-mail, and strained the facilities of Internet service providers.

Spam is a global concern, and Internet users world-wide are plagued by this problem. According to some industry estimates, spam currently accounts for more than fifty percent\textsuperscript{14} of all e-mail traffic, and the number of unwanted e-mails is increasing exponentially.

\textsuperscript{11} It is estimated that spam costs South African businesses between R7 billion and R13.1 billion per annum just in terms of lost productivity. See "SA Spam Summit An Unequivocal Success" \textit{TechSmart} (2003) Issue 6/1.

\textsuperscript{12} Michalson "The Law Vs The Scourge Of Spam" available at \url{http://www.itweb.co.za/sections/specialfocus/michalson030919.asp} (3 October 2003).

\textsuperscript{13} See further Chapter 2 below for the history of spam.

\textsuperscript{14} See further Microsoft "Letter From Bill Gates To The U.S. Senate Commerce Committee Regarding Spam Hearings" available at \url{http://www.microsoft.com/presspass/misc/BillgSpam05-21-03.asp} (2 July 2003).
The growth in spam also imposes significant costs on Internet Service Providers, businesses, and other organisations, since they can only handle a finite volume of e-mail without making further investments in their infrastructure. It is a problem that costs the global economy billions of dollars a year in lost productivity, anti-spam measures and computer resources.\textsuperscript{15}

\textbf{PART B: SCOPE AND PURPOSE OF THIS STUDY}

5. \textbf{Objectives and Methodology}

The title and subject of this thesis is \textit{Bulk Unsolicited Electronic Messages (SPAM): A South African Perspective.}

The objective of this thesis is to give a South African perspective of the nature and the extent of the threat of spam, and to propose possible solutions that may be utilised to address this problem.

In order to achieve this objective, this thesis looks at what spam is, and why it is a problem. The problem of spam is examined within the context of South African law, including a discussion of the ECT Act and the application of various common law mechanisms. A study of comparative legislation is also necessary because it is important to recognise trends in spam legislation in other jurisdictions so as to ensure a measure of interoperability with those laws. This leads to a discussion of the international nature of the problem

\textsuperscript{15} See further Chapter 2 below.
and jurisdictional issues, because the practical difficulties in identifying spammers, and the lack of jurisdiction over offshore offenders affect the practical implementation of the current protection offered by the ECT Act.

Various constitutional concerns may also arise in the context of spam, and this thesis suggests that the right to freedom of expression must be balanced against other competing rights and values, including the right to privacy.

It is submitted that spam can only be defeated by a combination of legal measures, informal measures (including self regulation and social norms), technical measures and consumer education. Various alternative solutions that are available to supplement the law are therefore explored.

Finally, this thesis identifies the need for direct anti-spam legislation in South Africa, and suggests various clauses that will need to be catered for in the legislation.

The focus of this paper is on all unsolicited bulk email, and is not limited to only commercial bulk e-mail. This is because many of the issues associated with spam arise due to its unsolicited and bulk qualities and not its content. In any event, this distinction may be somewhat academic as the majority of unsolicited e-mail messages today are commercial in nature.
6. **Chapter Outlines**

Chapter two serves as a general introduction to this thesis. It answers the questions: what is spam, why is it a problem, and how does it impact on the workplace. One of the issues that is examined is the difficulty of defining spam, and the difference between unsolicited bulk e-mail and unsolicited commercial e-mail. This chapter discusses the extent of the threat of spam, and identifies issues such as the threat to e-mail in general, the ways in which spammers obtain e-mail addresses, the illegal or objectionable content of some spam, and the impact of cost shifting on the Internet backbone, Internet Service Providers, and individual users. This chapter also analyses spam in the workplace and looks at the Interception and Monitoring Prohibition Act\(^\text{16}\) and the Regulation of Interception of Communications and Provision of Communication-Related Information Act\(^\text{17}\). Consent precedents and clauses to be included in a communications facilities policy are also suggested. Finally, this chapter provides various common examples of spam.

Because spam is a relatively recent and evolving problem, the application of various elements of common law, regulation and self-regulation to the problem is also evolving, both within South Africa and internationally. Chapter three studies some of the legal mechanisms that are in place in South Africa that may be used to deal with the problem of spam. This

\(^{17}\) Act 70 of 2002.
chapter includes a brief history of Roman-Dutch law in South Africa and the nature and sources of South African law, including constitutional law, common law and statutory law. It looks at spam under current South African law, focusing on the Electronic Communications and Transactions Act\(^\text{18}\) ("the ECT Act") and potential problems with the ECT Act in the context of spam. Various other areas of law that may be applicable to the problem of spam, including, \textit{inter alia}, the law of privacy and the law of nuisance are also studied for the purposes of categorising spam into an area or areas of law.

Chapter four explores what comparative jurisdictions have done to address the problem of spam. The benefits of "opt-in" legislation are weighed against "opt-out" legislation, and legislation prohibiting only unsolicited commercial e-mail rather than all unsolicited bulk e-mail is discussed. Comparative legal approaches are also explored in order to illustrate possible avenues for the extension of the provisions of the ECT Act relating to spam.

Global computer-based communications cut across territorial borders, undermining the feasibility and legitimacy of applying laws based on geographic boundaries. New rules are needed to govern a wide range of new phenomena that have no clear parallel in the nonvirtual world. Chapter five focuses on the international nature of the problem of spam, and examines the compatibility of traditional laws, formulated with national

borders in mind, when applied to the Internet. Issues such as jurisdiction, including the concept of "place" on the Internet, uploading and downloading, and the difficulty of determining nationality in cyberspace are addressed. This chapter examines possible approaches that may be adopted where Internet-related disputes arise, such as unifying the choice of law rules, unifying a substantive law of the Internet, harmonising the laws of different jurisdictions, and recognising the Internet as a jurisdiction in its own right.

Chapter six discusses constitutional concerns that may arise in the context of spam. The right to freedom of expression is studied, including various instances where the right to freedom of expression must be balanced against competing rights and values. The right to privacy is also briefly examined including United States case law illustrating the restriction on the right to freedom of expression in favour of the right to privacy.

Chapter seven illustrates various alternative solutions that are available to supplement the law. This chapter focuses specifically on self regulation, technology and consumer awareness, since it appears that the solution to the spam problem lies in the co-ordination of these alternatives with legal approaches.
Chapter eight outlines the need for direct anti-spam legislation in South Africa, and suggests a framework of various clauses that will need to be catered for in the legislation.

This paper does not contain a separate chapter setting out conclusions and recommendations, because the above chapters are individually concluded in their own right.
CHAPTER 2
ANALYSIS OF THE NATURE AND THE PROBLEM OF SPAM

1. Introduction

In the context of the Internet, spam\(^1\) generally refers to unsolicited and unwanted electronic messages, usually transmitted to a large number of recipients. Spam is also called Unsolicited Bulk E-mail ("UBE"), or the more narrowly defined Unsolicited Commercial E-mail ("UCE").

---

\(^1\) The prevailing theory is that the use of the term 'spam' was adopted from the song in Monty Python's "Spam-loving Vikings" skit, in which a group of Vikings sang a chorus of "Spam, spam, spam…" in increasing crescendo, drowning out other conversation. The analogy was that unsolicited bulk e-mail was drowning out normal discourse on the Internet. It refers to bulk, mass, or repeated posting or mailing of substantially identical messages. See Chissick *Electronic Commerce Law and Practice* (2000) 2\(^{nd}\) Edition at xxxviii; Froomkin "Critical Theory Of Cyberspace" *Harvard Law Review* volume 116 at page 825.

The term was first used in the early 1990's to describe email messages not related to the topic of discussion that swamped newsgroups. The term is rumoured to have originated from the MUD/MUSH community. It reportedly came to be used in connection with online activities following a mid-1980s episode in which a participant in a MUSH created and used a macro that repeatedly typed the word "SPAM", interfering with others' ability to participate. See Falk "The Net Abuse FAQ Revision 3.2" s2.4, available at [http://www.cybernothing.org/faqs/net-abuse-faq.html](http://www.cybernothing.org/faqs/net-abuse-faq.html) (16 May 2003); Rich "Internet Legal Issues: Spam" available at [http://www.publaw.com/spam.html](http://www.publaw.com/spam.html) (16 May 2003); Kadow’s Internet Dictionary available at [http://www.msg.net/kadow/answers/s.html](http://www.msg.net/kadow/answers/s.html) (15 May 2003); A MUSH, or a multi-user shared hallucination, is a type of MUD (a multi-user dimension or dungeon). See Howe "Free Online Dictionary of Computing" available at [http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?Multi-User+Shared+Hallucination](http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?Multi-User+Shared+Hallucination) (20 October 2003) (defining "MUSH") and [http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?Multi-User+Dimension](http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?Multi-User+Dimension) (20 October 2003) (defining "MUD").

"SPAM" is also the trade mark of a popular canned meat product produced by Hormel Foods Corporation. See Hormel Foods Corporation "Spam And The Internet" available at [http://www.spam.com/ci/ci_in.htm](http://www.spam.com/ci/ci_in.htm) (10 June 2003). "SPAM" written in capital letters is the trade mark term for Hormel’s canned lunch meat while "spam", in lowercase, is popular slang for unsolicited bulk e-mail.
Chapter 2

This chapter examines what spam is and why it is a problem. Part A looks at various definitions of spam, including the difference between unsolicited bulk e-mail and unsolicited commercial e-mail.

Part B discusses why spam constitutes a threat, and identifies issues such as the threat to e-mail in general, the ways in which spammers obtain e-mail addresses, the illegal or objectionable content of some spam, the use of misleading subject lines, and the impact of cost shifting on the Internet backbone, Internet Service Providers, and individual users. Part B also looks at the potentially unlimited volume of spam, deceptive practices employed by spammers and the viability of "opt-out" options.

Part C analyses spam in the workplace and looks at the Interception and Monitoring Prohibition Act\(^\text{20}\) and the Regulation of Interception of Communications and Provision of Communication-Related Information Act.\(^\text{21}\) Consent precedents and clauses to be included in a communications facilities policy are also suggested. Part C also tracks the South African Energizer decision\(^\text{22}\) and looks at the United States as a comparative jurisdiction. This part is included to illustrate the impact of spam in the workplace and the potential problems that it creates in the work environment.

\(^{21}\) Act 70 of 2002.
\(^{22}\) The decision handed down by Advocate Roland Sutherland SC in the private arbitration of Jacqueline Bamford and 4 others and Energizer (SA) Limited[2001] 12 BALR 1251 (P).
Part D provides various examples of spam, including chain letters, sympathy hoaxes, petitions, urban legends, the myth of email tracking, destructive codes and viruses, cartoons, scams, and the efforts of paedophiles and pornographers. This part is included to enable the reader to appreciate the numerous different forms of messages that may be regarded as spam.

Finally, Part E comprises a conclusion for the present Chapter.

PART A: HISTORY AND DEFINITION OF SPAM

2. Introduction

Spam is the Internet equivalent of junk mail and telemarketing. Most spam is of a commercial nature and is often used for advertising dubious products, financial scams, and get-rich quick schemes. However, spam may also be misleading and deceptive, like those advertising miracle diet and health products, or contain offensive or sexually explicit material. A message need not be offensive or commercial, or be sent fraudulently, to qualify as spam. The term “spam” has also been used to describe virus warnings, urban legends, jokes, chain letters, and similar messages forwarded by friends, relatives and other acquaintances.23

---

Spam is typically anonymous, indiscriminate and global and has therefore become a popular vehicle for promotions that may be illegal, unscrupulous or use tactics that would not be commercially or legally viable outside the virtual environment.

Spam usually has one or more of the following characteristics:\(^\text{24}\)

a) It is sent in an untargeted and indiscriminate manner, often by automated means;

b) It includes or promotes illegal or offensive content;

c) Its purpose is fraudulent or otherwise deceptive;

d) It collects or uses personal information;

e) It is sent in a manner that disguises the originator;

f) It does not contain a valid or functional address to which recipients may opt out of receiving further unsolicited messages.

2.1 **Typical Conduct Of Spammers**

The Court in *Hotmail Corp v Van$ Mony Pie, Inc*,\(^\text{25}\) detailed the conduct of various spammers in that case. The actions of the spammers in this case are evidence of the means by which spammers generally operate, and the


damage that the actions of spammers can have on an Internet Service Provider ("ISP").

The defendants were sending spam e-mails to thousands of Internet email users, which were intentionally falsified in that they contained return addresses bearing Hotmail account return addresses, including Hotmail's domain name, when in fact the messages did not originate from Hotmail or a Hotmail account. The spam was transmitted through e-mail providers other than Hotmail, and the spammers falsely designated a real Hotmail email address as the point of origin. The spam messages advertised pornography, bulk e-mailing software, and "get-rich-quick" schemes.

The defendants had also created a number of Hotmail accounts for the specific purpose of facilitating their spamming operations. These accounts were used to collect responses to their e-mails and "bounced back" or undelivered messages in what amounted to a "drop box" whose contents were never opened, read or responded to. These Hotmail accounts were also used to serve as legitimate return addresses for recipients wishing to respond to the e-mails.

As a result of the falsified return addresses, Hotmail was inundated with hundreds of thousands of misdirected responses to the defendants' spam, including complaints from Hotmail subscribers regarding the spam and
“bounced back” e-mails which had been sent by the defendants to non-existent or incorrect e-mail addresses.

This overwhelming number of e-mails took up a substantial amount of Hotmail's finite computer space, and threatened to delay and otherwise adversely affect Hotmail's subscribers in sending and receiving email. It resulted in significant costs to Hotmail in terms of increased personnel necessary to sort and respond to the misdirected complaints, and it damaged Hotmail's reputation and goodwill.

3. The History Of Spam

Prior to the commercialisation of the Internet, spam was not a significant problem: "Unsolicited e-mail consisted mostly of messages from pranksters, chain letters, and inappropriate messages sent to established email lists by individuals who were either unaware that their message would go to the entire list or unaware that their messages were inappropriate for that forum".26

One of the first recorded instances of spam dates back to 3 May 1978 when Gary Theurk, a marketer at the Digital Equipment Corporation ("DEC"),

spammed ARPAnet users about new DEC products.\footnote{ARPA, the Advanced Research Projects Agency, was created in 1958 as part of the United States Department of Defense. ARPAnet enabled scientists and the military to share computer resources and collaborate on research projects. It was the network that formed the basis for the Internet. See NOIE "Spam" available at http://www.noie.gov.au/publications/noie/spam/final_report/what.htm (15 May 2003).} This message was a clear violation of the ARPAnet official "acceptable use policy" which limited it to use in support of research and education. They were chastised for breaking the ARPAnet appropriate use policy and a notice was sent out reminding others of the rule.

Probably the first major commercial spamming occurred in April 1994, when two lawyers from Phoenix, Arizona, Canter and Siegel, posted a message for the United States immigration status "Green Card lottery".\footnote{A raffle for non-Americans to win a US work permit. Canter and Siegel offered to complete immigration lottery forms for $95 per person, or $145 a couple, not mentioning that it was free to enter. See further Lloyd Information Technology Law (2000) at page 557.} They hired a mercenary programmer to post their advertisement to every newsgroup\footnote{Approximately 6,000 news groups.} on USENET, the world's largest online conferencing system. Canter and Siegel incurred a cost of thirty dollars for their advertising efforts, or the cost for their ISP subscription. Their Internet Service Provider, Internet Direct, however, cancelled their account after a flood of complaints from Internet users rendered Internet Direct’s systems inoperative.\footnote{In response to incidents such as this, Internet service providers began adding provisions to their subscriber terms and conditions prohibiting the posting of commercial advertisements to non-commercial USENET groups.}
4. A Definition Of Spam

As an American judge\textsuperscript{31} observed about pornography, "I know it when I see it". There is a similar problem with defining spam - it is difficult to define, but you know it when you see it.

It is necessary to have an accurate definition of spam in order for anti-spam provisions to be effective. This will assist Internet Service Providers and regulatory authorities to enforce their terms and conditions or any regulations or laws regulating spamming. It will also assist legitimate direct marketers to ensure that their activities are both ethical and legal.

Arriving at an agreed definition of spam is a potentially contentious issue, however. ISPs, privacy and consumer protection groups, blacklists, the direct marketing industry, and spammers themselves, all have their own interests and views. Many want to define spam as anything they do not like or did not ask for. Many want to claim that any traffic sent to their machine without their invitation is an invasion of their property or theft of their resources. However, our system of law and justice is based on the principle of letting some of the guilty go unpunished to avoid punishing the innocent. We therefore have to accept that any fair system we design will not cover every spam. If we are able to catch 99 percent of spam, this will be enough to turn it from a mailbox destroyer to an occasional nuisance.

\textsuperscript{31} Stewart J in Jacobellis v Ohio378 US 184 (1964) 197.
4.1 The Difference Between Unsolicited Bulk E-mail And Unsolicited Commercial E-mail

Spam may be defined as Unsolicited Bulk Email ("UBE"), or more narrowly as Unsolicited Commercial Email ("UCE").

4.1.1 Unsolicited

The key element of most definitions of spam is that the email messages must be "unsolicited". In general, a communication is considered to be unsolicited if there is no prior relationship between the parties, and the recipient has not explicitly consented to receive the communication. "Unsolicited means that the recipient has not granted verifiable permission for the message to be sent".

Bulk e-mail would probably not be regarded as spam where the recipient has previously dealt voluntarily with the sender before, and the sender can reasonably assume, on the basis of that existing relationship, that the recipient is prepared to accept messages of the type being sent.

Some bulk e-mail is permission based, where the recipient has asked to receive it, for example where a user agrees to receive e-mail or a newsletter as part of a mailing list. This "opt-in" email usually provides a benefit such

---

33 The Spamhaus Project "The Definition Of Spam" available at
as free information or sales prices. However, a user may previously have asked a sender for bulk email, but then later asked that sender not to send further emails, or did not indicate a desire for additional emails. Any emails sent after the initial request may be regarded as unsolicited.

A mere visit to a Web site does not constitute a solicitation by the visitor for further communication from the party that owns or operates the Web site. Failing to click on a "do not send me marketing literature by e-mail" button on a Web sign up form does not convey explicit permission. An e-mail address that is placed on a Web page, on a mailing list, or on Usenet, also does not imply consent.

4.1.2 Commercial

Some definitions of spam only include messages that are commercial in nature. The term UCE is most frequently used in the United States where constitutional restrictions are believed to prevent legislation restricting other types of spam. UCE is generally defined in terms of message content rather than the sender’s actual or presumed motivation for sending the message. A typical definition includes any message that promotes the sale of goods or services.


Such a request is commonly referred to as an "opt-out" request.

See Chapter 4 (Australia) and Chapter 8 below discussing consent.

The First Amendment right to freedom of speech, see further Chapter 6 below.

4.1.3 Bulk

It is arguable that the real issue with spam is not about content. The main concern with spam relates to the method of delivery. Therefore, spam is often defined as messages sent in large quantities, or in bulk.

"Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content". It is often the use of automation to send the same message to multiple unrelated parties.

A bulk message could be a single message that is sent to a very large number of recipients. Typically, this is where the recipients’ addresses are contained in one or more blind carbon copy ("bcc") header lines.

The header of a standard email message includes several lines identifying the intended recipients of the message. The "To" field identifies the primary addressee or addressees. The "carbon copy field" ("cc") designates secondary addresses, and the bcc field is used to list recipients whose names and email addresses will not appear on the copies of the message delivered to the recipients. The bcc field is useful when sending a message to a large number of people, because it reduces the size of the message header, and it protects the privacy of the recipients. It also conserves bandwidth and improves the readability of the message.
Spammers use the bcc field to conceal the fact that the message is being sent to a large number of recipients. However, filters usually detect these messages because the "to" and "cc" headers are blank.

A bulk message could also be separate but identical copies of a message that are sent to a large number of recipients. In this instance, spammers use a server called a "mail exploder" that takes an incoming message and forwards copies of the message to multiple recipients.

Usually the recipient’s personal identity and context are irrelevant because the message is equally applicable to many other potential recipients. It is usually very easy to identify mail that is written specifically for you, and mail that is generated for bulk delivery. Trivial or mechanised personalisation such as "Dear Mr Jones, we see that you are the holder of the Jones.com domain" does not make the personal identity of the recipient relevant in any way.

---

A message that differs from recipient to recipient only by details, for example, the recipient’s name, account number, blocks of random words, etc, is the same message. A message that uses different wording to express the same idea may also be considered to be the same message.42

The main problem with the term "bulk" is setting a threshold for how many copies of a message must be sent and within what time period in order for them to qualify as a bulk transmission.43 "As a rough rule of thumb, if a human makes a conscious and informed decision, on a message by message and recipient by recipient basis, that the individual message should be sent to that individual recipient, it is probably not bulk".44 However, laws and industry codes may deal with anything that is unsolicited and commercial. Therefore you can be in breach of such laws or codes by sending just one unsolicited advertisement via e-mail.

4.1.4 UCE or UBE

There are many varieties of non-commercial spam, including chain letters, joke e-mails, urban legends, virus hoaxes, religious messages, political

43 Setting a quantity threshold for messages to qualify as spam also creates an incentive for spammers to send just enough messages to stay marginally below the threshold. The United States CAN SPAM ACT solves this problem by setting a cumulative threshold of more than 100 e-mails during a 24-hour period, more than 1 000 e-mails during a 30-day period, or more than 10 000 e-mails during a 1-year period. See further Chapter 4 below.
messages, fundraising solicitations, etc. However, the majority of unsolicited bulk e-mail messages contain commercial advertisements, and most unsolicited commercial e-mails are sent in bulk. Therefore, the distinction between UBE and UCE may be somewhat academic.

4.1.5 Reasons For Defining Spam As UCE

There are several arguments that support defining spam as UCE rather than UBE. Defining spam as UCE would eliminate the problem of establishing a threshold for how many messages are required to qualify as "bulk". Non-commercial messages, particularly political and religious messages may be constitutionally protected under the right to freedom of speech. Therefore, focusing on the commercial aspect allows regulators to steer clear of the legal issues associated with other forms of speech, such as unsolicited political messages.

Regulation that is confined to commercial messages will therefore be more readily adopted globally than regulation applicable to both commercial and non-commercial messages.

It is also arguable that because spam shifts costs onto the recipient, commercial messages are particularly objectionable and should therefore be the primary focus of attention.
4.1.6 Reasons For Defining Spam As UBE

While the vast majority of spam is sent with a commercial motive, this is not an inherent feature of spam. It is important to focus on the bulk aspect of spam, rather than the commercial aspect for a number of reasons.

The primary argument for defining spam as UBE is that the commercial or non-commercial nature of an unsolicited message is independent of the harm that is caused. Spam is really only an issue because it is sent in bulk.\(^4^5\) Therefore, the sender’s motivation is largely irrelevant. It is also often the case that the UCE is not undesired, for example, where it contains product enquiries or job applications.

Examining the commerce aspect requires regulating email on what it says rather than how it is sent, and this could have constitutional implications.\(^4^6\) A restriction against all unsolicited bulk e-mail is arguably more content neutral than a rule that focuses on commercial messages. Furthermore, a definition focusing only on commercial messages has the potential of opening the floodgates to a massive increase in non-commercial spam. There are also several ways of promoting commercial causes without advertising a product for sale.

\(^{4^5}\) Non-bulk e-mail can not ever overload servers or make a significant impact on mailboxes.
\(^{4^6}\) See further Chapter 6 below.
4.1.7 Unsolicited and Bulk

Restricting all unsolicited e-mail, rather than UBE or UCE, is not a practical option. Individual, non-commercial unsolicited messages are far less objectionable than UCE or UBE, and a much stronger case can be made for constitutional protection of such messages.

Many spammers argue that not all unsolicited bulk e-mail should be condemned and restricted as spam. For example, Rich\(^47\) asks the question: "will it be considered spam when a publisher does an unsolicited email advertising of its new book, 101 ways to achieve physical fitness after your heart attack, to the e-mail addresses of people who have recently suffered a heart attack?". Spammers have also been seen to defend their spam by saying things like, "this is not spam since it is not a scam"; "this is not spam since it is a one-time mailing"; "this is not spam since we include a way to be removed", etc.

For the purposes of this paper, spam is defined as unsolicited bulk email, regardless of its content. Therefore, if the message is in bulk and it is unsolicited, it is spam. However, it should be noted that in order for an e-mail to be spam, it must be both unsolicited and bulk. An unsolicited e-mail could be a normal e-mail, for example, job enquiries, product enquiries, etc. A bulk e-mail could also be a normal email, for example, newsletters, discussion

lists, etc. It is only the combination of an e-mail being unsolicited and in bulk that classifies it as spam.

PART B : EXTENT OF THE THREAT OF SPAM

5. Introduction

"The true cost of spam is hard to quantify. While there are outrageous estimates of how many billions of dollars this pest costs the world, there is no way to measure the frustration it causes".\(^{48}\)

Before discussing possible solutions to the spam problem, it is useful to examine the major factors that contribute to the spam problem. It should be noted that these problems only arise when email is abused. A user would not get a significant quantity of e-mail without bulk e-mail abuse, and therefore their waste of time and resources would be negligible. Similarly, ISPs are only burdened by the volume of e-mail they have to process. Privacy is only invaded through the use of automated address harvesting, and this practice is only of use with bulk mailing.

6. Threat To E-mail

E-mail is an extremely important and effective means of communication and is used by millions of people on a daily basis for personal and commercial

\(^{48}\) "Drowning In Spam" This Day 23 October 2003.
purposes. However, its convenience and efficiency is being threatened by the exponential increase in the volume of spam.

According to some industry experts, spam makes up more than 50% of all e-mail traffic and is seen as a growing threat to users' confidence of the Internet.\textsuperscript{49} AOL alone blocks over 2 billion messages a day,\textsuperscript{50} and the volume of spam is increasing at an alarming rate. Spam accounted for only 8 percent of e-mail traffic in mid 2001.\textsuperscript{51} According to a report in 2003 by MessageLabs, an e-mail filtering company, "the problem has grown at a rate of more than 2 300 percent in the past year, from 2.3 percent of messages a year ago to more than 55 percent".\textsuperscript{52} Industry experts have predicted that 60 percent of e-mails will be spam by mid-2004.\textsuperscript{53}

Spam is making e-mail less useful and reliable as a channel for communication and legitimate e-commerce as valid messages are sometimes overlooked or deleted.\textsuperscript{54} It is impeding the continued growth of

\textsuperscript{52} See Uhlig "We Can't Stop E-Mail Spam, Says MP" available at http://www.telegraph.co.uk (22 July 2003).
\textsuperscript{54} See further Lemke, The Washington Times "Valid E-Mail Thrown Out With Trash" available at
the Internet, and it has the potential to destroy the value of electronic mail.\textsuperscript{55} Cost increases that result from an increase in volume may even lead many sites to discontinue supporting standard e-mail altogether.\textsuperscript{56}

Having to sort through cleverly worded spam disguised as legitimate e-mail in order to access their personal e-mail has caused many people not to use e-mail to its fullest potential. Many users find themselves so overwhelmed with unwanted e-mail that they avoid checking their e-mail as often as they would otherwise, again reducing the effectiveness of e-mail as a valuable medium of communication.

Seventy percent of e-mail users who responded to a survey by the Pew Internet & American Life Project said that spam has made their online experience unpleasant or annoying, and 25 percent said that spam has caused them to reduce their use of e-mail.\textsuperscript{57}

Spam is also an impediment to Internet access because it can clog an ISPs available bandwidth. Spam is a contributing factor in many slowdowns of


\textsuperscript{56} E-mail address harvesting by spammers has lead many people to replace "mailto" links on Web pages with Web-based response systems that conceal one or both parties' e-mail addresses.

Internet e-mail which interfere with timely receipt of wanted material. It is making the Web harder and less pleasant to use, and for new users it can be a confusing and off-putting hurdle to online communication.

The use of filters by a recipient's e-mail software can reduce some of the negative effects of spam, but filters cannot eliminate spam altogether. Filters also run the risk of filtering out legitimate e-mail.

Widespread spam has also had a significant human cost in that many users are deterred from placing postings to mailing lists or on Usenet news, for fear of having their name put on mailing lists and receiving spam. Numerous newsgroups have grown silent due to the influx of spam and the harvesting of participants' e-mail addresses. People will either post a fake address, making personal replies difficult, or will avoid posting to Usenet at all, thus depriving the fora of their input. People also avoid putting their e-mail address on their WebPages, because WebCrawlers search for e-mail addresses on behalf of spammers.

7. Privacy Concerns – How Do Spammers Get Your Address?

Technology has provided the means to easily gather the e-mail addresses of large numbers of users and to distribute information to them, quickly and at
almost no cost. "You can buy a CD-ROM with millions of e-mail addresses for next to nothing and send it out for next to nothing". The manner in which e-mail addresses and personal information are collected and handled raises significant privacy issues.

"It is not uncommon for address collectors to covertly harvest e-mail addresses from the Internet, as users visit certain sites, and buy and sell them in bulk without the knowledge or consent of the owner."

Internet marketers can get e-mail addresses when people make their email addresses public by placing advertisements, inquiring about offers or participating in newsgroups or chat-rooms, or placing their e-mail addresses on their Web site. Address lists are also created by stealing e-mail addresses from Internet mailing lists. Internet users also often unwittingly give out their e-mail addresses to companies that sell this data on to others.

---

61 This technique is referred to as "address harvesting", where e-mail addresses are obtained or "harvested" from public places such as Web sites, newsgroups, chat rooms, mailing lists, etc.
62 A particularly nasty variant of spam is sending spam to mailing lists (public or private e-mail discussion forums). Because many mailing lists limit their activity to their subscribers, spammers use automated tools to subscribe to as many mailing lists as possible, so that they can access the lists of addresses, or use the mailing list as a direct target for their attacks. See Hazen Mueller "What Is Spam?" available at http://www.spam.abuse.net/overview/whatisspam.shtml (24 October 2003).
Marketers also use software that can broadcast spam to every address within a domain.\textsuperscript{63} Certain software programmes are also able to randomly generate thousands of names and addresses.\textsuperscript{64} These are then sent out en masse in the hope of reaching a bone fide user.

8. **Illegal Or Objectionable Content And Misleading Subject Lines**

Many of the objections to spam relate to its content. Most people object to receiving e-mail containing commercial advertising, particularly those that promote fraudulent business schemes such as "get rich quick" schemes and pyramid schemes. Others are offended by spam that contains sexually explicit material or political messages. These messages may also cause embarrassment to users, and employees may be contravening their employer’s e-mail policies when they receive unsolicited messages advertising pornography services or containing racist remarks, for example.

The indiscriminate method of distribution of spam is of particular concern as it is common for minors to receive spam that is pornographic, illegal or offensive. According to a survey released by Symantec, a United States


\textsuperscript{64} This technique is referred to as "dictionary spamming". For example, agates; bgates; cgates, etc.
Internet security firm, more than 80% of children who use e-mail receive spam, or unsolicited advertising, on a daily basis.\textsuperscript{65}

Spam may also pose a security threat where it contains hostile file attachments or embedded code, such as virus spam.

Some kinds of spam are illegal in some countries. In the case of pornography, and especially child pornography,\textsuperscript{66} mere possession of such material can be enough for the recipient to attract criminal liability.

The provisions of the Films and Publications Act\textsuperscript{67} prohibit the distribution of child pornography, explicit violent sexual conduct, bestiality, explicit sexual conduct which degrades a person and which constitutes incitement to cause harm or explicit infliction of extreme violence.\textsuperscript{68} The Films and Publication Act was amended by the Film and Publications Amendment Act\textsuperscript{69} to bring Internet material within its ambit. The definition of "publication" now includes the words "any message or communication, including a visual presentation,


\textsuperscript{67} Act 65 of 1996.

\textsuperscript{68} These types of publications are classified under Schedule 1 of the Act as "XX" publications. Sub-sections 25-30 of Chapter 7 prohibit conduct in relation to publications classified as XX, including distribution, possession and exhibition.

\textsuperscript{69} Act 34 of 1999.
placed on any distributed network, including, but not confined to, the Internet”.

9. **Cost Shifting**

Many senders of spam defend it as being an extension of traditional unsolicited mail and other direct marketing practices, but spam is different in that it shifts almost all the costs of the message onto the recipients and their ISPs. This makes spam analogous to a tele-marketer calling "collect" or junk mail arriving "postage due".

The single biggest factor leading to the growth of spam is the low cost of sending such material. Unlike in traditional print media, the originator of spam often bears none or very little of the distribution costs because e-mail is considered a free feature of Internet access. Spammers face virtually no economic constraints. The incremental cost of sending a message on the Internet is essentially zero. There is therefore no disincentive (other than the ire of recipients) to sending spam to vast numbers of people.

In the normal course of advertising, a sender would weigh the expected benefits against the costs involved in order to decide how broad or narrow their target market should be. Traditional advertisers would weigh the cost against the projected revenues of the advertising campaign. In the case of spammers, however, there is no incentive to consume resources in an
efficient manner. Spammers will therefore send as many messages as possible, with no regard for the response rates or the costs borne by third parties.

Internet access in South Africa is relatively inexpensive.\textsuperscript{70} A spammer can send spam to millions of recipients without any ongoing costs other than ISP access. The cost of sending out a million emails is not significantly more than the cost of sending out a hundred.\textsuperscript{71} In 1998 IBM’s Almaden Research Centre\textsuperscript{72} estimated that it cost between $0.000082 and $0.000030 to send a single email, and data from the Global Internet Project site\textsuperscript{73} suggests that it costs spammers only 0.00032 cents to obtain one e-mail address. The result is that there is no natural limit on the amount of spam that will be transmitted, and if the spammer gets a hit rate of only one response in one thousand, his efforts will have been worthwhile.

Traditional forms of advertising have a cost to the sender that increases with volume. It costs much more to send traditional "junk mail" to one million recipients than it costs to send to only one recipient. These increasing costs

\textsuperscript{70} Free trial accounts have also been offered, for example by ABSA.
\textsuperscript{71} A spammer’s costs include finding a co-operative or naive Internet service provider, figuring out how to send spam, composing the message text, and setting up a system for receiving payment and processing orders. These costs are generally independent of the volume of messages that is sent, and therefore the spammer has an incentive to send as many messages as possible, with little regard for the response rate or the costs borne by third parties.
\textsuperscript{73} http://www.gip.org/publications/papers/spam061802.asp (4 November 2003).
force advertisers to consider their return on investment, and result in a natural limit on the volume of direct mail solicitations". 74

The necessary conclusion is that if the spammer is not paying for their advertising to be transmitted, somebody else must be paying for it. It was a deliberate design decision that all e-mail would use the resources of the recipient. The Internet was built on a shared-cost, flat-rate model with the basic contract, "I pay for my end, you pay for yours". 75

While the cost of receiving a single bulk e-mail is minimal, the cost of receiving multiple e-mails can be considerable. Although the physical cost of a single spam is insignificant, the true cost of spam as a whole comes because there is so much of it. Spam costs each recipient money, time and resources. It also places a significant physical and financial burden on the Internet system and ISPs.

9.1  The Internet Backbone

Spam sent over the Internet backbone causes delays for all Internet users. It is an impediment to Internet access because it can clog an ISPs available

---

75 Templeton "Commentary On Ad-Hoc Working Group On UCE" available at http://www.templetons.com/brad/spam/adhoc.html (10 June 2003). There were pay-to-send e-mail systems in earlier eras, such as MCI-Mail and CompuServe. These systems were discontinued because of the shared-cost, flat rate Internet cost accounting contract.
Where mailing lists have outdated addresses on them, many messages are rejected ("bounced"), causing the intended ISP to send a return response, which in turn wastes more bandwidth. Spam is also sometimes sent to maliciously interrupt services by overloading e-mail servers.

### 9.2 Internet Service Providers

Spam places a significant burden on ISPs by consuming massive amounts of network bandwidth, memory and storage space. Spam can significantly increase the processing and storage requirements of ISPs, and ISPs are forced to increase their bandwidth, memory and storage space to accommodate the increased e-mail capacity.

ISPs are also burdened by spam that is relayed through their system by spammers attempting to hide the true origin of their messages. "The messages may cause the ISPs e-mail server to crash or to slow down to such an extent that the service cannot temporarily be used or may cause delays in the delivery of all e-mail to that particular ISPs servers or may force these subscription services to temporarily stop accepting e-mail messages for delivery. This, in turn, may harm the ISPs reputation and goodwill".

---

76 The range of frequencies that they use to transmit data for their customers.
ISPs must spend time and money implementing filters\(^79\) and responding to subscriber complaints, because Internet users complain to their ISPs about spam that they receive.\(^80\) When Internet users receive too many unsolicited messages via a particular ISPs service, they terminate their subscription accounts with that ISP, resulting in lost revenue for the ISP.

Many ISPs have had to bear the additional expense of having to educate users about the nature of spam and why they are receiving it.

### 9.3 Individuals

For individual users (and employers), spam means increased download times and lost productivity. Recipients have to spend the time to read and discard the messages. They have to spend time to sort spam from wanted mail, open and read unwanted spam that is disguised as e-mail the user might want to read, etc.

The soft costs of spam most frequently cited by e-mail users are the diversion of time and loss of productivity. Even if all users do is delete spam, it still costs them time. While it does not take that long to detect and delete a

---

\(^79\) *The Star* 15 July 2003 “Are You Also Sick Of ‘Spam’?” reports that Telkom Internet, one of South Africa’s largest ISPs with more than 100 000 users, will offer its clients a free service that will not only filter spam, but will also provide free anti-virus software.

\(^80\) In *America Online Inc v IMS* (24 F. Supp. 2d 548 (E.D. Va 1998)), America Online alleged that the defendant-spammer’s actions resulted in 50 000 complaints.
single message, having to delete 20 messages every day starts to add up. This is a waste of time, and millions of users are forced to do it. AOL has said that they were receiving 1.8 million spams from Cyber Promotions per day until they got a court injunction to stop it. "Assuming it takes the typical AOL user only 10 seconds to identify and discard a message, that’s still 5 000 hours per day of connect time per day spent discarding their spam, just on AOL".81

Similarly, the time taken to respond to and unsubscribe from email lists in order to avoid future e-mails, or to report spam to an ISP, can be significant.

Spam is also a drain on business productivity and is a costly waste of time and resources as it clogs corporate networks and distracts workers. It is also sometimes a vehicle for viruses that can cause serious damage. For many users who use the Internet in business, there is an e-mail window open all the time on the screen, and e-mail is dealt with all day as it comes in. Spam interrupts these users continually, like a telephone that randomly rings with wrong numbers. Therefore, the cost of spam to a large company due to lost time and productivity is potentially very large.

---

Many users pay their Internet access providers by the amount of time they are connected or by the amount of data they download, and users with fixed-cost Internet access accounts often have to pay for the measured telephone service costs for the time connected to their Internet access providers to download the mail. Spam causes users to spend more time downloading and reading their messages, and increases the amount of data they have to download, thus causing them to stay on-line longer and incur further expense.  

The users’ ISP has to have sufficient equipment and personnel to handle all their traffic. The ISP cannot distinguish between spam traffic and legitimate messages. This means that they have to accept and process all messages, including spam: “America Online has publicly stated that about half of all the electronic mail they process is UBE. That is, half of the costs for handling electronic mail is UBE. Other large ISPs have reported that as much as 10 percent of their operating costs are related to processing UBE. The ISPs pass these costs on to their customers as higher prices.”

Users may also choose to spend the time and resources to set up filters. However, “the use of poisoners, filters and blocking software can be costly,

---

and creates an escalating cat and mouse game as spammers attempt to circumvent each new round of anti-spam software”.

10. **Unlimited Volume**

Some of the concern over spam arises because of the prospect that the volume of spam could increase exponentially in the future. To appreciate the possibility of there being an unlimited volume of spam being generated, one should consider how much paper junk mail would be distributed if paper, printing and postage were nearly free.

According to the Coalition against Unsolicited Bulk Email, Australia, if we start with the assumption that spam is a perfectly acceptable way of advertising, then every advertiser should be allowed to use it. To get an idea of how many potential advertisers there are in South Africa, every entry in Yellow Pages represents something that an individual vendor might like to advertise to as many people as they can. If spam is an acceptable advertising method, and it costs nothing, most of these advertisers would use it. This gives an indication of how many potential spam advertisements might be sent by advertisers in South Africa if spam were an acceptable method of advertising.

---


We must add an estimate for potential spam advertisements for all the other countries of the world since there is no reliable way for a spammer to know what city or country a recipient is in, and with e-commerce a customer can be anybody, anywhere in the world.

From this one can see that the amount of advertising that could be distributed is potentially unlimited. \(^{86}\)

11. Deceptive Practices

The problem with spam is not just the volume of it. Often, the problem is tracking down the perpetrators.\(^{87}\) Most filtering techniques involve filtering messages based on the name or address of the sender: "But it is inexpensive for senders to obtain new valid or forged e-mail addresses, phone numbers, post office boxes, or other identifiers that serve as pseudonyms in cyberspace. As long as their business does not rely on building a positive reputation over time, it costs bulk mailers little to repeatedly change pseudonyms, thus thwarting many filtering efforts".\(^{88}\)

---

\(^{86}\) According to the Direct Marketing Association in the United States, $36 Billion is spent each year on postal direct marketing. If this amount were used for e-mail marketing, every person in the United States would receive 13 000 messages per day. See McCurley "Deterrence Measures For Spam" available at [www.almaden.ibm.com/cs/k53/pmail/pmail.ppt](http://www.almaden.ibm.com/cs/k53/pmail/pmail.ppt) (4 November 2003).

\(^{87}\) This is one of the problems encountered by section 45 of the ECT Act. Senders are required to provide consumers with the "option to cancel", but this is rendered ineffective if the sender is able to make subsequent mailings appear to originate from a different source. See further Chapter 3 below.

Many senders of unsolicited e-mail use false return addresses, or "forged headers", which disguises the true source of the spam and makes it appear that it is coming from someone else. Spammers may also use forged headers to route spam through a reputable organisation in an attempt to entice recipients to open and respond to their messages. There are significant costs to the victims in terms of damage to commercial reputation and time and resource costs in rectifying this damage.

Spammers also use multiple e-mail addresses or disguise the routing information so that they can't be identified. When recipients try to respond, the messages often bounce back to the Access provider, clogging up the ISPs system.

Often spammers use "hit and run" spamming. These spammers get a trial account at an Internet provider for a few days, or use false information in order to open legitimate email accounts, and then use these accounts to send thousands of messages. These accounts are then closed or left dormant and the spammer repeats this process elsewhere. Their aim is to

---

89 This is also known as "spoofing" and may constitute fraud. See further Chapter 3 above for a discussion on fraud.
90 This may constitute fraud to the extent that this misrepresentation causes prejudice to the recipients or the entities from which the spam appears to have been sent. See further Chapter 3 above for a discussion on fraud.
91 Where spam causes an e-mail server to crash, this may be considered a denial of service attack, which could constitute malicious injury to property, or a cyber crime under section 86(2) of the ECT Act in so far as it constitutes an unauthorised interference with data. This form of interference is also provided for under Article 4 (Data interference) and Article 5 (System interference) of the Convention on Cybercrime.
stay one step ahead of the game to avoid companies like Hotmail tracking them down and cancelling their privileges.\textsuperscript{92}

These practices are all used to make it difficult to identify senders of allegedly fraudulent or deceptive spam.

\subsection*{12. "Opt-out" Options}

Often spam mail will not contain an "opt-out" option. However, where an "opt-out" is provided, it is not advisable to respond to the spammer to request that one’s name be removed from the mailing list. Since spam tends to generate a lot of complaints from recipients, spammers usually try to deflect these complaints by using a false return e-mail address, often combined with a false remove address.\textsuperscript{93}

The senders of spam usually generate their messages on a purely random basis. If a recipient replies, it only serves to confirm that their e-mail address is valid and active, and may result in even more unsolicited mail being received.

\textsuperscript{92} See \textit{msn.co.za} "About Junk E-Mail" available at \url{http://www.msn.co.za/antispam/about/Default.asp} (10 October 2003).

\textsuperscript{93} Section 45(1)(a) of the ECT Act has been unsuccessful in catering for a valid opt-out. It does not require that the sender provides accurate details in the opt out mechanism, and also does not require that the opt out details remain valid for a certain period of time. Further, as noted above, the "option to cancel" is also rendered ineffective if the sender is able to make subsequent mailings appear to originate from a different source. See further Chapter 3 above.
According to Howard Beales, director of the FTC’s Bureau of Consumer Protection in the United States, "We are also working on spam cases that involve claims that you can opt out, when in fact what clicking on the link to unsubscribe will do is simply verify that you have a valid e-mail address, so that you can then get lots of spam instead of a little".  

Often the return e-mail addresses used by spammers are invalid, resulting in replies being returned. Even if the spammer does receive the message, it will most likely be ignored.

13. Responses To Spam

The way in which the Internet community responds to spam can be problematic. Retaliation can go beyond the complaint stage. Some users have resorted to methods that are illegal or which break Internet "rules".

Spammers and their service providers have been subjected to flames, reputation attacks, invasions of privacy, email bombs and other denial-of-

---

95 See Howe Free On-Line Dictionary of Computing available at http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?flame (25 March 2004) defining "flame" as "An electronic mail or Usenet news message intended to insult, provoke or rebuke, or the act of sending such a message" or "To speak incessantly and/or rabidly on some relatively uninteresting subject or with a patently ridiculous attitude or with hostility towards a particular person or group of people". 
96 This practice refers to sending, or urging others to send, massive amounts of electronic mail to a single system or person, with intent to crash or spam the recipient's system". See Howe Free On-Line Dictionary of Computing available at http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?mailbomb (25 March 2004).
service attacks, and even threats of violence and property damage. "Canter & Siegel of CyberSell (the "Greatest Spammers of all Time") and Jeff Slanton (the "King of Spam"), have lived to regret such blatant abuse of net educate. In retaliation, much of their personal information has leaked onto the Internet, and their email boxes are often flamed, once to the tune of 30,000 times in one day". 97

Automated filtering and blocking techniques, blackholing of spam-friendly sites, and other responses to spam 98 also interfere with legitimate e-mail traffic.

PART C: SPAM IN THE WORKPLACE

14. Introduction

The increasing use of email as a means of mass communication exposes businesses to additional risks of liability. Careless and defamatory e-mail may cause major embarrassment or damage to the company, and may also expose individuals and the company to litigation. Categories of spam in the workplace usually include the following material: pornography, sexually offensive, other offensive (including racist and anti-Semitic jokes), trade mark offences and chain letters.

98 These technical solutions are discussed below in Chapter 7.
Businesses also face loss of productivity, confidentiality breaches and network congestion. However, the use of e-mail facilities and Internet access by employees is making it increasingly difficult for employers to police the information which employees either access or disseminate in the business environment.

"In many companies, e-mail has replaced the telephone for the purposes of casual electronic conversation and much employee communication now takes place over private or public networks, via e-mail. Employees often assume that, like telephone conversations, these communications are private and are protected from interception by the employer, yet this is not always the case". 99

Monitoring technologies make it possible for employers to monitor employee communications and activities such as e-mail, file change, etc. Blocking software products allow businesses to censor the content of incoming and outgoing e-mail and can prevent access to certain Internet Web sites. The content of a message can be scanned to determine whether it contains a set of pre-determined keywords or phrases such as "sex", "Nazi" or "credit card number". If an e-mail (or attachments thereto) contains one of these keywords or phrases the message can be blocked and/or deleted.

The question that arises is whether the employer may intercept and/or monitor the electronic communications of an employee? Some businesses may monitor employee’s e-mails as part of their overall security measures, whereas other employers monitor e-mails due to concerns about trade secret misappropriation or liability for employee defamation, harassment and other electronic abuses by employees.

Many employees feel that the monitoring of their e-mails by their employer amounts to an invasion of privacy. However, employers will usually only seek to monitor or intercept any unlawful communication, which includes breaches of statute, common law and the employee’s conditions of employment. The fundamental right to privacy of communications has to be balanced against the need for law enforcement in the information age, and the right to economic activity of the employer.

A company has a legitimate business interest in preventing inappropriate and unprofessional comments and illegal activity over its e-mail system. Companies contend that since the employee works on the company’s computer equipment during office hours at the cost of the company, and since the company can be held liable for the emails of its employees, the employee has no right to privacy regarding the e-mails.
There has been a significant amount of interest in the privacy of employee e-mail communications, and the legality of dismissals based on inappropriate or offensive e-mails. However, there is currently no South African case law or legislation which expressly deals with these issues.

15. **Constitutional Right To Privacy**

The law of privacy is well developed in South Africa. The law of privacy is part of the South African common law and the right to privacy is entrenched in the Constitution of the Republic of South Africa ("the Constitution").

Section 14 of the Constitution guarantees all employees a right to privacy. Section 14(d) states that "everyone has the right to privacy, which includes the right not to have the privacy of their communications infringed".

In *Protea Technology v Wainer* the Court identified the competing interests of the employee and the employer to be the employee’s right to privacy versus the employer’s right to economic activity. However, the employer’s right to economic activity is not expressly guaranteed in the Constitution. Employers must therefore rely on Section 22 of the Constitution, which guarantees "freedom of trade, occupation and profession".

---

100 The law of privacy is discussed more fully under Chapter 3 below.
101 Act 108 of 1996.
102 1997 (9) BCLR 1225 (W).
Employers may also look to section 36 of the Constitution, whereby the right to privacy may be limited where such limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors. This involves a balancing process "which calls for the balancing of different interests. In the balancing process, the relevant considerations will include the nature of the right that is limited, and its importance to an open and democratic society based on freedom and equality; the extent of the limitation, its efficacy, and particularly where the limitation has to be necessary, whether the desired ends could reasonably be achieved through other means less damaging to the right in question". ¹⁰³

Employees are often given access to communication tools that are owned by the company to assist them in performing their jobs efficiently. It is important for employees to understand that a company's e-mail, Internet and computer system are the property of the company and the e-mail facility has been established for the purpose of facilitating the business objectives of the employer. The company should therefore be entitled to decide the manner in which they should be used and be able to regulate their use: "Workplace e-mails are a business tool and an employer is accordingly entitled to monitor that such a tool is used for its benefit and is not abused". ¹⁰⁴

¹⁰³ Chaskalson P in S v Makwanyane 1995 (3) SA 391 (CC).
An employer must accept that reasonable personal usage of its e-mail and telephones will take place, and communications of a private nature may not be accessed by the employer. However, obscene or threatening material on a company's computer system may be accessed and an employee cannot rely on his right to privacy to block access to such information.

In order to strike a balance between employee’s personal privacy rights and the right of the employer to protect its business interests, it is essential that a comprehensive Internet and e-mail usage policy\textsuperscript{105} be put in place.

16. **The Interception and Monitoring Prohibition Act**

The Interception and Monitoring Prohibition Act\textsuperscript{106} ("the Monitoring Act"), is intended to prevent the secret and unauthorised interception and monitoring of a communication which is being transmitted by telephone or over a telecommunications line and the recordal of conversations between parties on a tape recorder without their consent.

\textsuperscript{105} Examples of clauses relating to spam that should be included in a communications facilities policy are suggested below.
The prohibition on interception and monitoring is contained in section 2(1) of the Monitoring Act. This provision states:

"No person shall-

(a) intentionally and without the knowledge or permission of the dispatcher intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line; or

(b) intentionally monitor any conversation or communication by means of a monitoring device so as to gather confidential information concerning any person, body or organisation."

Under the Monitoring Act, interception and monitoring are dealt with separately. Interception is permitted if the sender gives permission or knows about the interception. Therefore, personal employee e-mail may be intercepted if it is sent, but not if it is received.

Monitoring, on the other hand, is not permitted simply if the sender gives permission or knows about the monitoring. The Monitoring Act states that a communication between two parties cannot be monitored without a court order. Monitoring is permitted if it is not for the purpose of "gathering confidential information".

The Monitoring Act does not define a "communication" or a "conversation"; nor does it define the word "intercept". "Monitor" is defined as "the recording of conversations or communications by means of a monitoring device"; and a "monitoring device" is defined as "any instrument, device or equipment which is used or can be used, whether by itself or in combination with any other instrument, device or equipment, to listen to or record any conversation or communication". A "telecommunications line" includes "any apparatus, instrument, pole, mast, wire, pipe, pneumatic or other tube, thing or means which is or may be used for or in connection with the sending, conveying, transmitting or receiving of signs, signals, sounds, communications or other information".

The Monitoring Act was drafted at a time when there was generally not a significant amount of e-mail and Internet use, and the Act therefore does not cater directly for e-mail communications. To date there have been no reported cases that address the question whether email communications would fall within the definition of a "communication" under section 2(1) of the Monitoring Act, and it is therefore a moot point whether e-mail would be deemed to be a communication within the Monitoring Act.
17. **The Regulation of Interception of Communications and Provision of Communication-related Information Act**

The Regulation of Interception of Communications and Provision of Communication-related Information Act\(^\text{107}\) ("the Interception Act"), was assented to by the President on 30 December 2002, and published on 22 January 2003. The Interception Act is however not yet in force, and will only come into operation on a date fixed by the President in the Government Gazette.

Sections 2 and 6 of the Interception Act regulate the extent to which individuals and corporations may lawfully intercept and monitor their employee’s communications. The Interception Act therefore provides some guidance in determining whether or not a company acts lawfully when it monitors or accesses its employees’ emails or monitors the Web sites its employees browse.

17.1 **The General Prohibition Against Interception**

Section 2 of the Interception Act provides that:-

"No person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or transmission."

\(^{107}\) Act 70 of 2002.
A "communication" includes both a direct communication and an indirect communication.

"Indirect communication" means the transfer of information, including a message or any part of a message, in any form or combination of forms, by means of a telecommunication system or a postal service. Such forms of information transfer include speech, music or other sounds, data, text, visual images, signals or radio frequency spectrum.

"Direct communication" means either oral communication between two or more persons (not amounting to an indirect communication), which occurs in the immediate presence of all the persons participating in that communication; or an utterance by a person participating in an indirect communication, if the utterance is audible to another person who, at the time when the indirect communication occurs, is in the immediate presence of the person participating in the indirect communication.

A communication would therefore include an e-mail and downloading information from the Internet as indirect communications. "It must be stressed that indirect communication is the transfer of information in any form including a postal service and this will include interception and monitoring of
e-mails, telephone calls, Internet usage, telefax transmissions and ordinary post”.

The Interception Act defines "interception" as the acquisition of the contents of any communication through the use of any means, including an interception device, so as to make some or all of the contents of that communication available to a person other than the sender or recipient or intended recipient of the communication. The definition of "interception" includes the "monitoring of any such communication by means of a monitoring device; viewing, examination or inspection of the contents of any indirect communication; and diversion of any indirect communication from its intended destination to any other destination".

The operation of blocking and filtering software would therefore amount to the interception of an email since these software products are designed to examine and inspect the content of an e-mail.

Section 49(1) of the Interception Act provides that a person shall be guilty of an offence if they intentionally intercept or attempt to intercept or authorise or procure any other person to intercept or attempt to intercept, at any place in the Republic, any communication in the course of its occurrence or

---

transmission. A person found guilty of such an offence shall be liable to a fine not exceeding R2 million or to imprisonment for a period not exceeding ten years.

The Interception Act must be read together with section 86(1) of the Electronic Communications and Transactions Act 25 of 2002 ("the ECT Act"), which provides that subject to the Interception Act, a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence. Section 89(1) of the ECT Act provides that the penalty for contravening section 86(1) would be a fine or imprisonment for a period not exceeding twelve months.

Therefore, companies do not have the right to monitor and intercept employee’s e-mail, and they can be held criminally liable if they intercept and read an employee’s e-mail.

This gives effect to Article 3 of the Council of Europe Convention on Cybercrime, that states that communications of employees, whether or not for business purposes, are protected against interception:

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law,

\[109\] A person that attempts to circumvent the protections of computers from unauthorised access is usually referred to as a "hacker". See Chapter 3 below.
when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system".

17.2 Exceptions To The General Prohibition

The general prohibition on interception of communications contained in section 2 is, however, tempered by various exceptions. These include interception in terms of a court order, interception by one of the parties to the communication, interception where there is written consent of a party to the communication, and interception in connection with the carrying on of a business.

Section 4 of the Interception Act states that any person, other than a law enforcement officer, may intercept a communication if he or she is a party to that communication. However, according to Buys, the definition of "party to a communication" confirms that it refers to the natural person sending or receiving the e-mail and not the business employing such person.


The Interception Act expressly permits interception of a person's data or voice communication where such person (which could include an employee) has given his or her prior written consent to the monitoring of the usage of the telecommunications system. Section 5 provides that:

"Any person …… may intercept any communication if one of the parties to the communication has given prior consent in writing to such interception, unless such communication is intercepted by such person for purposes of committing an offence."

For these purposes, a party to a direct communication is any participant or any person to whom the direct communication is directed, whereas a party to an indirect communication is the sender or (intended) recipient.

Section 6 of the Interception Act provides for the monitoring and interception of electronic communications in connection with the carrying on of a business.

17.3 *Interception In Connection With The Carrying On Of A Business*

The business monitoring exception is useful for employers, because one of its aims is to provide employers with a lawful means of intercepting business communications without having to obtain consent from employees.
The requirements that an employer must meet in order for interception in terms of the business monitoring exception to be lawful relate to:

a) The nature and content of the intercepted communication;

b) The purpose for which the interception is effected;

c) The nature of the telecommunications system involved; and

d) The measure of control exercised over the interception process by the system controller.

Under section 6(1) and 6(2), an employer may lawfully monitor, examine and otherwise intercept employees' telephone conversations, e-mails, faxes and other forms of indirect communication in the course of the carrying on of its business provided that:

a) such communication is the means through which a transaction is entered into in the course of that business (or otherwise relates to that business or otherwise takes place in the course of the carrying on of that business);

b) such communication is intercepted for a legitimate purpose, namely to:

- establish the existence of facts;

- investigate or detect the unauthorised use of the employer’s telecommunication system; or

- secure the effective operation of the employer’s telecommunications system or as an inherent part of the effective operation of such system;
c) such communication is intercepted in the course of its transmission over a telecommunication system that is provided for use wholly or partly in connection with the business of the employer; and

d) the system controller has made all reasonable efforts to inform all individuals using the telecommunication system in advance that indirect communications transmitted through it may be intercepted, and the system controller has intercepted the communication himself or herself (or has consented to such interception).

It should be noted that the business monitoring exception only applies to indirect communications transmitted over a telecommunications system, as defined in the Telecommunications Act\(^\text{112}\) ("the Telecommunications Act"), which are intercepted during the course of transmission.

In terms of the Telecommunications Act, a telecommunication system is defined as "any system or series of telecommunications facilities or radio, optical or electromagnetic apparatus or any technical system used for the purpose of telecommunication, whether or not such telecommunication is subject to re-arrangement, composition or processes by any means in the course of the transmission or emission or reception".

\(^{112}\) Act 103 of 1996.
Therefore, e-mail and Internet usage by employees may be lawfully intercepted by an employer in the course of the carrying on of any business if all the other requirements for lawful interception in terms of the business monitoring exception have been met.

However, the business monitoring exception appears to be limited to e-mail "in the course of its transmission" through a telecommunications system. This creates the possibility that communications that are no longer being transmitted over a telecommunications line but which are statically stored in an employee’s inbox are excluded. Therefore, once the email or other message or download arrives at its destination, the business monitoring exception ceases to apply.

17.4 Scope Of The Business Monitoring Exception

It is unclear what the legislature envisaged by "in the course of the carrying on of any business". The business monitoring exception has to some extent been modelled on the United Kingdom Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations of 2000 (SI 2000 No 2699) ("the British Regulations").

---

113 See further Opperman and Goodburn "Licence To Bug Only In Exceptional Circumstances" Business Day Monday 8 March 2004.
For the purposes of the British Regulations, a communication which is relevant to a business includes a communication by means of which a transaction is entered into in the course of that business, or which otherwise relates to that business; or a communication which otherwise takes place in the course of the carrying on of that business.

The British Regulations regard the monitoring of communications so as to determine whether or not they are relevant to the employer's business as a lawful interception. Therefore, the British Regulations envisage the interception of communications transmitted on the employer's communication system for the purpose of establishing whether or not a communication relates to the business of the employer. This does not, however, give employers the right to monitor personal communications without the employee's consent.

In terms of the Interception Act, only communications that are relevant to the employer's business in the manner defined can be intercepted under the business monitoring exception. However, the Interception Act does not authorise an employer to intercept communications so as to determine whether or not they are relevant to their business. It is therefore unclear how the employer would know whether a particular communication is private or business related. This creates a potential problem in that the wrongful interception of what was erroneously thought to be a business-related
communication may result in an employer committing an offence in terms of the Interception Act.

17.5 "Legitimate Purpose" In Terms Of The Business Monitoring Exception

The "legitimate purpose" provisions of the Interception Act are aimed at balancing employees' rights to privacy with the need for business to prevent the misuse of telephones, e-mail and the Internet, as well as to protect business systems against viruses, hackers and similar threats.

"The interception of communications for the purpose of detecting hardware and software problems or errors, monitoring for viruses, attempts at hacking and other threats to the system, automated processes such as caching or load distribution, and ensuring compliance with software license agreements should qualify as measures taken "to secure … the effective operation of the system" and would arguably serve as legitimate reasons for intercepting indirect communications during the course of transmission under the business exception". 115

---

Internet and e-mail usage policies must therefore set the parameters for any expectation of privacy, and clearly define the circumstances under which interception will be lawful.\textsuperscript{116}

17.6 \textit{Consequences Of The Act}

The Interception Act does not prohibit the interception and monitoring by the employer of communications made by employees. It appears from the Act that an existing policy in force at the company and which is a term and condition of the employee's employment and which provides that the company shall monitor and intercept e-mail and Internet usage is sufficient to protect the employer from liability in terms of this Act.

However, it is arguable that where employees have given consent in writing to the monitoring and interception of the email and Internet usage, this is insufficient unless it is given specifically in terms of the Interception Act and after the date of promulgation of the Act. It could be argued that such consent was given in terms of another statute and is therefore not applicable in these circumstances. In order to attempt to avoid disputes in regard to interception and monitoring of use of the e-mail and Internet systems it would be prudent to obtain the written consent of employees in terms of the Interception Act. "What you need is a phrase which says the employer

\textsuperscript{116} Examples of clauses relating to spam that should be inserted into the Communications Facilities Policy of a company are given below. The unlawfulness of an invasion of privacy is discussed in Chapter 3 below.
reserves the right to intercept, monitor, read, filter, block and act upon any electronic communications and stored files of the employee”.  

It is submitted that companies should distribute a memorandum to employees explaining the necessity of signing a consent in favour of the employer more specifically on the basis that this practise has already been in force within the organisation and that there has in the past been a significant amount of abuse in regard to e-mail and Internet usage.

Some commentators suggest that because of section 6, such prior written permission is not necessarily required. If the other criteria of section 6 are met, employers need to take all reasonable steps to communicate to users that personal email might be monitored and intercepted. The reference to detection of unauthorised use is also extremely wide, and would include interception to determine whether spam is being sent and received.

However, section 6 seems to indicate that only business-related communications may be intercepted, and does not extend to personal e-mails. Buys is further of the view that “communications may only be intercepted without consent "in the course of its transmission over a

---

118 A precedent is suggested below.
119 Thornton “Where Legislation Stands On Personal E-mail In The Office” available at
telecommunications system”. A "telecommunications system" is defined in terms of the Telecommunications Act of 1996 and a server operated by a private business is probably not part thereof.\textsuperscript{120}

In light of the uncertainty over the application of section 6, and the substantial criminal penalties for illegal interception, it would be prudent for employers to obtain prior written consent which will allow them to lawfully intercept communications in circumstances where the business exception does not apply. Employers must put in place clear and comprehensive rules and policies relating to the use by their employees of the employer’s telecommunication system and setting the parameters for the personal use of telephones, e-mail and the Internet.

Employers should also be able to demonstrate that "reasonable efforts" were taken to inform employees that communications may be monitored and intercepted. Employees should be provided with an electronic copy of the company policy and should be informed that the company intends monitoring communications from time to time. Employers must ensure that its company policy is brought to the attention of all employees, and that it is able to demonstrate that the employees received the communication.

\textsuperscript{120} "The Use Of E-Mail Blocking Software Will Soon Be Illegal In South Africa" available at \url{http://www.legalbrief.co.za/view_1.php?artnum+11156} (16 July 2003)
17.7  *Suggested Consent Precedents*

[Insert Company Name]

In terms of the Regulation of Interception of Communications and Provision of Communication-Related Information Act, No 70 of 2002, employees are required to consent to the monitoring of their usage of the telecommunications systems of the company.

You are requested to complete the attached consent form and to return it to the Human Resources Manager.

The requirement that you should sign the consent form does not constitute a material change to your conditions of employment as the company already monitors telecommunications usage and this has become an established practice at the company. It is an operational requirement that you should consent to such monitoring and you will be aware that it is required for safety, health, ethical, reduction of risk and other reasons.

Should you have any query please contact the Human Resources Manager. Should any employee refuse to sign this form, it may become necessary to withdraw the telecommunications facilities.

Date: _________________________

Managing Director
[Insert Company name]

(the "Company")

CONSENT TO INTERCEPTION

I, the undersigned,

[insert name of employee]

hereby formally consent to my employer, [Insert Company name], intercepting or attempting to intercept, authorising or procuring any authorised employee of the Company to intercept or attempt to intercept any communication, whether direct or indirect, in the course of its occurrence or transmission issued by me by usage of the telecommunications systems of the Company. I acknowledge that the Company will seek only to monitor and intercept any unlawful communication which includes breaches of statute, common law and my conditions of employment. This consent constitutes a consent in terms of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

Date: _________________________

[Insert employee's name]

_________________________
Witness
17.8  

Communications Facilities Policy

The following examples of clauses relating to spam should be inserted into the Communications Facilities Policy of a company.

**Introduction**

Examples of clauses to be inserted in this section include:

- Employees have access to a personal computer and consequently to electronic mail, online services, the Internet and the World Wide Web.

- The use of e-mail is encouraged, as communication is made more efficient and effective, and the Internet and the World Wide Web can also be a valuable source of information. These facilities are provided to facilitate the business of the Company.

- The Company is concerned with protecting and securing information about the Company itself and its clients. The Company is also a business enterprise and therefore it needs to monitor and manage the use of the Company's resources.

- Employees should be aware that the Company may monitor employee activities. Illegal activity or activity that violates any of the Company's policies and rules may result in appropriate disciplinary action, which may lead to dismissal and/or disclosure of evidence to law enforcement officials.

- The purpose of this policy is to define the rules of conduct and behaviour of all Company employees when utilising the Internet and the Company's communication facilities.
Use of the communication facilities and services

Examples of clauses to be inserted in this section include:

- Employees are allowed access to communication facilities for bona fide Company business purposes. Such facilities may also be used for personal, non-business purposes as long as such use does not cause a significant distraction or disruption of normal work activities. Non-business communications must comply with the standards of communication set forth in this policy.

- Employees have a responsibility to use the communication facilities in a lawful and informed and responsible way and in a manner which conforms to computer network etiquette, courtesy and corporate policy.

- Employees should apply exactly the same standards of care and professionalism when using electronic communications facilities as they would apply in any other business related communications.

Prohibited conduct

Examples of misconduct to be inserted in this section include:

- use of the communications facilities for unlawful or malicious activities;

- use of defamatory, abusive or objectionable language in either public or private communication;
- activities that cause congestion and disruption of the Company's networks and systems (e.g. large e-mail attachments, chain letters or graphics);

- use of the communications facilities for communications that contain improper or unlawful statements including, but not limited to, ethnic slurs, racial epithets or anything that may be construed as harassment or disparagement of others based on race, national origin, sex, sexual orientation, age, disability or religious beliefs, or communications that contain sexually explicit or offensive images, cartoons, graphics, sound or text;

- viewing, downloading, copying, storing and/or distributing undesirable, indecent and/or obscene graphics, images, cartoons, sound or text from e-mail, the Internet, the World Wide Web or any data storing utility on the Company's computer system and/or network;

**Monitoring of communication by the Company**

- The Company, in its discretion, reserves the right to monitor usage patterns for Internet and telephonic communications and monitor and examine the contents of email messages where there are reasonable grounds for suspecting that some form of unlawful activity, breach of Company policy or abuse is taking place, or where issues, concerns, grievances or disciplinary matters have already arisen.
E-mail usage

Examples of clauses to be inserted in this section include:

- All correspondence sent over the Internet, such as email, bulletin board notes and other messages should be treated as if they are public and printed on the Company's letterhead.

- Employees should observe the same standards when sending e-mails that apply when acting for the Company in normal written communications.

Vicarious liability

- When a user accesses the Internet from the Company's network, the user's affiliation is determined from the Internet address. Thus, both the Company and the authorised user initiating a communication over the Internet may be accused as being potentially liable for any improper use.

- Vicarious liability means having indirect legal responsibility for the acts of another person. An employer may be vicariously liable for the acts of its employees, even where the employer was not at fault for any damages caused by the employee's conduct. Therefore, if a user engages in an unlawful activity through the Internet, a party could attempt to institute legal proceedings against the Company and the user jointly and severally.
Non-Compliance

- All Employees are responsible for complying with this policy. Failure to comply with the conditions of this policy may lead to appropriate disciplinary action being taken against the user concerned.

Policy updates

- The Company may in its sole discretion revise this policy. The details of any such revision will be disseminated to Employees.
- This policy will be placed on the Company's intranet for the purposes of easy access.

18. The Labour Relations Act

In terms of the Code of Good Practice contained in Schedule 8 of the Labour Relations Act,\textsuperscript{121} it is not appropriate to dismiss an employee for a first offence, except if the misconduct is serious and of such gravity that it makes a continued employment relationship intolerable. It is submitted that spam that contains certain material, for example racist or other offensive material, may warrant dismissal in circumstances where relations at the workplace could be impaired.

\textsuperscript{121} Act 66 of 1995.
19. **The Energizer Decision**

At least some of the speculation on this issue can be laid to rest by the decision in the private arbitration of *Jacqueline Bamford and 4 others and Energizer (SA) Limited* (*"Energizer"*).\(^\text{122}\) The arbitration award was handed down by the arbitrator, Advocate Roland Sutherland SC, on 2 October 2001.

The applicants were employees of Energizer, employed at its head office in Midrand. Energizer is a multinational company which conducts business in 160 countries around the world. The company manufactures batteries for electrical appliances. It operates in a highly competitive market in which the defending of market share is largely a function of marketing the brand in the public eye. The maintenance of a sound customer relationship with the buyers in the major chain stores is important in order to preserve not only shelf space, but the extent of shelf space for the product in competition with other products. Conduct by the company or conduct associated with or attributed to the company, which identifies the company with behaviour or practices seen as repugnant to broad based social mores is likely to upset these customer relationships.

Certain of Energizer's staff, including the applicants, were authorised to use the e-mail facility at the company. Over time, routine reports of the company's local and international telephone account to Energizer's Managing Director ("the MD"), reflected an unacceptably high cost. The international
bill had to be paid in dollars, and with the poor Dollar-Rand exchange rate, it was felt that this was a prudent trend to monitor. During the course of 1999 and 2000 reminders were issued to staff to be careful about over-using the telephone and e-mail systems.

A particular instance of abuse came directly to the attention of the MD when he received an e-mail, as did all other staff, emanating from one of the applicants, Ms E Oosthuizen. She forwarded a petition, originating from a political party, calling for a general protest in regard to the imposition of new rates and taxes on property. He regarded the utilisation of the company facility for this purpose as inappropriate and he sent a message requesting her to refrain from using the company systems and time to send such e-mails.

Parallel to these developments, there were concerns relating to the efficiency of the hardware and software being utilised. Ms J Bamford, one of the Applicants, who later withdrew from the arbitration, complained frequently of how slow her personal computer was performing. On a number of occasions software specialists were called in to examine it, but were bereft of explanations and achieved no improvement. The MD eventually decided to conduct an investigation into what the personal computer was being used for in an endeavour to seek an explanation of the deficiencies experienced by Bamford.

He asked the server supervisor in Singapore to furnish him with access to all the material which was stored and recorded as having been sent or received in Bamford’s email box. Because he was aware that there was a strong social bond with a fellow employee and applicant, Ms N Wollenschlaeger, he also asked for the contents of her email box. He also decided to check whether or not Oosthuizen, who had specifically to his knowledge been abusing the system with chain mails, had complied with his instruction to cease and he called for her e-mail box.

He was shocked by what he found. The volume of material ran into thousands of communications. Much of it was pornographic and involved a series of images of a sexual nature which ranged from the merely lewd to the grotesque. In addition there were multiple examples of jokes, many of which were utterly crude and tasteless running to substantial megabytes. He also found many chain letters, mainly of an inane and vacuous nature.

He took the view that the integrity of Energizer had been compromised. The reason for this was that he was appreciative of the ease with which the domain name of Energizer could be associated with the material which had been passing through cyberspace. He was offended that Energizer should be associated with what he regarded as pornography and other joke communications which were either sexist, racist or in violation of trade mark rights of major operations. This conduct was inconsistent with workplace etiquette and was a violation of policies.
Ultimately, each of the five applicants were summarily dismissed on one or more of the following charges put to them at individual disciplinary enquiries:

a) Repeated violations of company policies and procedures regarding use of the Energizer electronic mail system;

b) Repeated receipt of and onward forwarding to other Energizer staff of obscene pornographic material and jokes;

c) Violation of company procedures regarding work environment policies.

In reaching his decision in regard to the fairness of the applicants’ respective dismissals, the arbitrator considered, *inter alia*, the following issues:

a) whether there was a clearly communicated rule in the workplace which the employees would have understood to mean that they were not entitled to send chain mail or to traffic in pornography or other joke and entertainment material; and

b) whether the company had invaded the applicants’ rights to privacy in monitoring their private e-mail communications.

The arbitrator found that whilst the company’s standard policy document did not deal with e-mail communications and further did not spell out the prohibitions in respect of e-mail usage, there was quite enough in the text of that policy to indicate that the “tone” of the workplace was expressly regulated by the employer. In addition, the arbitrator held that it was not cogent to argue that the reasonable reader of the MD's email instruction to
Oosthuizen of 6 June (which was copied to all employees) could have believed that any chain mail after that date was tolerable.

In having regard to the sanction imposed on the applicants, the arbitrator found that, objectively speaking, the trafficking in chain mail and in pornography was damaging to the business of the company. The most obvious damage was in clogging up the system and running up costs. Furthermore there was a danger of the outside world becoming aware of the exchange of these messages and there was some risk of the domain name of the company being associated with such transmissions. The trade mark violations demonstrated how frivolous abuse of the company communication system creates the risk of harm. It was further objectively foreseeable that some recipients would be offended by the material distributed.

In view of the seriousness of such transgression, the arbitrator held that the sanction of dismissal was appropriate in the circumstances.

Although the matter of invasion of privacy was raised by the applicants, little was made of it during the course of the arbitration. The arbitrator found, in this regard, that a distinction had to be drawn between "personal" and "private" communications. In this regard, the arbitrator found that the communications in question were not personal in nature, and consisted entirely of material generated by anonymous third parties and distributed for
the consumption of interested parties on the Internet.\textsuperscript{123} Accordingly, the arbitrator held that the personal dignity or personal affairs of the applicants had in no way been disturbed.

Furthermore, all the information which was the subject matter of the proceedings, was derived from storage facilities in the company's own e-mail system. The arbitrator found that it can hardly be said, even in respect of genuinely "personal" communications, that individuals are entitled to deposit intimate material in their employer's storage facility and require their employer not to examine it.

Whilst this decision may be viewed as a victory for employers, the award does not give employers a license to unfettered monitoring and interception of their employees' e-mail communications. Commentators have argued that it is "an unconstitutional invasion of privacy for companies to intercept staff e-mail. A company must show it had a reasonable and justifiable reason, such as if staff abused the system by distributing illegal material or confidential company information".\textsuperscript{124}

\textsuperscript{123} It is submitted that while this test was laid down in a private arbitration, this is an excellent test that should be followed in similar cases involving spam.
\textsuperscript{124} McQuoidMason, University of Natal, Durban in the article by Anstey "Women Fired For E-Mailing 'Porn'" \textit{The Sunday Times} 21 January 2001.
The decision highlights the need for a comprehensive Internet and E-mail policy which sets out prohibited use of the employer's electronic facilities. In addition, it is critical that employers obtain employees' consent prior to intercepting and monitoring their on-line communications. Employers should ensure that employees are trained on policy compliance and advised of the risks of sending emails or browsing the Internet, both for the employer and the employee. There is little value to the employer who implements such a policy without educating its employees on these issues.

20. **Toyota South Africa**

In a similar decision, a white employee of Toyota South Africa was dismissed because he used company email facilities to send a graphic of a gorilla with the head of Zimbabwe’s President Robert Mugabe. The matter was referred to arbitration by the Commission for Conciliation, Mediation and Arbitration, where commissioner Richard Lyster upheld the dismissal saying the cartoon was racist and offensive.

21. **The United States**

In the United States there have been several court cases in which employees that were dismissed on the basis of statements made in e-mail messages

---

125 *Cronje v Toyota Manufacturing* (2001) 22 ILJ 735 (CCMA).
have sued their former employers for violating their privacy rights by intercepting their e-mail messages.\textsuperscript{126}

Current American case law\textsuperscript{127} dealing with an employee's right to privacy versus a company's legitimate business interest in investigating employee e-mail, shows that United States courts generally protect the company's interest and most courts have found that the interests of the company outweigh an employee's expectation of a right to privacy.

In a Pennsylvanian case\textsuperscript{128}, the court found that "even if the employee had a reasonable expectation of privacy as to the contents of his email over the company's e-mail system ... a reasonable person would not consider the company's interception of the communications [which the company found to be inappropriate and unprofessional] to be a highly offensive invasion of his privacy ... and the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over the e-mail system outweighs any privacy interest the employee may have in those comments". The dismissal of the employee was accordingly upheld.

\textsuperscript{126} Dirom "Employers' Rights To Monitor Employee Email Under United States Law" available at \url{http://www.murdoch.edu.au/elaw/issues/v8n4/dirom84_text.html#t47} (10 October 2004).

\textsuperscript{127} See Dirom "Employers' Rights To Monitor Employee Email Under United States Law" available at \url{http://www.murdoch.edu.au/elaw/issues/v8n4/dirom84_text.html#t47} (10 October 2004).

PART D: TYPES OF SPAM

22. Introduction

"You can spot most of these messages easily because their topics contain inflated promises, uppercase letters or multiple exclamation marks. The identities of the senders are usually camouflaged or falsified, because people sending out garbage don’t want to take responsibility for it".129

Spam takes on many forms, including advertisements for products and services, chain letters, destructive code or viruses, cartoons, scams, and other general spam that comes from paedophiles, pornographers, and other unsound sources. These will be discussed separately below.

Spelling errors in the examples included below are part of the original messages and have not been corrected.

23. Advertisements For Products And Services

As part of a study,130 Lorrie Cranor and Brian LaMacchia analysed a collection of 400 unique messages sent to the AT&T and Lucent sub-domains under study during March, April, and May 1997 and identified by e-mail administrators as spam. They classified the messages in this collection

according to the types of products or services they advertised and recorded several other characteristics of each message.

Thirty-six percent of the messages advertised money-making opportunities, including pyramid-style schemes, multi-level marketing systems, and investment opportunities. Eleven percent advertised adult entertainment, singles services, and sexually-oriented products and services. Ten percent advertised direct email marketing products and services, including bulk email services, lists of email addresses, and software for harvesting email addresses or sending out bulk mailings. Nine percent advertised informational and how-to guides. Seven percent advertised Internet services and various computer hardware and software products, office supplies and machinery, and related services. Three percent were either non-commercial messages or suspected to have been solicited by the recipient. The remaining messages advertised other products and services, including phone services, vacation packages, nutritional supplements, weight loss products, credit cards, cable de-scramblers, and online newsletters.

Only 36% of the messages contained instructions for being removed from the mailing list, and reports from e-mail administrators suggest that many of these instructions are likely faulty or deliberately misleading. Perhaps most telling about the nature of these messages was the fact that fewer than 10 percent identified the name, postal address, phone number, and e-mail address of the sender. The low percentage of identified senders and the
types of products and services being offered support the general perception among spam recipients that most spam is not coming from "legitimate businesses."

23.1 *Financial Services Advertisements*

These typically include offers for mortgage services, home loans, debt consolidation, credit monitoring services, etc. They also offer money making methods, including work from home offers, lotteries, contests, and clubs that offer some kind of financial or product incentive.

23.2 *Health Advertisements*

These include diet plans and clubs, fitness magazine subscriptions, Web sites to order health supplements, etc. The most common health advertisements contain advertisements for Viagra, etc.

23.3 *Other Merchandise And Services*

These include business supplies, printer cartridges, ink refills, business cards, electronics, software, music, cosmetics, clothing, art, etc. They also advertise insurance services, real estate services, education offers, job placement services, etc.
24. **Chain Letters**

Family members and friends often forward every e-mail they receive, resulting in an in-box overflowing with forwarded jokes, inspirational homilies, urban legends and fake virus alerts. Electronic chain mail often contains messages that promise good luck if you forward them to others and bad luck if you do not. A new marketing technique called "viral marketing" describes a technique used by marketers where individuals are recruited to forward solicitations to their acquaintances on the merchant's behalf.\(^{131}\)

Messages that urge you to forward them to everyone in your address book are usually hoaxes and are simply not true. Forwarding unsolicited messages perpetuates the problem and wastes time and bandwidth. Chain letters are forbidden on the Internet, and may result in a user's network privileges being revoked. "No big company is going to give you a gift certificate, no child is sick or missing, and there is no such thing as e-mail tracking".\(^{132}\) These hoaxes usually employ age-old marketing triggers. The dying girl touches our hearts and hits our compassion trigger. The story about a killer virus presses our fears of getting infected. Hoaxes that promise us something for nothing appeal to our greed. These hoaxes are so credible and convincing that people are willing to believe them and pass them on.


Hoax Busters\textsuperscript{133} list five signs that a message is a hoax:

a) "URGENT": The email will have a great sense of urgency. It will use multiple exclamation marks and capitalisation. The subject line will typically be something like: URGENT!!!!!! WARNING!!!!!! IMPORTANT!!!!!! VIRUS ALERT!!!!!!

b) TELL ALL YOUR FRIENDS: There will always be a request that you share this "important" warning by forwarding the message to everybody in your e-mail address book.

c) THIS ISN'T A HOAX: The body of the email will contain some form of corroboration, such as a quote from an executive of a major corporation or from a government agency official. Sometimes the message will include a sincere-sounding premise. For example: My neighbour, who works for Microsoft, just received this warning so I know it's true. He asked me to pass this along to as many people as I can. Statements such as "This is serious!" or "This is not a hoax!" can be deceiving. Just because the message says it is not a hoax does not mean that it isn't one.

d) DIRE CONSEQUENCES: The e-mail text will predict dire consequence if you don't act immediately. The message may inform you that the virus will destroy your hard drive, bring bad fortune, etc.

e) HISTORY: Look for a lot of >>>> marks in the left margin. These marks indicate that the message has been forwarded numerous times before it has reached you.

\textsuperscript{133} See \url{http://www.hoaxbusters.org} (3 March 2003).
24.1  *Sympathy Hoaxes*

Sympathy hoaxes usually describe a person that has had something terrible happen to them, such as an accident or terminal disease. These hoaxes also take the form of a plea about a lost or missing child. Most of these messages are not true and are made up by an Internet hoaxster. In rare instances these letters may have had a basis in fact. However these messages are still circulating long after that person has grown up, been cured, or has been found. The problem with sending out messages such as these is that there is no way to stop them after the problem is resolved, and they end up becoming an urban legend.\(^ {134} \)

Any reference to the Make-A-Wish Foundation donating money, for example seven cents, is a con because the Make-A-Wish Foundation does not participate in those kinds of appeals. The Foundation specialises in granting the wishes of terminally ill children.

24.2  *Petitions*

It is not possible to actually sign an e-petition. In the absence of identifying details such as physical addresses and phone numbers, the names listed on these petitions are unverifiable and easily falsified. In true chain letter fashion, the same "signatures" are replicated over and over in multiple copies of the message, and eliminating these repetitive "signatures" is impossible. It

\(^ {134} \) Urban legends are discussed below.
is, however, an easy way for spammers to come up with large lists of valid e-mail addresses.

E-petitions are self-perpetuating chain letters, and their originators have no control over them. Recipients often alter the texts at will before forwarding them, corrupting the accuracy of the information. The circulation of e-petitions can not be predicted or limited. They cannot be recalled and they cannot be stopped. Some existing e-mail petitions are still circulating years after their originators have disavowed them.

The address listed in the message usually does not exist, and completed copies of the petition are simply bounced back from the server, rendering them useless. Because of the large volume of email traffic, the originator’s ISP will usually cancel their account.

Chain letters have also proven themselves to be ineffective. The petitions are unlikely to carry much weight with anyone in authority, especially as compared to a flood of personal messages from a comparable number of individuals. These petitions have no validity at all because no signature can be checked or validated. If people want to have an impact they should rather write a real letter in their own words. Propagating chain letters is also specifically prohibited by the terms of service of most Internet service providers and users face the risk of losing their account.
The following chain letter has been distributed around the Internet, protesting against a Web site where it is suggested cats are being maltreated. In fact, the Web site is a joke.

"To anyone with love and respect for life: In New York there is a Japanese who sells bonsai-kittens". Sounds like fun huh? NOT!

These animals are squeezed into a bottle. Their urine and faeces are removed through probes. They feed them with a kind of tube. They feed them chemicals to keep their bones soft and flexible so the kittens grow into the shape of the bottle. The animals will stay their as long as they live. They can't walk or move or wash themselves. Bonsai-kittens are becoming a fashion in New York and Asia.

See this horror at: http://www.bonsaikitten.com

Please sign this email in protest against these tortures. If you receive an e-mail with over 500 names, please send a copy to: anacheca@hotmail.com. From there this protest will be sent to USA and Mexican animal protection organizations"
"Boycott" chain letters are also becoming more prevalent. There have been calls for people to boycott food companies, clothing and cosmetic companies, soft drink companies, etc. In typical chain letter fashion, these messages are filled with rumour and innuendo. They do nothing more than play on people's fears and personal prejudices.

I received the following boycott chain letter in my work inbox:

Subject: FW: Well done Oprah

HATS OFF TO OPRAH!

I'm sure many of you watched the recent taping of The Oprah Winfrey show, where her guest was Tommy Hilfiger.

On the show, she asked him if the statements about racism he was accused of saying were true.

Statements like "... if I'd known African-Americans, Hispanics, Jews and Asians would buy my clothes, I would not have made them so nice. I wish
these people would “NOT” buy my clothes as they are made for upper class white people.”

His answer to Oprah was a simple “YES”.

When Hilfiger answered in such manner, she immediately asked him to leave her show.

A suggestion:

Don't buy your next shirt or Perfume from Tommy Hilfiger.

Let's give him what he asked for: Let's not buy his clothes. Let's put him in a state where he himself will not be able to afford the ridiculous prices he puts on his clothes.

BOYCOTT HILFIGER AND PLEASE SEND THIS MESSAGE TO EVERYONE YOU KNOW

24.3 Urban Legends

An urban legend is an amusing story or anecdote, sometimes with an element of truth to it, that is so frequently retold that it becomes common knowledge.
Urban legend-like messages normally contain all of the signs of the usual "important Internet warnings of dire and imminent threats to you and your loved ones", such as:

a) a statement assuring us that the information presented is true;

b) a description of some horrible crime perpetrated against innocent victims;

and

c) a cautionary closing paragraph typed in capital letters and ending with multiple exclamation points.

These messages do not include any verifiable details, such as dates, names of cities, names of victims, names of police contacts, etc. However, warnings like these sometimes offer valid warnings, such as: keeping your eyes on your children at all times, be careful of giving rides to strangers, don't make safety judgements based solely on a person's appearance, etc.

The "Kidney Theft" spam is one of the most well known urban legends. Drugged travelers awaken in ice-filled bathtubs to discover that their kidneys have been harvested by organ thieves. The kidney harvesting story has been in circulation on the Internet since early 1997. The idea of kidney theft has appeared in the television show "Law & Order" and in several books and films, including the horror movie "Urban Legend".
The Neiman Marcus Cookie Hoax\textsuperscript{135} is another example of an urban legend that keeps doing the rounds:

"This message is sent to you with the hope you will forward it to EVERYONE you have ever even seen the e-mail address of. In the spirit of the originator, please feel free to post it anywhere and everywhere.

Okay, everyone...a true story of justice in the good old U.S. of A. Thought y'all might enjoy this; if nothing else, it shows Internet justice, if it can be called that.

My daughter & I had just finished a salad at Neiman-Marcus Cafe in Dallas & decided to have a small dessert. Because our family are such cookie lovers, we decided to try the "Neiman-Marcus Cookie". It was so excellent that I asked if they would give me the recipe and they said with a small frown, "I'm afraid not". Well, I said, would you let me buy the recipe? With a cute smile, she said, "Yes". I asked how much, and she responded, "Two fifty". I said with approval to just add it to my tab.

\textsuperscript{135} Although the cookie story is a hoax, the actual cookie recipe does exist and is available online for free from Neiman Marcus.
Thirty days later, I received my VISA statement from Neiman-Marcus and it was $285.00. I looked again and I remembered I had only spent $9.95 for two salads and about $20.00 for a scarf. As I glanced at the bottom of the statement, it said, "Cookie Recipe - $250.00". Boy, was I upset!! I called Neiman's Accounting Dept. and told them the waitress said it was "two fifty", and I did not realize she meant $250.00 for a cookie recipe.

I asked them to take back the recipe and reduce my bill and they said they were sorry, but because all the recipes were this expensive so not just everyone could duplicate any of our bakery recipes... the bill would stand.

I waited, thinking of how I could get even or even try and get any of my money back.

I just said, "Okay, you folks got my $250.00 and now I'm going to have $250.00 worth of fun". I told her that I was going to see to it that every cookie lover will have a $250.00 cookie recipe from Neiman-Marcus for nothing. She replied, "I wish you wouldn't do this". I said, "I'm sorry but this is the only way I feel I could get even", and I will.
So, here it is, and please pass it to someone else or run a few copies... I paid for it; now you can have it for free.

(Recipe may be halved.):

2 cups butter

2 tsp. Soda

5 cups blended oatmeal

2 cups brown sugar

1 8oz. Hershey Bar (grated)

2 tsp. baking powder

2 tsp. Vanilla

4 cups flour

2 cups sugar

24 oz. chocolate chips

1 tsp. Salt

4 eggs

3 cups chopped nuts (your choice)

Measure oatmeal and blend in a blender to a fine powder. Cream the butter and both sugars. Add eggs and vanilla; mix together with flour, oatmeal, salt, baking powder, and soda. Add chocolate chips,
Hershey Bar and nuts. Roll into balls and place two inches apart on a cookie sheet. Bake for 10 minutes at 375 degrees. Makes 112 cookies.

Have fun!!! This is not a joke --- this is a true story. That's it. Please, pass it along to everyone you know, single people, mailing lists, etc...

24.4 E-mail Tracking

"E-mail tracking" is an Internet myth. There is no special software that exists that can monitor the path of any message through multiple forwards by an ever-increasing number of senders to an ever-increasing number of recipients. Even if "e-mail tracking" did exist, monitoring the exponentially increasing circulation of a successful chain letter would be impossible.

Give-away hoaxes go into great detail describing the wealth that you will receive from a big company if you send their message to everyone that you know. There is no way that the company could know that you have forwarded these messages to anyone, and there is no reason why they would be willing to bankroll such a give-away. There is no method of tracking e-mail and no person or company is paying out money, or giving away gift certificates, to people who forward chain letters.
Companies such as McDonalds, Pizza Hut or AOL, do not make charitable contributions based upon strangers forwarding chain letters. And, even if they wanted to, there is no way that they can track how many people receive it. No one is collecting signatures and there is no technology that could send such information back to them.

The concept of e-mail tracking first appeared in November 1997 in the Bill Gates $1 000 giveaway hoax. A recent version of this letter reads as follows:

"Dear Friends,

Please do not take this for a junk letter. Bill Gates is sharing his fortune. If you ignore this you will repent later. Microsoft and AOL are now the largest Internet companies and in an effort to make sure that Internet Explorer remains the most widely used program, Microsoft and AOL are running an e-mail beta test.

When you forward this e-mail to friends, Microsoft can and will track it (if you are a Microsoft Windows user) for a two week time period. For every person that you forward this e-mail to, Microsoft will pay you $245.00, for every person that you sent it to that forwards it on, Microso ft will pay you $243.00 and for every third person that receives it, you will be paid $241.00."
Within two weeks, Microsoft will contact you for your address and then send you a cheque."

There are several variants of this chain letter being forwarded around the Internet. It is very similar to the "Dear YAHOO User" chain letter:

"Urgent: Please Forward!

Hello to everyone from the Hotmail Headquarters!

This is just a little test to see who is actively using their e-mail account and in effect deleting all inactive users accounts. This process will make the whole site faster and easier to use for the active users.

Now on to what to do with this e-mail. All you have to do is forward this on to at least 10 registered Hotmail users.

If you don’t forward this on within 48 hours of reading it, your account will be deactivated momentarily until you contact Hotmail Headquarters."
In February 2003 a new version of the Hotmail hoax started circulating. It includes some obvious spelling mistakes:

Dear Hotmail User,

We understand that you have previously received many messages that have stated the closing of accounts not being used within our servers. This message, however, is your final warning. Within this message is encoded a small program that will locate and debug your account when sent to fifteen other Hotmail users. If you do not send this message to fifteen Hotmail users within 24 hours of receiving this message, your account will be PERMANETLY SHUT-DOWN. When and if you send this, we hereby grant that you will no longer receive such messages as this one.

We realize that this process is becoming an annoyance, however, this is the final message you will receive from the Hotmail Announcement staff. Thank you for your time and cooperation.

Sincerely,

Calvin W. Kreantz

MSN Accounts Coordinator
25. **Destructive Codes And Viruses**

The original "Wobbler" email warned of an infected file called california.exe containing the Wobbler virus. It first appeared in 1998 and was a hoax.

This, however, is a prime example of a virus writer taking the name of a well-known virus hoax and turning it into a real virus (or "worm"). This worm will e-mail itself to up to 100 addresses in the victim's address book. It invites the recipient to read the attachment for more information, and includes an attached file. The attached file is designed to display the Wobbler hoax warning, while in the background it sends a copy of itself to users in the address book. The worm spreads as either Wobbler.txt.vbe or Wobbler.txt.jse. It is the attachment that makes this different from all of the other false e-mail virus warnings, that don't include attached files.

The Budweiser frogs screensaver is also a well-known virus hoax. In 1997 the Budweiser beer company placed a screensaver on their Web site depicting the Budweiser frogs from their advertising campaign. Shortly afterwards an e-mail began circulating warning people not to download the file:
Subject: READ IMMEDIATELY AND PASS ON!

DANGER!!!VIRUS ALERT!!!

This is a new twist. Someone is sending out a very desirable screensaver: the Budweiser Frogs. But if you download it, you will lose everything!!! Your hard drive will crash!!!

DO NOT DOWNLOAD IT UNDER ANY CIRCUMSTANCES!

It just went into circulation yesterday. Please distribute this message. This is a new, very malicious virus and not many people know about it.

This is WHAT THE SCREENSAVER OFFER WOULD LOOK LIKE!

File: BUDSAVER.EXE (24643 bytes) DL Time (28800 bps):

This information was announced yesterday morning from Microsoft. Please share it with everyone that might access the Internet.

Once again, pass this along to EVERYONE in your address book.
so that this may be stopped. AOL has said that this is a very
dangerous virus and that there is NO remedy for it at this time.

There is no known virus (or Trojan horse) which masquerades as a Budweiser Frogs screensaver. However, users should always be very cautious when downloading or using executables of unknown origin. One variant of this virus hoax mentions the Bug's Life screensaver, BUGGLST.ZIP.

Most virus hoaxes:

a) falsely claim to describe an extremely dangerous virus;

b) use pseudo-technical language to make impressive-sounding, but impossible, claims;

c) falsely claim that the report was issued or confirmed by a well-known company;

d) ask you to forward it to all your friends and colleagues.
The continued re-forwarding of these hoaxes simply wastes time and e-mail bandwidth. Where e-mails contain file attachments, they should be treated with caution as they may be infected with a virus.

26. **Cartoons**

"Frog in a blender" (Blender.exe) and "Fish in a bowl" (Fish.exe) are both harmless multimedia cartoon-style jokes that have circulated over the Internet. However, anyone can potentially infect these files with a virus, whether deliberately or accidentally. It is advisable, therefore, to delete any unsolicited executable files received via e-mail as there is always the possibility that they are infected.

27. **Scams**

One of the most common forms of spam is "scam-spam". This type of spam typically includes money and identity theft schemes. They ask for credit and personal information, or they include an offer not to sell you something, but to give you a money held in a foreign bank account.

Unfortunately, people frequently fall for these scams. However, there is no one in a foreign country that wants to give you money, and reputable businesses do not ask for credit and personal information via e-mail, especially the government.
Nigerian section 419 scams are the most popular scam spams. Users receive an e-mail from an alleged "official" representing a foreign government or agency, with an offer to transfer millions of dollars into their personal bank account. This money could be from any number of sources: the transfer of funds from over invoiced contracts, sale of crude oil at below market prices, disbursement of money from wills, contract fraud (C.O.D. of goods or services), purchase of real estate, or conversion of hard currency. Rather than return the money, they desire to transfer the money to a foreign account. The sums to be transferred average between $10,000,000 to $60,000,000 and the recipient is offered a commission of up to 30 percent for assisting in the transfer. The confidential nature of the transaction is emphasised and there are usually claims of strong ties to government officials.

Other examples of scam spam include:

a) There is a problem with your [MasterCard, Visa, etc.] account. Your personal information is needed to correct it;

b) The government has discovered a problem with your census or tax records. Your personal information is needed to correct it;

c) You have just won a lottery. Send a handling fee to receive your winnings;

d) A deposed government official in a foreign country wants to share his wealth with you. Send a handling fee to receive your money.
28. **Paedophiles and pornographers**

Spam promoting pornographic Web sites and services is also referred to as Sporn. For example, a message with the header "You've GOT to see this!!" is spam pointing to a pornography site.

**PART E : CONCLUSION**

As discussed above, spam may be defined as unsolicited bulk e-mail or more narrowly as unsolicited commercial e-mail. It is submitted that the commercial or non-commercial nature of an unsolicited message is independent of the harm that is caused, and that spam is really only an issue because it is sent in bulk. The above chapter therefore finds that a definition of spam should be based on the volume and indiscriminate nature of the e-mail, and not only on whether the communication was commercial. Therefore, a definition of bulk unsolicited e-mail is proposed.

From the discussion above, it can be seen that spam constitutes a very real threat for network administrators, businesses and individual Internet users that threatens to undermine the usefulness of e-mail. The problem with spam is that almost all of the related costs are shifted onto the recipients. This low cost of sending such material is, in turn, the single biggest factor leading to the growth of spam.

---

136 Spam containing pornographic material, or directing users to pornographic Web sites would fall under the ambit of the Films and Publications Act 65 of 1996. See further paragraph 7 of this Chapter above.
Spam also creates potential problems in the work environment. Careless and defamatory email may cause major embarrassment or damage to the company, and may also expose individuals and the company to litigation. Businesses also face loss of productivity, confidentiality breaches and network congestion. While monitoring technologies make it possible for employers to monitor employee communications, this may amount to an invasion of privacy. The above chapter discusses the privacy of employee e-mail communications, and the legality of dismissals based on inappropriate or offensive e-mails. However, there is currently no South African case law or legislation which expressly deals with these issues.

Various examples of spam are included in the above chapter, including advertisements for products and services, chain letters, destructive code or viruses, cartoons, scams, and other general spam that comes from paedophiles, pornographers, and other unsound sources. These examples serve to illustrate the various forms of messages that may be regarded as spam.
CHAPTER 3
SOUTH AFRICA

1. Introduction

This chapter examines spam in the South African context.

Part A looks at a brief history of Roman-Dutch law in South Africa and the nature and sources of South African law, including constitutional law, common law and statutory law.

Part B looks at spam under current South African law. This part focuses on the Electronic Communications and Transactions Act\(^{137}\) ("the ECT Act")\(^{138}\) and potential problems with the ECT Act in the context of spam.

Part C looks at various other areas of law that may be applicable to the problem of spam, including \textit{inter alia} the law of privacy and the law of nuisance. This section is important for the purposes of categorising spam into an area or areas of law.

Finally, Part D provides a conclusion for the present Chapter.

\(^{137}\) Act 25 of 2002.
\(^{138}\) The provisions of the ECT Act came into effect on 30 August 2002.
PART A : A BRIEF HISTORY OF SOUTH AFRICAN LAW

2. **Introduction**

This part provides an outline of how South African law has developed over the years, and gives a brief overview of Roman-Dutch law, constitutional law, common law and statutory law.

3. **Roman-Dutch Law In South Africa**

Roman law is one of the fundamental sources of South African law. Roman-Dutch law is the legal system that applied in Holland during the seventeenth and eighteenth centuries. It was the product of the fusion of medieval Dutch law, which was mainly of Germanic origin, and the Roman law of Justinian, as adopted in the "Reception".\(^{139}\)

Roman-Dutch law was introduced into South Africa when Jan van Riebeeck occupied the Cape of Good Hope in 1652 for the Dutch East India Company.\(^{140}\) From 1652 until 1795, the Cape was under the rule of the Dutch East India Company and, subject to minor local variations, the law of Holland was applied as the law of the Cape.\(^{141}\)

\(^{139}\) "The ‘Reception’ connotes the adoption of Roman law as a system in the German Reich and its feudal dependencies, of which Holland was one, during the fifteenth and sixteenth centuries". Hahlo and Kahn *The South African Legal System and Its Background* (1973) at page 485.

\(^{140}\) Known as the "Vereenigde Geoctroyeerde Oost-Indische Compagnie" or "VOC".

The British first occupied the Cape in 1795, and in 1806 the British occupation became permanent. Roman Dutch law remained the basic common law of the Cape Colony, but fresh statutes passed in the Netherlands could no longer become law at the Cape.¹⁴²

Notwithstanding the official retention of Roman Dutch law as the law of South Africa, English law had a strong influence on the law of the Cape. English civil and criminal procedure were substantially taken over, and the English law of evidence was adopted in its entirety. English mercantile law and English company law were also introduced.

References to English law became common in South Africa. The early legal training of many of the judges and advocates, and the familiarity of the profession with the English legal structure, together with the ease of reading English, the detailed reports of English decisions, the ready access to textbooks on English law, and the influence of the Privy Council Final Court of Appeal, encouraged the use of English legal rulings as persuasive material where Roman Dutch books were silent, vague or contradictory.

The Supreme Court of South Africa was established when the Union of South Africa was established in 1910. The Appellate Division of the Supreme Court had jurisdiction over the whole of South Africa and played an important role.

¹⁴² See further Du Plessis and Kok An Elementary Introduction to the Study of South
in harmonising the common law of South Africa and making it largely uniform throughout the country.

Modern South African law is unique in that it is Roman-Dutch law, modified to some extent by the influence of English law. The basis and main content of our common law has been the Roman-Dutch law of the seventeenth and eighteenth centuries and the Roman-Dutch writers have been consistently consulted by the Supreme Court.

Some doctrines of English law have been retained, but many have been eliminated in favour of Roman-Dutch law.\textsuperscript{143} Our courts are merely guided by English precedents, and are not bound by them. Our courts may also look to comparative law, especially the legal systems of the United States and the continent of Europe. However, the rules of foreign law and decisions of foreign courts are merely persuasive.

This makes South African Law unique in that we still have a living law that is able to cope with new technological developments such as the Internet and e-mail.\textsuperscript{144}

\textsuperscript{143} The Association of Law Societies of the Republic of South Africa \textit{Our Legal Heritage} (1982) at page 33.
\textsuperscript{144} This is because our law has not been codified and may still be expanded and added to by the Courts.
4. The Nature And Sources Of South African Law

4.1 Constitutional Law

In South Africa, the Constitution\textsuperscript{145} is the most important source of law. It is the supreme law of the Republic and any law which conflicts with it may be declared invalid by the judiciary. Therefore, the judiciary is empowered to declare any law and any conduct invalid to the extent that it conflicts with the Constitution.

Section 2 of the Constitution, entitled "Supremacy of Constitution", provides:

"This Constitution is the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled".

Chapter 2 of the Constitution\textsuperscript{146} enshrines the rights of all people in South Africa and affirms the democratic values of human dignity, equality and freedom. Section 7(2) provides that the state must respect, protect, promote and fulfil the rights in the Bill of Rights. In terms of section 8(1), the Bill of Rights applies to all law, and binds the legislature, the executive, the judiciary and all organs of state.


\textsuperscript{146} The Bill of Rights.
4.2 Common Law

The common law of South Africa may be defined as that part of our law which has not been enacted by Parliament, the provincial councils, the town councils or any other similar body with law-making powers.

"The common law of South Africa is the Roman-Dutch law as found in the Corpus Juris Civilis, the writings of the Roman-Dutch jurists and the placaats applicable at the Cape".\textsuperscript{147} Judicial precedents in South Africa, in the form of reported decisions of the superior courts, also form part of our common law.

In practice, South African lawyers look to reported decisions of the superior courts, current South African legal textbooks and articles in legal journals for applicable South African common law.

4.3 Statutory Law

Statutory law is the law contained in the statutes or legislation enacted by law-making bodies. Acts of Parliament that are properly enacted and promulgated are considered law in the Republic, and our courts have no power to refuse to apply the law as enacted by Parliament. Provincial councils and town councils have subordinate lawmaking powers and may

\textsuperscript{147}Du Plessis and Kok An Elementary Introduction To The Study Of South African Law(2001) 2\textsuperscript{nd} Edition page 24. These are referred to as the old authorities.
prescribe laws for their areas. These subordinate laws may, however, be declared invalid by the courts.

PART B: SPAM UNDER SOUTH AFRICAN LAW

5. Introduction

This part discusses spam under South African law, with particular reference to the ECT Act.

6. The Electronic Communications and Transactions Act

Spam is not illegal per se in South Africa. However, section 45 of the ECT Act provides for the regulation of unsolicited goods, services or communications.

The ECT Act has, as some of its objectives, to provide for the facilitation and regulation of electronic communications and transactions; ... to prevent abuse of information systems; ... and to provide for matters connected therewith.

Section 45 of the ECT Act, entitled "Unsolicited goods, services or communications", provides that:

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

Therefore, in terms of section 45 of the ECT Act, a person who sends unsolicited commercial communications must:

a) provide the consumer with the option to cancel its subscription to the mailing list;

b) identify the source from which the consumer's personal information were obtained, on the request of the consumer; and

c) not send a second unsolicited commercial communication to a person "who has advised the sender that such communications are unwelcome".
In terms of section 45 of the ECT Act, a sender of spam may be found guilty of an offence in certain circumstances, and liable on conviction to an unspecified fine, or a maximum of 12 months imprisonment.\textsuperscript{148}

Alternatively, in terms of section 49 of the ECT Act, a consumer may choose not to institute criminal proceedings against a spammer, but rather lodge a complaint with the Consumer Affairs Committee established by section 2 of the Consumer Affairs (Unfair Business Practices) Act.\textsuperscript{149}

7. **Potential Problems With Section 45 Of The ECT Act**

Many of the potential problems in relation to section 45 of the ECT Act arise from the absence of definitions.

Michalson is of the view that, "[g]iven the high cost of litigation, coupled with the fact that no organisation wants to be the subject of a “test case”, and given the enormity of the spam problem, it might be necessary for the legislature to either revisit section 45 of the ECT Act, or enact a standalone “anti-spam” law, or for the South African Law Commission to deal with the issue in the pending Privacy Act which it is currently working on".\textsuperscript{150}

\textsuperscript{148} Under section 89(1) of the ECT Act.
\textsuperscript{149} Act 71 of 1988.
\textsuperscript{150} Michalson "The Law Vs The Scourge Of Spam" available at
Although the Law Commission has released a green paper investigating what privacy legislation is required in South Africa for comment,\textsuperscript{151} it is submitted that the spam problem is serious enough to warrant comprehensive stand-alone legislation\textsuperscript{152} of its own.

7.1 \textit{Definition Of Spam}

While the ECT Act regulates "unsolicited commercial communications", this term is not defined in the Act. Section 45 of the ECT Act also only deals with "unsolicited commercial communications" and it is therefore unclear why the section is entitled "Unsolicited goods, services or communications". It may be that under the wording of the heading of section 45, the communication must promote the sale of goods or services.

7.1.1 "Unsolicited"

According to Ebersohn,\textsuperscript{153} "unsolicited communications" is defined as "communication by means of data messages". However, "communication by means of data messages" is the ECT Act's definition of "electronic communications" and not "unsolicited electronic communications".

\textsuperscript{151} The South African Law Reform Commission Issue Paper 24 (Project 124) on Data Protection and Privacy.
\textsuperscript{152} A framework for dedicated anti-spam legislation is proposed in Chapter 8 below.
It is often difficult to assess whether a communication is unsolicited, particularly where there is a prior relationship between the sender and the recipient. In general, a communication could be considered to be unsolicited if:

a) there is no prior relationship between the parties;

b) the recipient has not expressly consented to receive that communication;

or

c) the recipient has previously sought to terminate the relationship, usually by instructing the sender not to send any more communications in the future.

7.1.2 "Commercial"

It should be noted that the ECT Act only prohibits the sending of commercial spam. Sections 45(1) and 45(4) specifically state "Any person who sends unsolicited commercial communications...".

Therefore, to be covered by section 45 of the ECT Act, the message must be commercial in nature, for example offering a commercial transaction, or directing the recipient to a location where a commercial transaction can take place. Messages without any commercial content that do not contain links or directions to a commercial Web site or location are not covered by the ECT Act.
7.1.3 Bulk

The ECT Act applies to both single and bulk e-mail messages that are commercial in nature. The ECT Act makes no reference to bulk messaging, and a single unsolicited commercial electronic message could be spam. The message does not need to be sent in bulk, or received in bulk to be considered spam.

However, given that the real problem with spam lies in the volume of e-mail messages, and not their content, measures need to be put in place to deal with unsolicited bulk e-mail as well.

The difference between unsolicited bulk e-mail and unsolicited commercial e-mail is an important distinction. There are many varieties of non-commercial spam, including charitable fundraising solicitations, opinion surveys, religious messages, political advertisements, virus hoaxes and other urban legends and chain letters.

For example, a medical doctor who sends spam to millions of consumers informing them about a deadly disease, and that it can be cured, will not be contravening section 45 of the ECT Act, unless he mentions that he can

---

154 The difference between UBE and UCE is discussed under Chapter 2 above.
provide the cure.\textsuperscript{155} A message can only be commercial if the sender expects some kind of commercial interest.

The same would apply to a person who sends an unsolicited e-mail to millions of people about terrorism, his hatred of a certain religion, etc., unless it can be proved that there is some commercial interest in the sending of the e-mail message.

\textbf{7.2 Section 45 Does Not Apply To Legal Persons Or ISP's}

Section 45 only applies to "consumers", and not to legal persons.

The ECT Act defines a "consumer" as

"any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier".

Therefore, if spam is sent to legal persons, such as companies or close corporations, for example, the provisions of section 45 do not apply.

Section 45 of the ECT Act also does not protect the interests of ISP's against spammers. While consumers may request removal from a mailing list, ISP's

\textsuperscript{155} Gereda "The Truth About Spam" \textit{De Rebus} September 2003 page 51.
incur losses with every spam sent. A single ISP may carry e-mail addresses of thousands of consumers, who are required to receive at least one spam before submitting a removal request, in terms of the ECT Act. ISPs therefore carry the largest burden of the spam problem and yet have no remedies under the ECT Act.

7.3 "Opt-out"

When the ECT Act was being drafted, in the first half of 2001, spam was not the problem that it represents today, and the drafters therefore decided to follow the "opt-out" principle. The ECT Act thus aims to protect consumers by requiring that anyone sending unsolicited commercial communications must provide the consumer with the option to cancel their subscription to that mailing list.

The practical effect of the "opt-out" principle is that businesses and individuals are allowed to send (and recipients are obliged to receive) at least one unsolicited communication, provided that it contains an "opt-out" mechanism. This provision therefore only prohibits a recurrence of spam. A dedicated spammer could, therefore, theoretically use an infinite number of different addresses to send an infinite number of different spam messages without attracting the provisions of section 45.
Michalson\textsuperscript{156} makes the point that "[o]n a strict legal interpretation of sections 45(1)(a) and (b) it is a moot point as to whether the sender is statutorily obliged to provide "the option to cancel" (whether in the form of an e-mail address or a hyperlink to a Web site) in the first e-mail sent. This issue is important as the potentially innocent act of a sender (eg where the sender is negligent and simply forgets to provide the option to cancel in their first electronic communication) is now criminalized".

95\% of spam messages are designed to show a false address for the sender,\textsuperscript{157} making it difficult to track down and prosecute the perpetrator. If it is impossible to prove where the message originated from, it will be impossible to prove that the same sender has continued to send spam after being requested to stop.

It is also unclear what the "option to cancel" in section 45(1)(a) entails. Presumably, this is in the form of the provision of an e-mail address of the sender or a hyperlink to a Web site. However, section 45 does not require that the sender provides accurate details of his identity, such as his name or physical or electronic addresses. Section 45 also does not require that the opt out details remain valid for a certain period. A spammer could potentially change these details the next day and still not fall foul of section 45.

As noted in Chapter 2, in practice, a return address usually only serves to confirm the existence of a particular e-mail address, and opting out often results in more spam being sent to that address.

8. **Other Provisions Of The ECT Act**

8.1 **Enforcement Of The ECT Act**

In terms of section 45 of the ECT Act, a sender of spam may be found guilty of an offence in certain circumstances, and liable on conviction to an unspecified fine, or a maximum of 12 months imprisonment.\(^{158}\)

Alternatively, unsolicited communications may constitute an unlawful business practice which may be reported to the Consumer Affairs Committee under section 49 of the ECT Act. Therefore, in terms of section 49 of the ECT Act, a consumer may choose not to institute criminal proceedings against a spammer, but rather lodge a complaint with the Consumer Affairs Committee established by section 2 of the Consumer Affairs (Unfair Business Practices) Act.\(^{159}\)

Therefore, the only recourse offered to consumers under the ECT Act is that where a sender does not comply with a recipient's unsubscribe request, a complaint may be registered with the consumer affairs committee.

8.2 **Jurisdiction**\(^{160}\)

Section 90 of the ECT Act provides:

"A court in the Republic trying an offence in terms of this Act has jurisdiction where

(a) the offence was committed in the Republic;

(b) any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;

(c) the offence was committed by a South African citizen or a person with permanent residence in the Republic or by a person carrying on business in the Republic; or

(d) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed".

This "long-arm" provision is effective in ensuring that our courts may exercise jurisdiction over any spamming activities that occur within the Republic or where the effect of the spamming activities are felt within the Republic.

\(^{158}\) Under section 89(1) of the ECT Act.

\(^{159}\) Act 71 of 1988.

\(^{160}\) The international nature of the problem of spam and jurisdictional issues that arise are discussed under Chapter 5 below.
8.3  **Section 86(2)**

Section 86 of the ECT Act provides for "unauthorised access to, interception of or interference with data".

Forgery of message headers could be a crime under section 86(2) of the ECT Act, which makes the intentional and unauthorised interference with data "in a way which causes such data to be modified", a criminal offence.

Spam that causes an email server to crash could also be considered a denial of service attack. This could constitute a cyber crime under section 86(2) of the ECT Act insofar as it constitutes an unauthorised interference with data.

9.  **Case Law**

According to Business Day,\(^\text{161}\) The ECT Act has thus far only been used once to successfully punish a spammer with a R200 admission of guilt fine and no prosecution.

In another matter relating to spam, a company called Faxnet has used loopholes in the ECT Act to continue to spam consumers with unsolicited commercial e-mails offering potential customers a free South African fax to e-

\(^{161}\) "False Addresses Make Mockery Of Spam Law" available at
mail service. The spam includes a Web site that clients can visit for more information, as well as an address that recipients can use to unsubscribe if they do not wish to receive any further messages.\textsuperscript{162}

Faxnet initially hosted its Web site with service provider Hetzner Africa. However, as the ISP’s policy prohibited the sending of spam mail, Faxnet used an MWeb address that had not been registered to send the e-mails, which directed customers to their Web site from which they could unsubscribe. Faxnet registered an account using online registration, and then sent the mass spam from an account that did not exist.

Faxnet took advantage of the loophole in the ECT Act by providing this "opt-out" option, thereby making their spam legal. Hetzer Africa was unable to halt the spam as it was not generated via their servers and they were merely able to suspend the hosting of the Web site. Faxnet is now hosted elsewhere and is currently still sending out mass e-mails.

PART C : OTHER AREAS OF LAW

10. Introduction

While section 45 of the ECT Act specifically provides for spam, there are various other areas of law which could cast a wider net over several spamming activities.

11. The Law Of Privacy

"The right to privacy is recognised by social scientists as essential for the preservation of an individual's human dignity including his physical, psychological and spiritual well-being. Privacy, however, has been increasingly threatened by developments in technology and the mass media which are common features of modern society".  

11.1 Introduction

There is no South African legislation dealing specifically with the protection of the right to privacy. It is therefore important to evaluate the right to privacy in the light of both the common law and the Constitution.

Prior to the inception of the interim Constitution, \(^{164}\) South African common law recognised an action for the invasion of privacy. In 1996, the right to

\(^{163}\) McQuoid-Mason The Law of Privacy in South Africa (1978) at page xxxix.

privacy was entrenched in the Bill of Rights in the final Constitution.\(^{165}\) The recognition and protection of the right to privacy as a fundamental human right in the Constitution provides an indication of its importance.

McQuoid-Mason observes that while section 14 of the Constitution creates a constitutional right to privacy, this does not mean that "all previous notions of privacy will be forgotten and fall into disuse". Rather, the courts will continue to employ those common law actions which "are in harmony with the values of the Constitution".\(^{166}\)

However, the Constitutional Court\(^{167}\) has cautioned against a straightforward use of common law principles to interpret fundamental rights and their limitation.

The determination of whether an invasion of the common law right to privacy has taken place is a single inquiry. It essentially involves an assessment as to whether the invasion is unlawful.\(^{168}\) Under the Constitution, however, a two-stage analysis must be employed in deciding whether there is a violation of the right to privacy. First, the scope of the right must be assessed to determine whether law or conduct has infringed the right. Secondly, if there


\(^{167}\) In Berstein v Bester NO 1996 (2) SA 751 (CC).
has been an infringement, it must be determined whether it is justifiable under the limitation clause.\textsuperscript{169}

This section sets out the constitutional and common law right to privacy and illustrates the way in which the problem of spam may be addressed squarely under the law of privacy.

11.2 \textit{Section 14 Of The Constitution}

Section 14 of the Constitution guarantees a general right to privacy by providing that:

"Everyone has the right to privacy, which includes the right not to have

a) their person or home searched;

b) their property searched;

c) their possessions seized; or

d) the privacy of their communications infringed".

This section is made up of two parts: the first part guarantees a general right to privacy, whereas the second part protects against specific infringements of privacy.

\textsuperscript{168} The presence of a ground of justification means that an invasion of privacy is not wrongful.\textsuperscript{169} De Waal, Currie, Erasmus \textit{The Bill of Rights Handbook} (2001) 4\textsuperscript{th} Edition at page 269.
The right against searches and seizures and infringement of communications is a subordinate element of the right to privacy. Therefore, constitutional protection is only triggered when the search, seizure or interception of communication has infringed the general right to privacy. This is apparent from the wording of section 14, because the right against searches, seizures and interception of communications is placed within the parameters of the general right to privacy.

The general right to privacy, however, is not confined to protecting individuals against searches and seizures or interference with private communications. The wording of section 14, which states "everyone has the right to privacy, which includes…", indicates that the list is not intended to be exhaustive.

This was confirmed in Mistry v Interim Medical and Dental Council of South Africa, where the Court assumed that even though breach of informational privacy was not expressly mentioned in section 13 of the interim Constitution, it would be covered by the broad protection of the right to privacy guaranteed by section 13.

\[171\] 1998 (7) BCLR 880 (CC) at paragraph 14.
Devenish\textsuperscript{172} comments on the consequences of the constitutionalisation of the right to privacy:

"The constitutionalisation of this right endorses and entrenches an existing process of development and in addition creates new rights to privacy, as has occurred in other regimes where constitutionalisation has already occurred. This development has given rise to a broad classification of rights, involving substantive privacy rights, that is those protecting personal autonomy, and informational privacy rights, that is those preventing disclosures and access to information. These new rights must inevitably give rise to new actions in relation to the interests protected by both the common law and the Constitution as against both the state and other individuals. Constitutionalisation must therefore result in both an adaptation of the existing common law and a more radical transformation, so that "what once were victimless crimes are now lawful pursuits, the invasion of which creates a constitutional tort"."

The right to privacy, like most of the rights in Chapter 2, is not an absolute right, and it may be limited in terms of the limitations clause.\textsuperscript{173} In terms of section 39 of the Constitution, when interpreting the Bill of Rights, the values which underlie an open and democratic society based on human dignity, freedom and equality, should be promoted.

\textsuperscript{172} Devenish \textit{A Commentary on the South African Bill of Rights} (1999) at page147.
\textsuperscript{173} Section 36.
11.3  The Common Law Of Privacy

The common law of privacy is based on the Roman law *actio injuriarum*, which affords a general remedy for wrongs to interests of personality. The common law recognises the right to privacy as an independent personality right which the Courts consider to be part of the concept of a person’s 'dignitas'.

At common law a breach of a person’s privacy constitutes an *iniuria*. This occurs when there is an unlawful intrusion on someone’s personal privacy or an unlawful disclosure of private facts about a person.

A person’s right to privacy entails that such a person should have control over his or her information and should be able to conduct his or her personal affairs relatively free from unwanted intrusions.

According to McQuoid-Mason, “freedom from intrusions or publicity implies that the individual has control not only over who communicates with him, but also who has access to the flow of information about him”.

---

174 Potgieter and Visser *Law of Delict* 2nd Edition at page 333. See also *O’Keeffe v Argus Printing and Publishing Co Ltd and Another* 1954 (3) SA 244 (C) at 247F-249D and *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1979 (1) SA 441 (A) at 455H-456H.

175 *Financial Mail (Pty) Ltd And Others v Sage Holdings Ltd And Another* 1993 (2) SA 451 (A).

176 Neethling *Persoonlikheidsreg* at page 39 fn 329 as quoted in the South African Law Reform Commission issue paper 24 "Privacy and Data Protection".

11.4  **Natural And Juristic Persons**

It is important to note that the common law regards the right to privacy to be applicable to individuals as well as to juristic persons.\(^{178}\)

The applicability of the Bill of Rights to a juristic person is also set out in section 8(4) of the Constitution, which provides that: "A juristic person is entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of that juristic person".

Therefore, the right to privacy extends to natural and juristic persons. The implication of this is that individual users, corporate networks, and ISPs are protected by the right to privacy.

11.5  **The Delict Of Invasion Of Privacy**

It is trite that the South African law of delict is primarily based on the Roman and Roman-Dutch law principles of the *lex Aquilia* and *actio injuriarum*.\(^{179}\)

Invasion of privacy as a delict may be defined as:

"any intentional and wrongful interference with another’s right to seclusion in his private life".\(^{180}\)

\(^{178}\) See *Financial Mail (Pty) Ltd And Others v Sage Holdings Ltd And Another* 1993 (2) SA 451 (A); *Financial Mail and Motor Industry Fund Administration v Janit* 1994 (3) SA 56 (W).
Therefore, intention, wrongfulness and impairment of personality must be established for delictual liability.

The unlawfulness of an invasion of privacy is judged in light of the contemporary boni mores and the general sense of justice of the community, as perceived by the Court.\footnote{Delanga v Costa 1989 (2) SA 857 (A).} This is an objective test premised on the "current values and thinking of the community".\footnote{Financial Mail (Pty) Ltd And Others v Sage Holdings Ltd And Another 1993 (2) SA 451 (A) at 462G.}

In Roman and Roman-Dutch law *animus injuriandi* (intention to injure) was the gist of an action for *injuria*. The test for intention is subjective and is considered to be present:

(a) when an act is done by a person with the definite object of hurting another in regard to his person, dignity or reputation;

(b) when an unlawful act is done as a means of effecting another object the consequence of which act such a person is aware will be to hurt another in regard to his person, dignity or reputation.\footnote{McKerron The Law of Delict (1971) at page 10.}

Therefore, in Roman and Roman-Dutch law, *animus injuriandi* required (a) intention to injure; and (b) consciousness of wrongfulness.
11.6  Privacy and the Internet

"In every electronic communication an Internet user gives away some form of personal information. Every e-mail message contains a header with information about the sender and the recipient. Virtually every electronic transaction will involve the transfer of personal data such as credit card numbers, telephone numbers, physical addresses and e-mail addresses".\(^\text{184}\)

Technology has provided the means to easily gather the e-mail addresses of large numbers of users and to distribute information to them, quickly and at almost no cost.\(^\text{185}\) However, the manner in which email addresses and personal information are collected and handled raises significant privacy issues.\(^\text{186}\)

The ECT Act\(^\text{187}\) defines "personal information" as:

"information about an identifiable individual, including, but not limited to:- ... any identifying number, symbol or other particular assigned to the individual; the address ... of the individual; ... the name of the individual where it appears with other personal information relating to the individual...".

\(^{184}\) Buys Cyberlaw@SA (2000) at page 365.
\(^{186}\) See Chapter 2 above.
\(^{187}\) Section 1.
It is therefore submitted that an e-mail address would be considered to be personal information in terms of the ECT Act, especially where the e-mail address contains the name of the individual and other personal information relating to the individual.\textsuperscript{188}

11.7 \textit{Categories Of Invasion Of Privacy}

Burchell\textsuperscript{189} is of the view that the four categories originally suggested by Prosser\textsuperscript{190} may provide useful guidelines for the South African law of privacy. These are: intrusions, publication of private facts, presentation of persons in a false light and appropriations.

11.7.1 Intrusions

This form of invasion of privacy occurs where there is an intrusion "upon the plaintiff's physical solitude or seclusion".\textsuperscript{191} According to the old authorities, it was an \textit{injuria} to violate a person's domestic peace.\textsuperscript{192}

McQuoid-Mason\textsuperscript{193} is of the view that an action for invasion of privacy may lie where a person's peace and tranquillity in his home are disturbed by another continuously telephoning him, or persistently calling to sell him something.

\textsuperscript{188} For example, where an email address contains "the name of the individual @ the name of the company where the individual is employed".
\textsuperscript{190} Prosser \textit{Law of Torts} at page 804.
\textsuperscript{191} Prosser \textit{Law of Torts} at page 807.
\textsuperscript{192} McQuoid-Mason \textit{The Law of Privacy in South Africa} (1978) at page 153.
Neethling\textsuperscript{194} suggests that an action will also lie where a person's mental repose has been disturbed by a flood of advertisements in the mail or by telephone.

It is therefore submitted that ISP's and recipients may similarly regard spam as an unwanted intrusion. While this matter is yet to be decided in South Africa, Buys\textsuperscript{195} is of the view that our Courts, like those in America, would grant such protection.

In \textit{Cyber Promotions Inc v America Online Inc},\textsuperscript{196} the Court held that the ISP's property was not a public forum in which Cyber Promotions Inc had a right to speak.\textsuperscript{197} Further, in \textit{CompuServe Inc v Cyber Promotions Inc}\textsuperscript{198} a claim in delict was allowed on the grounds that spamming amounted to trespass on personal property without consent.\textsuperscript{199}

Spammers make use of the property of others to deliver their communications, such as the service of an ISP and the mailbox of the recipient. Buys\textsuperscript{200} asks "to what extent private property owners may exercise their common law right to determine what forms of expression are

\begin{itemize}
  \item \textsuperscript{193} McQuoid-Mason \textit{The Law of Privacy in South Africa} (1978) at page 152 – 153.
  \item \textsuperscript{194} See McQuoid-Mason \textit{The Law of Privacy in South Africa} (1978) at page 153.
  \item \textsuperscript{195} Buys \textit{Cyberlaw@SA} (2000) at page 383.
  \item \textsuperscript{196} 1996 WL 633701 (ED PA 1996).
  \item \textsuperscript{197} See Chapter 6 for a summary of this case.
  \item \textsuperscript{198} 962 F Supp 1015 (SD OH 1997). See Street and Grant \textit{Law of the Internet} (2000) at page 167 and 238 – 240 for a discussion of this case.
  \item \textsuperscript{199} See Chapter 6 for a summary of this case.
\end{itemize}
permissible on their property", and "do spammers have the right to express themselves on private property without the consent of the owner?"

11.7.2 Publication Of Private Facts

The right to privacy may be invaded by the publication of private facts. This often occurs where the spammer sends out messages containing private information about others.

The right to privacy may be also invaded by using or disclosing information stored on computer data banks. Address lists are often created by stealing e-mail addresses from Internet mailing lists. Internet users also often unwittingly give out their e-mail addresses to companies that sell databases and e-mail addresses on to others.

11.7.3 Presentation Of Persons In A False Light

An action for invasion of privacy may lie where a person is exposed to publicity which, even though it is not defamatory, places him in a false light in the public eye.

Our law protects a person's identity and any distorted or fictitious digital manipulation or unauthorised use would be actionable. For example, it is

---

200 Buys Cyberlaw@SA (2000) at page 383.
201 A mailing list would constitute a data bank containing personal information.
possible to create a new image of a person by combining separate images through digital manipulation. This manipulation could be used to portray that person in a false light.²⁰²

11.7.4 Appropriations

This form of invasion occurs where a person's image, name or likeness is appropriated without their consent. These cases may overlap with defamation and passing-off.

There is a similarity between "false light" and "appropriation" invasions of privacy in that in both instances the person is exposed to publicity by having his image, name or likeness used by another. It is the misuse of the image, name or likeness which constitutes an affront to his dignitas and entitles him to an action for invasion of privacy.²⁰³

Therefore, it may amount to an invasion of privacy where a spammer assumes the identity of persons in the recipient's address book, making the message appear to originate from someone that is known to the recipient.

²⁰² For example, the chain letter that contained a picture of President Mugabe's face
11.7.5 Legitimate Expectation Of Privacy

The general right to privacy extends to those aspects of a "person’s life in regard to which a legitimate expectation of privacy can be harboured".\(^{204}\) This requires that a person must have a subjective expectation of privacy that society accepts as objectively reasonable.\(^{205}\)

Therefore, persons cannot legitimately complain about an infringement of privacy if they have either explicitly or implicitly consented to waive their rights in this regard.\(^{206}\)

The objective aspect of privacy is problematic. In *Berstein v Bester NO*, the Constitutional Court stated that "privacy is acknowledged in the truly personal realm, but as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly".\(^{207}\)

\(^{203}\) McQuoid-Mason *The Law of Privacy in South Africa* (1978) at page 208.


\(^{205}\) Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re: Hyundai Motor Distributors (Pty) Ltd v Smit 2001 (1) SA 545 (CC). In this judgment it was held that "wherever a person has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable, the right to privacy will come into play."

\(^{206}\) See *National Media Ltd v Jooste* 1996 (3) SA 262 (A) at 271.

\(^{207}\) *Berstein v Bester NO* 1996 (2) SA 751 (CC) at paragraph 67.
In *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re: Hyundai Motor Distributors (Pty) Ltd v Smit*, the Court held that the statements in *Berstein v Bester NO* characterises the right to privacy as lying along a continuum, where the more a person inter-relates with the world, the more the right to privacy becomes attenuated. However, Langa DP held further that the right to privacy should not be understood to mean that persons no longer retain such a right in the social capacities in which they act.

The information in question must either be private in nature, or there must be a reasonable expectation that it will be kept private. It is up to the individual concerned to determine the private nature of facts relating to them. However, it is important to note that personal information is not necessarily private information. "Information which is common knowledge, readily accessible to the public, previously disclosed or intended to be made public, such as postings to public message bases or news groups, is not private information".

Therefore, where users make their e-mail addresses public by placing advertisements, inquiring about offers or participating in newsgroups or chat-rooms, or placing their email addresses on their Web site, they may not be able to complain about invasions of privacy.

---

208 2001 (1) SA 545 (CC).
209 *Berstein v Bester NO* 1996 (2) SA 751 (CC).
11.8 Remedies

There are three generally accepted remedies for common law invasions of privacy:

a) the *actio injuriarum* (sentimental damages for injured feelings);\(^{211}\)

b) the *actio legis Aquiliae* (damages for actual monetary loss);\(^{212}\) and

c) the interdict.

Constitutional remedies are concerned with the acknowledgement and enforcement of fundamental rights. In the case of an infringement of the right to privacy as a fundamental right, in terms of section 38 of the Constitution a person is entitled to approach a competent court for appropriate relief, including a declaration of rights.

11.9 Data Protection

Data protection is an aspect of safeguarding a person’s right to privacy: “It provides for the legal protection of a person (the data subject) in instances where such a person’s personal particulars (data) are being processed by another person or institution (the data user). Processing of information

\(^{210}\) Burns *Communications Law* (2001) at page 400.

\(^{211}\) It is submitted that it would be difficult to claim emotional suffering as a result of spam.

\(^{212}\) For example, where the individual or ISP is able to demonstrate that the spamming activities have caused harm to their e-mail facilities or to their network.
generally refers to the collecting, storing, using and communicating of information".  

The South African Law Reform Commission has found that "in South Africa the traditional common law principles of protecting individual privacy and identity are unable to deal effectively with the new problems in the field of privacy and data protection, and apart from the Constitution itself, there is no legislation which deals specifically and fully with data protection".

In response to this precarious position, the South African Law Reform Commission published Issue Paper 24 (Project 124) on Data Protection and Privacy ("the Issue Paper").

The Commission found that although the expression of data protection varies across different declarations and laws, all require that personal information must be:

a) obtained fairly and lawfully;

b) used only for the specified purpose for which it was originally obtained;

c) adequate, relevant and not excessive to purpose, accurate and up to date;

---

214 The ECT Act (sections 50 and 51) merely provides for voluntary adherence to data protection principles.
d) accessible to the subject;

e) kept secure; and

f) destroyed after its purpose is completed.

12. The Law Of Nuisance

12.1 Introduction

If the requirements for an invasion of privacy are not met, it may be possible to fall back on nuisance as a remedy. Privacy is an aspect of impairment of a person's dignitas, whereas nuisance relates to interference with a person's property rights.\(^{216}\)

The legal principles applicable to neighbours of land are sometimes denoted by the term "nuisance" or "oorlas". This term derives from English law and involves the repeated unreasonable use of land by one neighbour at the expense of another.\(^{217}\)

It is submitted that while the law of nuisance primarily relates to the use and enjoyment of land, this principle may be extended to the use and enjoyment


\(^{216}\) McQuoid-Mason gives the example where a person persistently telephones a person but puts down the receiver without speaking each time the person answered. Here it might be argued that it is the plaintiff's peaceful occupation of his property which is being disturbed rather than his dignitas. If the element of animus injuriandi is present, however, such conduct could be regarded as an invasion of privacy.

of all property. Therefore, the law of nuisance may be applicable where the
use and enjoyment of a person's Internet or email facilities are affected by
spamming activities.

12.2   *English Law Of Nuisance*\textsuperscript{218}

The term "nuisance" under English law initially described structures or things
which obstructed, encroached on or impeded another's possession of land or
the enjoyment of servitutal or quasi-servitutal rights over land. These
nuisances were redressed by the assize of nuisance, a species of
possessory remedy under which the obstruction or encroaching object was
ordered removed or abated.

Nuisance was gradually extended to include obstructions or interferences
with "natural" rights of property, including the right to have land supported in
its natural state and rights to natural light and pure air. Further refinements
led to the right to occupy land and domestic residence free from the
discomfort caused by foul smells, loud noise, smoke, noxious gas or similar
deleterious matter or phenomena.

Certain types of obstruction of highways and similar public facilities gave rise
to the concept of a "public" nuisance. The notion of public nuisance was

\textsuperscript{218} See further Milton "Nuisance" *Law of South Africa* (1997) First Reissue volume
19 at paragraph 180.
gradually extended to include a wide variety of activities offensive to the public health or welfare (including eavesdropping).

12.3  *Roman And Roman-Dutch Law Of Nuisance* \(^{219}\)

Roman and Roman-Dutch law recognised a number of real remedies aimed at securing full use and enjoyment of land. What in English law would be classified as a nuisance was dealt with casuistically by particular remedies for particular types of interference with proprietary rights or the public welfare.

The remedies for interferences with the rights of adjoining or neighbouring landowners included: the *actio finium regundorum* (boundary disputes and encroachments); the *actio aquae pluviae arcendae* (removal of works interfering with the natural flow of draining surface waters); the *cautio damni infecti* (a procedure for securing against anticipated harm from a ruinous or dangerous structure); the *operis novi nuntiatio* (an action for anticipated harm arising from new buildings); the *interdictum quod vi aut clam* (an action for damages for harm arising from works or structures erected with force or secretly); the *interdictum de arboribus caedendis* (removal of overhanging branches); and the *interdictum de glande legenda* (concerning the collection of fruits falling onto to neighbouring land).

Interferences with the comfort of human existence arising from the emission of smoke, smells, noise, etc. were dealt with under the actio negatoria. This real action, related to the rei vindicatio, enabled a landowner to establish that his land was free of the burden of a praedial servitude. By asserting that his land was not subject to a servitude for receiving such immissiones, the plaintiff could obtain an order prohibiting the emission.

Roman law also recognised a public interest in unobstructed passage along public highways, public places and public rivers as well as an interest in maintaining streets and roads in a safe and sanitary condition. These "public" nuisances were casuistically redressed by way of separate interdicts.

12.4 South African Law Of Nuisance

The basis of liability on the ground of nuisance in South African law remains controversial. As Van der Walt comments:

"Aan die een kant word beweer dat ons positiewe reg insake oorlas suiwer op die Engelsregtelike leerstuk van "nuisance" gebaseer is, en aan die ander kant word die Aquiliese beginsels as grondslag voorgehou. Die implicasies is dat die Suid-Afrikaanse reg in verband met oorlas enersyds deur 'n Engelsregtelike deliksvorm sui generis beheers word of andersyds deur die omvattende beginsels van Aquiliese aanspreeklikheid. Die kenmerkende van eersgenoemde
benadering is dat die aanspreeklikheid vir die vergoeding van skade nie op skuld gebaseer word nie, terwyl in laasgenoemde geval die skuld van die verweerder by uitstek as die basis van aanspreeklikheid dien."

Neighbour law does not consist of a uniform system of rules which can be traced to one basic concept: "it is rather a conglomeration of casuistic rules from the spheres of both the law of things and the law of delict. The reason for this phenomenon must be sought in the historical development of neighbour law". 221

Because of the fragmentary treatment of neighbour law in Roman and Roman-Dutch law, early case law fell back on the English law "tort of nuisance". The courts reasoned that both English as well as Roman neighbour law were based on the age-old maxim "Sic utere tuo ut alienum non laedas". 222 It was decided as far back as 1882 by the full Bench of the Eastern Districts Court in Holland v Scott 223 that the English law of nuisance was identical to that of the Roman and Roman-Dutch Law. Both Barry JP, and Shippard J, were of the view that the maxim 'Prohibitne ne quis faciat in suo quod nocere possit alieno', was common to the English, Roman and

221 See further Van der Merwe "Neighbour Law" Law of South Africa (1997) First Reissue volume 27 at paragraph 302.
222 This maxim expresses the principle that every owner must use his property in such a manner as not to injure his neighbours: Milton Acta Juridica (1969) at page 123.
223 (1882) 2 E.D.C. 307.
Roman-Dutch systems. The same principle is expressed in different terms by the maxim ‘Sic utere tuo ut alienum non laedas’.

Roman and Roman-Dutch law forms of action were applied to matters such as encroachments upon land, removal of lateral support of land and interferences with draining surface waters. However, in relation to interferences with the comfort of human existence by odour, sound, smoke and the like, the South African courts were faced with a lack of authority in Roman and Roman-Dutch law, and adopted this part of the English law of nuisance.

However, the view that the rules of neighbour law are based on the English law tort of nuisance was rejected by Appellate Division in *Regal v African Superslate (Pty) Ltd.* Steyn CJ (Van Blerk JA concurring) held that the English law of nuisance had not been imported lock, stock and barrel into our law and that it was necessary to investigate our own common law sources to arrive at the principles upon which relief on the ground of nuisance could be granted.

---

224 1963 (1) SA 102 (A).
Further, in *East London Western Districts Farmers' Association v Minister of Education and Development Aid*, Viljoen JA stated:

"Although certain principles may coincide, the English law of nuisance is not our law".

12.5 *Public And Private Nuisance*

The term "public nuisance" has been authoritatively defined as:

"A nuisance whose harmful effect is so extensive as to effect the general public at large, or at least a distinct class of persons within its field of operation".

Therefore, a public nuisance is a wrong which affects the public at large, or some considerable class of them. It is a species of criminal offence, which has been defined as "an unlawful act or omission to discharge a legal duty, which act or omission endangers the lives, safety, health, property, or comfort of the public, or by which the public are abstracted in the exercise or enjoyment of any right common to all". Public nuisances do not fall properly within the law delict, since they may expose the responsible person to civil as well as criminal proceedings.

---

225 1989 (2) SA 63 (A) at 88.
226 *Three Rivers Ratepayers Association And Others v Northern Metropolitan* 2000 (4) SA 377 (W) at 380.
A private nuisance does not affect the public generally. It is a species of civil wrong, which may be defined as "any unreasonable use of land which in injuriously affects the use or enjoyment of neighbouring land".\textsuperscript{228}

12.6 Remedies

In \textit{Rand Waterraad v Bothma en 'n Ander};\textsuperscript{229} the Court held:

"Ons burereg is 'n versameling kusie stiese sakeregtelike en intellektuele regsreëls wat in ongemaklike kategorieë saamgesnoer word. Sien, byvoorbeeld, die opmerkings van Milton (1969 \textit{Acta Juridica} op 131), te wete:

'Nevertheless the development of the remedies under consideration has, for these reasons, been fragmentary and confusing. English and Roman-Dutch principles jostle each other, sometimes influencing each other, sometimes one dominating the other. The result is, of course, considerable confusion. Some remedies are dealt with by the rules of nuisance, others are governed by the Roman-Dutch forms of action'."

The remedies available under South African law are summed up by the Court in \textit{Dorland and another v Smits};\textsuperscript{230} as follows:

"The law does not permit an owner (or occupier) of property to use it unreasonably, that is to say to the undue detriment of his or her

\textsuperscript{228} McKerron \textit{Law of Delict} (1971) 7\textsuperscript{th} Edition at page 227.
\textsuperscript{229} 1997 (3) SA 120 (O) at 133.
\textsuperscript{230} 2002 (5) SA 374 (C) at 383.
neighbour's enjoyment of the latter's own property. (Neighbour here is not confined to next door neighbour.) Such improper usage, if continuing or likely to be repeated, may be interdicted as a nuisance; if accompanied by culpa and loss, it may form the basis for an action in damages. The Law of South Africa vol 19 (First re-issue) paras 214, 218. All this is trite, and many examples are to be found in the case law and in the textbooks”.

Damage is an essential element of liability for nuisance. This may consist either of some physical injury to the plaintiff's property, or of some interference with the plaintiff in unlawful enjoyment of his property. Therefore, a plaintiff must prove damage in an action for damages or for an interdict.

An interdict is generally regarded as the most effective remedy for a nuisance. In general, damages are not recoverable in an action of nuisance unless the nuisance causes actual physical injury to the property affected by it.

Therefore, it is submitted that individual users and ISP's may rely on the law of nuisance to interdict spammers. An action for damages may also lie

---

where the individual or ISP is able to demonstrate that the spamming activities have caused harm to their e-mail facilities or to their network.  

13. Defamation

The law of defamation in South Africa is based on the *actio injuriarum*. This is a flexible remedy arising from Roman law, which afforded the right to claim damages to a person whose personality rights had been impaired intentionally by the unlawful act of another. One of those personality rights is the right to reputation or *fama*, and it is this aspect of personality rights that was protected by the law of defamation. Therefore, our common law recognises an individual’s right to *fama* as an independent personality right.

This common law right is also entrenched in section 10 of the Constitution, which provides for the right to human dignity.

The threat of defamation through spamming is very real due to the ease with which the publishing can be effected and the potentially limitless

---

232 For example, where the spamming activities have caused an e-mail server to crash.
234 A person’s *fama* or good name is the respect and status he enjoys in society.
235 See chapter 6 for a further discussion on defamation and the constitutional right to dignity.
236 See further Buys *Cyberlaw@SA* (2000) at page 333 for a discussion of defamation and the Internet in South Africa.
audience to which the spam may be sent. Therefore, the law of defamation could potentially be invoked where the spam contains defamatory material.

14. **On-line Pornography**

The Films and Publications Act\(^ {237}\) is the principal statute governing issues of on-line pornography. This Act prohibits the distribution of child pornography, explicit violent sexual conduct, bestiality, explicit sexual conduct which degrades a person and which constitutes incitement to cause harm or explicit infliction of extreme violence. These types of publications are classified under Schedule 1 of the Act as "XX" publications, and the Act\(^ {238}\) prohibits certain conduct in relation to publications classified as "XX", including distribution, possession and exhibition.

The Films and Publications Act was amended by the Films and Publications Amendment Act\(^ {239}\) to bring Internet material within its ambit. The definition of "publication" now includes the words "any message or communication, including a visual presentation, placed on any distributed network, including, but not confined to, the Internet".

---


\(^{238}\) Sub-sections 25-30 of Chapter 7.

\(^{239}\) Act 34 of 1999.
Therefore, spam containing pornographic material, or directing users to pornographic Web sites would fall under the ambit of the Films and Publications Act.

15. **Fraud**

"Fraud is the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another".\(^{240}\)

Therefore, the elements of fraud are: misrepresentation, unlawfulness, prejudice and intention.

15.1 **Misrepresentation**

The first requirement for fraud is that there must be a misrepresentation or "a perversion or distortion of the truth". Person A must represent to person B that a fact or set of facts exists which in truth does not exist.

15.2 **Prejudice**

Fraud requires a misrepresentation which causes actual prejudice or which is potentially prejudicial. Therefore, no actual prejudice is required to constitute fraud. It is sufficient if the misrepresentation is of such a nature that it may cause harm or prejudice. The test is whether the misrepresentation is such

that a reasonable person might (or could), in the ordinary course of events, be deceived.

15.3  Application To Spam

Many senders of spam use false return addresses, or "forged headers",\textsuperscript{241} which disguises the true source of the spam and makes it appear that it is coming from someone else.

The common law offence of fraud may apply where the spammer forges his e-mail address, since this misrepresentation may cause or may have the potential to cause prejudice to the recipient, or to the recipient's ISP.

The recipient is prejudiced, or potentially prejudiced, by the fact that they are induced to open and read the message because of the forged information. This wastes the recipient's time and costs them money in terms of increased download times.\textsuperscript{242}

The recipient's ISP is also prejudiced, or potentially prejudiced, where the recipient attempts to reply to the message. Because the e-mail address is forged, any reply messages will be bounced back to the recipient's ISP. This

\textsuperscript{241} This is also known as "spoofing".
\textsuperscript{242} See Chapter 2 above for cost shifting onto individuals.
process wastes the ISPs limited resources and may cause the ISPs e-mail server to slow down or crash.

The recipient's ISP is further prejudiced where the spammer has sent large amounts of forged messages to a large number of that ISPs subscribers, since this again may cause the ISPs email server to slow down or crash, and the forged headers circumvent the protections of the ISPs filters. This may also result in lost revenue for the ISP, because when Internet users receive too many unsolicited messages via a particular ISP, they are inclined to terminate their subscription accounts with that ISP.243

Spammers may also use forged headers to route spam through a reputable organisation244 in an attempt to entice recipients to open and respond to their messages. Here there is prejudice or potential prejudice to the entities from which the spam appears to have been sent, in terms of damage to commercial reputation.

Many spammers use "hit and run" spamming. These spammers use false information to get a trial account at an Internet provider for a few days, or to open legitimate e-mail accounts, and then use these accounts to send thousands of messages. These accounts are then closed or left dormant and

243 See Chapter 2 above for cost shifting onto ISPs.
244 Where a spammer spoofs his e-mail address to reflect a third party's trade mark or business name, this may also amount to passing-off or trade mark infringement.
the spammer repeats this process elsewhere. Again, The ISPs involved are prejudiced, or potentially prejudiced, by this abuse of their email accounts that were allocated on the basis of the misrepresentation.

Often the content of the spam itself is also fraudulent.\textsuperscript{245} For example spam promising miracle diet products that are not what they claim to be, and bogus financial schemes.

16. **Hacking**

A person that attempts to circumvent the protections of computers from unauthorised access is usually referred to as a "hacker".\textsuperscript{246} "This simply means that the perpetrator logs into a computer network, and gains entry to it without having the necessary authority to do so".\textsuperscript{247}

Often spammers employ practices such as hacking to gain unauthorised access into other users' computers to send spam. User address books are also often the target of hackers seeking to obtain lists of approved addresses that can be used to send spam messages to.

\textsuperscript{245} An FTC study found that an estimated two thirds of spam contain some type of false information. Delio "Breaking News: Most Spam Is Bogus" Wired News available at \url{http://www.wired.com/news/print/0,1294,58664,00.html} (22 July 2004).

\textsuperscript{246} Hacking is different to spamming in that in the case of hacking, the user plays a passive role in the accessing of their computer by the hacker. In the case of spamming, on the other hand, while there is still an intrusion, the user has played an active role in allowing access to the "unwanted visitor" by opening the message.

\textsuperscript{247} Buys *Cyberlaw*@SA (2000) at page 425.
This violates the privacy of the user concerned and is an offence in terms of section 86(1) of the ECT Act.

17. **Other laws**

Various other laws may also be applicable to spamming activities. For example, the law of advertising may be applicable since the majority of spam contains advertising in some form.\(^{248}\)

There may also be an overlap with contract law where the sending of spam constitutes a breach of contract with the spammer’s ISP. Almost all ISPs have their users agree to what they call a "terms of service" contract, which normally includes an agreement not to abuse bulk e-mail.\(^{249}\)

Spammers often use multiple e-mail addresses or disguise the routing information so that they can't be identified. When recipients try to respond, the messages often bounce back to the Access provider, clogging up the ISPs system. Where spam causes an e-mail server to crash, this may be considered a denial of service attack, which could constitute malicious injury.

---

\(^{248}\) The law of advertising is discussed above under Chapter 7: The role of the advertising industry.

\(^{249}\) For example, MWEB’s "Terms and Conditions of Use", available at [http://www.mweb.co.za/policies/subscriber_terms.asp](http://www.mweb.co.za/policies/subscriber_terms.asp) (10 October 2004) states: “You hereby agree to adhere to generally acceptable Internet and e-mail etiquette. In this regard, without being limited to the examples listed below, you agree not to … engage in any abuse of e-mail or spamming …“.
to property, or a cyber crime under section 86(2) of the ECT Act in so far as it constitutes an unauthorised interference with data.

PART D : CONCLUSION

While section 45 of the ECT Act provides for the regulation of unsolicited goods, services or communications, the above chapter identifies potential problems with this section in effectively dealing with the problem of spam.

Many of the potential problems with section 45 arise from the absence of definitions. The term "unsolicited commercial communications" is not defined, and it is not clear what constitutes an "unsolicited message". This section also applies only to commercial communications, as opposed to all unsolicited communications, and it makes no reference to bulk messaging.

Further problems are created by the fact that Section 45 applies only to "consumers", and not to legal persons or ISP’s, leaving legal persons and ISP’s without any protection.

In following the "opt-out" principle, section 45 permits the sending of unsolicited communications, provided that the message contains an "opt-out" mechanism. This merely prevents a recurrence of spam from the same address and does not make spam illegal per se.
The above chapter continues to discuss various other areas of law which may be applicable to spamming activities, including the law of privacy, the law of nuisance, defamation and fraud, and finds that there are various common law avenues that may be drawn upon to deal with the problem of spam under South African law.
"Good people do not need laws to tell them to act responsibly, while bad people will find a way around the laws." - Plato (427-347 B.C.)

1. Introduction

The expense of litigation, and the uncertain status of the law regarding spam, has led to calls for legislation specifically designed to restrict or prohibit spam. However, there does not appear to be any country at present that has enacted a total prohibition on spam.

Most legislation that seeks to regulate spam, including South Africa's Electronic Communications and Transactions Act\textsuperscript{250} ("the ECT Act"), only prohibits unsolicited commercial e-mail. In other words, it only targets commercial spam, and does not provide for a blanket prohibition of all forms of spam. This partial prohibition usually goes further to provide that a spammer can only be prosecuted if they continue sending spam after the recipient has requested that their email address be removed from the spammer's mailing list.

\textsuperscript{250} Act 25 of 2002.
Some countries, including Canada, France, Ireland, and Luxembourg have failed to offer any protection at all.

Spam is a global industry, with many "offers" originating in countries other than those of the recipients, making it harder to prosecute or legislate. The United States of America is considered to be "the spam capital of the world". "Some 140 individuals, most of whom are US-based, are responsible for roughly 90 percent of the world's spam". A recent study of spam origins by spam filtering system provider Messagecare showed that after the United States (which contributes 33 per cent of the global spam pool), Asian-Pacific nations such as China (18 per cent) and South Korea (9 per cent) were leading contributors.

Anti-spam laws should therefore be harmonised across national borders, perhaps through international trade agreements, in order to be effective against spammers who target users across the globe.

Part A weighs the benefits of "opt-in" legislation against "opt-out" legislation. It also discusses legislation prohibiting only unsolicited commercial email

---

251 By some industry estimates, spam accounts for nearly 60 percent of global email.
rather that all unsolicited bulk email. Civil and criminal remedies and ISP Acceptable Use Policies are also briefly examined.

Comparative legal approaches are discussed in Parts B to I. The focus of this comparative study is on the legislation of various countries, including the United States of America, Canada, Australia, the United Kingdom and the European Union, Japan, China and Korea. The legislation in some of these countries tends to be broader in scope than South Africa's own ECT Act, and thus the material in this chapter illustrates possible avenues for the extension of the ECT Act.

Finally, Part J provides a general conclusion for the present Chapter.

PART A : GENERAL COMMENTS

2. Introduction

This part discusses spam legislation generally. It weighs "opt-in" legislation against "opt-out" legislation, and looks briefly at whether laws should regulate only commercial e-mail or all messages that are sent in large quantities. Civil and criminal remedies are briefly explored and the role of ISP Acceptable Use Policies is discussed.
3. "Opt-In" Versus "Opt-Out"

There is concern that the United States has adopted the wrong approach to spam regulation. The European Union has issued an anti-spam directive that calls for an "opt-in" approach, which means that a sender must first obtain a user's permission before sending a message. The United States, on the other hand, have devised more advertiser-friendly legislation that places the onus on the user to stop the flow of unsolicited e-mail promotions. Until the user requests that the messages cease, a spammer may continue to send unsolicited email. This places the onus on individuals to "opt-out" of receiving unsolicited email.

Experts have warned that this could lead to the meltdown of the Internet as a communications medium, because it would effectively legitimise spamming. Anti-spam advocates say the so-called "opt-out" rule favoured by American lawmakers shields unscrupulous spammers, who can mask their identity and send emails with impunity.

The reasoning behind the "opt-out" approach is that we live in a society where communications are by default free unless a person asks for them not to be sent. If a person states no preference, in a free society, they may be approached.
It is, however, likely that most people do not wish to receive spam from strangers. In this event, the system turns into an "opt-in" system where users decide what they wish to receive.

Much of the thinking around "opt-out" provisions worldwide tends to involve benchmarking spam against regular "junk" mail. The problem with this is that with direct mail, the incremental cost of each communication provides marketers with a sufficient incentive to refrain from communicating with persons who have submitted "opt-out" requests. Marketers are also restricted from sending unsolicited non-electronic communications to consumers in other countries – whereas with e-mail, the majority of unsolicited electronic communications originate from senders in other countries.

Unsolicited and bulk e-mail do not involve an analogous incremental cost and spammers lack a similar incentive to respect "opt-out" requests. Further, e-mail "opt-out" requests are rarely effective, and often serve only to verify active addresses. Some spammers go as far as to collect and sell e-mail addresses of those who have submitted such requests.

"Opt-in" gives consumers control over where they are sent emails from, thereby increasing the likelihood of them opening the commercial emails
they receive. "Opt-in" also provides marketers with clear information on how many consumers are interested in their product.

4. **Unsolicited Bulk E-mail or Unsolicited Commercial E-mail**

The problem with laws that regulate only commercial e-mail is that they examine the content of e-mail to determine legality. It is arguable, however, that the real issue with spam is not about content. The main concern with spam relates to the method of delivery. Therefore, laws should regulate messages sent in large quantities, or in bulk.

Many people think that because most spam is commercial, and because commercial speech is less protected under the Constitution, commercial spam should be regulated. Particularly in the United States, constitutional restrictions are believed to prevent legislation restricting other types of spam. However, if there is a larger problem, of which commercial speech is just one part, you cannot go after just the commercial speech because it is less protected.

There are many varieties of non-commercial spam, including chain letters, joke e-mails, urban legends, virus hoaxes, religious messages, political messages, fundraising solicitations, etc. However, the majority of unsolicited spam...
bulk e-mail messages contain commercial advertisements, and most unsolicited commercial e-mails are sent in bulk. Therefore, the distinction between unsolicited bulk email and unsolicited commercial e-mail may be somewhat academic.

5. **Civil Remedies**

ISPs can incur significant expense as a result of spam, because their systems are frequently burdened by large volume mailings. Therefore, ISPs may seek financial compensation through civil action. The details of civil liability are governed by legislation and case law which may vary from country to country. Generally, however, civil laws that apply to damages resulting from wrongful actions or breaches of contract would apply to online activity. ISP's may also claim liability under contract law where its terms of service contracts incorporate anti-spamming conditions.²⁵⁶

Major email providers such as AOL and Hotmail have sued spammers for "trespassing" on their networks, and have managed to have some bulk e-mailers banned from their services. For consumers however, individual users generally do not have the financial resources to engage in litigation to deter spam.

²⁵⁶ For example, an ISP may include a provision in their terms of use contract stating that subscribers that are using their facilities to send spam will have civil actions instituted against them.
Although some ISPs have gained temporary relief from spam through litigation, lawsuits are time-consuming and resource-intensive. When spammers are banned from targeting a specific ISP, they are also able to easily target other ISPs.

6. **Criminal Remedies**

Laws are needed to prohibit senders from misrepresenting their identity, falsifying the subject of a message, or using automated means to gather e-mail addresses without the owners’ consent. Once the government establishes its authority with a successful prosecution of false headers or return addresses, spammers will have to choose between identifying themselves and accept massive retaliation, or risk prosecution.

While spammers are hard to track down and prosecute, if criminal penalties\(^{257}\) are imposed on those that are caught it may deter others.

7. **ISP Acceptable Use Policies**

It should be noted that many businesses may have existing agreements with their ISPs on “Acceptable Use Policies” which specify a higher level of consent than is provided for in certain spam legislation. For example, they may require express consent or require the use of double “opt-in”

\(^{257}\text{In terms of section 45 of the ECT Act, a sender of spam may be found guilty of an offence in certain circumstances, and liable on conviction to an unspecified fine, or a maximum of 12 months imprisonment, under section 89(1) of the ECT Act.}\)
methodologies for confirming consent. ISPs do this to protect their business reputation and to avoid problems with spam blocking groups on the Internet.

Spam legislation does not overrule cases where a higher standard is required in an Acceptable Use Policy. Therefore, senders should adhere to their Acceptable Use Policies to avoid difficulties with their ISP.

PART B : THE UNITED STATES OF AMERICA

8. Introduction

Most states in the United States of America have enacted some form of anti-spam legislation. However, these were overtaken by the recent enactment of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN SPAM Act").

9. The CAN SPAM Act

The CAN SPAM Act is the first Federal law in the United States that regulates spam. These Federal guidelines will clear up the confusion of more than 35 state laws dealing with spam. The CAN SPAM Act became effective on 1 January 2004 and email marketers had 120 days from that date to comply with the new law.

---

9.1 Purpose Of The Act

The CAN SPAM Act aims to curb the most egregious practices of spammers by targeting email with falsified headers, but allows e-marketers to send unsolicited commercial e-mail provided the message contains an "opt-out" mechanism, a functioning return e-mail address, a valid subject line indicating the e-mail is an advertisement and the legitimate physical address of the sender.

Anti-spam activists argue that any unsolicited marketing pitch should be banned. These groups oppose legislation like the CAN SPAM Act as it would legitimise some unsolicited e-mail. However, the intention of the legislation is to balance the rights of e-mail users with those of legitimate marketers.

9.2 Unsolicited Commercial E-mail

The Act only prohibits unsolicited commercial e-mail, and does not prohibit all spam.

The term "commercial electronic mail message" is defined\textsuperscript{260} as:

"any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)".
9.3  Predatory And Abusive Commercial E-Mail

Section 4 of the Act prohibits "predatory and abusive commercial e-mail". This section provides that it is an offence to:

a) access a protected computer\(^{261}\) without authorisation, and send multiple commercial e-mails from or through such computer;\(^{262}\)

b) use a protected computer to relay or retransmit multiple commercial e-mails, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages;\(^{263}\)

c) materially falsify header information in multiple commercial emails and intentionally initiate the transmission of such messages;\(^{264}\)

d) register, using information that materially falsifies the identity of the actual registrant, for five or more e-mail accounts or online user accounts or two or more domain names, and intentionally initiate the transmission of multiple commercial e-mails from any combination of such accounts or domain names;\(^{265}\)

\(^{260}\) In section 3(2)(A).
\(^{261}\) In terms of section 3(13), the term "protected computer" has the meaning given in section 1030(e)(2)(B) of title 18, United States Code. It refers to a government computer, a financial institution computer, and any computer "used in interstate or foreign commerce or communication". Therefore, any computer with an Internet connection is protected.
\(^{262}\) Section 4(a)(1).
\(^{263}\) Section 4(a)(2).
\(^{264}\) Section 4(a)(3).
\(^{265}\) Section 4(a)(4).
e) falsely represent oneself to be the registrant of 5 or more Internet Protocol addresses, and intentionally initiate the transmission of multiple commercial e-mails from such addresses.\footnote{Section 4(a)(5).}

9.4 \textit{Multiple Commercial E-mail}

The term "multiple" is defined\footnote{Section 4(d)(3).} as more than 100 e-mails during a 24-hour period, more than 1,000 e-mails during a 30-day period, or more than 10,000 e-mails during a 1-year period.

9.5 \textit{False Or Misleading Transmission Information}

The Act further provides that it is an offence to send a commercial e-mail to a protected computer:

a) where the header information is materially false or materially misleading;\footnote{Section 4(d)(3).} or

b) where the subject heading is likely to mislead a recipient about a material fact regarding the contents or subject matter of the message.\footnote{Section 4(d)(3).}
9.6 "Opt-out"

The CAN SPAM Act follows the "opt-out" approach. It requires e-mail users to "opt-out" of unwanted commercial e-mail, instead of requiring e-mail senders to get permission before sending.

The new law was not warmly received by consumer groups that urged Congress to follow the tougher state laws that, in some cases, required "opt-in" standards. The Coalition Against Unsolicited Commercial E-mail prefers a law requiring marketers to obtain user's permission before sending them any e-mails. It maintains that the alternative method of consumers asking marketers not to send them any more messages has not worked.

According to Hazen-Mueller,\(^{270}\) "this bill does not stop a single spam from being sent. It only makes that spam slightly more truthful. It also gives a federal stamp of approval for every legitimate marketer in the U.S. to start using unsolicited e-mail as a marketing tool".\(^{271}\)

The Act provides that it is an offence to send a commercial e-mail to a protected computer that does not contain a functioning return e-mail address.

\(^{269}\) Section 5(a)(1).
\(^{269}\) Section 5(a)(2).
\(^{270}\) Chairman of the Coalition Against Unsolicited Commercial E-Mail (CAUCE).
or other Internet-based mechanism, clearly and conspicuously displayed, that a recipient may use to submit a reply e-mail requesting not to receive future commercial e-mails from that sender. This address must remain valid for a period of at least 30 days after the transmission of the original message.

The Act further provides that it is an offence for a sender or any person acting on behalf of the sender to send a commercial email to a recipient more than 10 business days after the receipt of a request not to receive future commercial e-mails from that sender.

The legislation also prohibits the sale or other transfer of an e-mail address obtained through an "opt-out" request. This provision is designed to prevent the treatment of this class of e-mail as a confirmation of a "live" e-mail address and the sale of that information to would-be spammers.

---

272 For example an Internet link.
273 A return electronic mail address or other mechanism does not fail to satisfy this requirement if it is unexpectedly and temporarily unable to receive messages or process requests due to a technical problem beyond the control of the sender if the problem is corrected within a reasonable time period.
274 Section 5(a)(3).
275 Section 5(a)(4).
Chapter 4

9.7 Compulsory Information

All messages are required to provide the following information:\textsuperscript{277}

a) clear and conspicuous identification that the message is an advertisement or solicitation;

b) clear and conspicuous notice of the opportunity to decline to receive further commercial e-mails from the sender; and

c) a valid physical postal address of the sender.

Where commercial e-mails include sexually oriented material, this must also be indicated in the subject heading.\textsuperscript{278}

9.8 Aggravated Violations

The Act provides for certain aggravated violations relating to spam - It is an offence:

a) to send a commercial email where the email address of the recipient was obtained using an automated means\textsuperscript{279} such as address harvesting or dictionary attacks;\textsuperscript{280}

b) to use scripts or other automated means to register for multiple email accounts or online user accounts from which to transmit spam;\textsuperscript{281} and

\textsuperscript{276} Section 5(a)(4)(A)(iv).
\textsuperscript{277} Section 5(a)(5).
\textsuperscript{278} Section 5(d)(1).
\textsuperscript{279} Section 5(b)(1).
c) to relay or retransmit spam from a protected computer or computer network where access is unauthorised. 282

9.9 Penalties

Spammers face civil penalties for using automated means to register for multiple e-mail accounts from which to send unlawful unsolicited commercial e-mail, a technique commonly used by spammers to cycle rapidly through different originating addresses, making the spammers hard to track down and the unsolicited commercial e-mail they send more difficult for Internet service providers and other e-mail service providers to filter.

The Act also imposes criminal penalties for some common spamming practices such as hacking into someone’s computer to send spam, using open relays to send spam that is intended to deceive, and registering five or more e-mail accounts using false information and using those accounts to send bulk spam.

Penalties include fines, imprisonment of up to 5 years, or both. Where a person is convicted of an offence, the Court must also order forfeiture283 of any property that constitutes or is traceable to the proceeds obtained from

---

280 The techniques of address harvesting and dictionary attacks are discussed in Chapter 2 above.
281 Section 5(b)(2).
282 Section 5(b)(3).
283 Section 4(c)(1).
such offence; and any equipment, software, or other technology used or intended to be used to commit or to facilitate the commission of such offence.

Businesses knowingly promoted in spam with false or misleading header information\(^\text{284}\) are also subject to FTC penalties and enforcement remedies, regardless of whether the FTC is able to identify the spammer who initiated the e-mail.

The Act envisages fines of up to $250 per e-mail message sent, and fines of up to $2 million for certain types of spam.

9.10 \textit{Enforcement}

The Federal Trade Commission (FTC) is charged with enforcing the new law. The Act does not allow individual e-mail users to sue spammers.\(^\text{285}\) Instead, the FTC, other federal agencies, and state attorneys general can bring a civil action on behalf of Internet users.\(^\text{286}\)

\(^{284}\) Section 6.

\(^{285}\) Consumers are not likely to have the resources to bring litigation against spammers. However, in many states, pre-existing anti-spam legislation included the rights for citizens to sue spammers directly or through class-action lawsuits. Under the new federal law, US citizens no longer have those rights. See Asaravala "With This Law, You Can Spam" available at http://www.wired.com/news/business/0,1367,62020,00.html (1 April 2004).

\(^{286}\) Section 7(f).
The CAN SPAM Act is unique in that an ISP can institute civil action against spammers and recover damages of up to $1 million. A Court also has a discretion to award additional penalty damages in favour of the ISP of up to three times the damages amount.

9.11 Exemptions

The CAN SPAM Act does not prohibit unsolicited email sent by political, religious or non-profit groups.

9.12 The Federal Trade Commission

The FTC is required to report back to Congress within two years on the effectiveness of the law and the need, if any, for modifications.

The agency also has nine months to draft suggestions for the implementation of a system to grant a reward of not less than 20 percent of the total civil penalty for the first person to report the identity of a spammer violating the Act, as a type of bounty plan.

Within 18 months of enactment, the FTC is required to produce a report on possible mandated subject line labelling, such as ADV for advertising. As

---

287 Section 7(g).
288 It would be useful to include this aspect in South African legislation to ensure that the legislation is keeping up with this rapidly changing technology. See Chapter 8 below.
currently drafted, the Can Spam Act requires spam to carry information identifying it as an advertisement or solicitation but does not mandate any specific language.

9.13  "Do not spam" List

The CAN SPAM Act requires the Federal Trade Commission to consider a national "do-not-spam" list of e-mail addresses,\textsuperscript{289} similar to the FTC's popular do-not-call registry. The FTC has subsequently reported that a "do-not-spam" list "would fail to reduce the amount of spam consumers receive, might increase it, and could not be enforced effectively".\textsuperscript{290}

Reservations have been expressed about the registry because almost all spammers are already violating various laws. While most telemarketers are legitimate businesses, most spammers are not legitimate, and therefore the attractiveness of a "do-not-spam" registry is questionable. In the telemarketing industry, organisations can be traced through telephone records, whereas the e-mail marketing industry can hide behind false e-mail addresses. It would therefore be difficult to trace marketers that abuse the list.

\textsuperscript{289} The FTC was given six months after the enactment of the bill to propose a plan for creating the e-mail registry or alternatively to explain to Congress why the creation of such a list is not currently feasible.

It would also be difficult to prevent the "do-not-spam" list from itself becoming a spam list. Although the FTC would protect the master list from falling into the wrong hands, a national "do-not-spam" list would be an attractive target for unscrupulous marketers. The FTC could use encryption to ensure that the e-mail marketers are able to abide by the terms of the registry without actually seeing the e-mail addresses it contains, but spammers could find ways around this protection.

9.14 Potential Problems With The CAN SPAM Act

Some experts have expressed concerns that the CAN SPAM Act is likely to fail and may actually increase the amount of spam. Concerns have been raised that the CAN SPAM Act will create a safe haven for e-mail marketers willing to follow certain rules for spamming. By effectively legalising spam, the law could open the floodgates to unwanted mail. Any spam that is stopped could be replaced by a deluge of "legitimate" offers now legalised by the law. Marketers will be permitted to send as many e-mail solicitations as they wish, provided the messages include accurate "from" addresses, truthful subject lines and clear "unsubscribe" links.

291 FTC Chairman Timothy Muris cited the possibility of spammers using the registry as a free list of e-mail addresses to add to their databases as the chief obstacle in its implementation. See Asaravala "FTC Says No To Antispam Registry" Wired News available at http://www.wired.com/news/print/0,1294,63862,00.html (1 October 2004).

The CAN SPAM Act also does not prevent United States based spammers from moving their operations off-shore and continuing to operate off-shore.

10. **Case Law**

On 28 April 2004, in a landmark case in Detroit, Federal authorities filed the first criminal charges under the new CAN SPAM Act. The defendants were accused of disguising their identities in hundreds of thousands of sales pitches for fraudulent weight-loss products and delivering e-mails by bouncing messages through unprotected relay computers on the Internet. Since 1 January 2004, consumers have complained to the FTC about 490,000 spam messages linked to Phoenix Avatar.

Their company sold a weight-loss patch under the corporate names AIT Herbal, Avatar Nutrition, Phoenix Avatar and others. Consumers who wanted to purchase the products clicked on a hyperlink in the message and were connected to one of the defendants’ many Web sites. The defendants were allegedly earning nearly $100,000 per month from product sales. The FTC alleges that the claims made for these diet patches are false and that the patches, which sell for $59.95, will have no effect at all.

---


294 Consumers forward unwanted spam e-mail to the FTC, which maintains them in a database.
The spammers hoped to obscure their identities by using innocent third party e-mail addresses in the "reply-to" or "from" fields of their spam\(^{295}\). When spam was undeliverable and bounced back, tens of thousands of undelivered e-mails bounced to unwitting third parties. The spam also did not offer consumers the ability to "opt-out" of receiving future e-mail.

According to the FTC, the deceptive claims violate the FTC Act and the spoofing and failure to provide an "opt-out" capability violate provisions of the recently enacted CAN-SPAM Act.

A United States District Court entered a Temporary Restraining Order requiring an end to the illegal spamming and deceptive product claims and freezing the defendants' assets\(^{296}\).

**PART C : CANADA**

11. **Introduction**

Canada is an example of a country that has not yet enacted specific anti-spam legislation: "The distribution of unsolicited promotional and product information, in print form or over electronic networks is not illegal nor is it regulated in Canada".\(^{297}\) Such a transmission does not appear to constitute

\(^{295}\) A practice known as spoofing.

\(^{296}\) At time of writing, this matter had not been finalised.

an offence under the mischief provisions of the Criminal Code, and there are no other Canadian laws of general application that deal with bulk or unsolicited e-mail.

12. **Other Legislation**

Apart from advertising within the Canadian broadcasting system, advertising is generally not regulated. There are, however, specific provisions in various other laws dealing with matters such as tobacco advertising and misleading advertising in the Competition Act.

13. **The Personal Information Protection and Electronic Documents Act**

Under the Personal Information Protection and Electronic Documents Act, e-mail addresses are considered to be personal information. This Act establishes clear obligations and responsibilities for those who collect, store and use personal information. The collection and use without consent of personal information, such as e-mail addresses, could run counter to the

---

298 In 1985, the Canadian Criminal Code was amended to create two groups of new offences. One group dealt with unauthorised access and use of computers, and the second group dealt with mischief in regard to computers and data. Computer mischief offences could apply in cases where spamming would interfere with or obstruct a person's access to data or use of a computer system, and the sender was "reckless" in that he or she understood that this was likely to occur. See "Internet And Bulk Unsolicited Electronic Mail (SPAM)" available at [http://e-com.ic.gc.ca/english/strat/Spam.html](http://e-com.ic.gc.ca/english/strat/Spam.html) (15 May 2003).


requirements of the Act. However, this privacy legislation applies only to organisations located in Canada.

14. **The Canadian Charter of Rights and Freedoms**

Spam is considered to be a form of expression and, as such, any attempt by the government to control it, regardless of the means, would have to be consistent with section 2 of the Canadian Charter of Rights and Freedoms.

15. **Industry Canada**

In 1999, Industry Canada released an information document on bulk unsolicited electronic mail\(^301\) which stated that the application of existing laws, appropriate Internet industry policies, technology and consumer awareness could, to a large extent, deal with abusive e-mailing. In this document the government also encouraged industry stakeholders to deal with bulk unsolicited e-mail, through voluntary industry-wide code and practices.\(^302\)

With the significant rise in the volume of junk e-mail experienced, the department began discussions with some industry and consumer stakeholders as part of a review of its current policy. In January 2003, the


\(^302\) For example, the Canadian Marketing Association (CMA) has established a code and guidelines dealing with Internet use for the distribution of promotional materials.
department issued a discussion paper\textsuperscript{303} that was sent to a small number of organisations representing ISPs, information technology industries, businesses and consumers. The Discussion Paper raised a number of questions relating to government policies, enforcement of existing laws such as the Criminal Code, network technologies, industry business practices as well as consumer education and awareness.

PART D : AUSTRALIA

16. Introduction

The provisions of the Australian Spam Act of 2003\textsuperscript{304} ("Spam Act") came into effect on 10 April 2004. The Spam Act was enacted on 12 December 2003 with a proviso that its penalty provisions would come into effect 120 days later.\textsuperscript{305} This grace period was included to ensure that people could learn about the requirements of the Spam Act, and ensure that their business practices satisfy those requirements.

16.1 Purpose Of The Spam Act

The Spam Act sets up a framework for regulating commercial email and other types of commercial electronic messages.


According to the Australian Communications Authority,\textsuperscript{306} "the Spam Act was developed in response to the problems caused by the growing volume of unsolicited commercial electronic messages, or spam. Spam threatens the viability and efficiency of electronic messaging. It damages consumer confidence, obstructs legitimate business activities and imposes many costs on users. The legislation prohibits unsolicited commercial electronic messages".

There are, however, many legitimate uses for electronic messaging. It is an important tool for business, and it allows simple and low cost communication with consumers who are increasingly using such technologies to access information. The Spam Act therefore includes rules aimed at preserving legitimate business communication activities and encouraging the responsible use of electronic messaging. The Act states that commercial electronic messages must accurately identify their sender,\textsuperscript{307} and include a way for the recipient to unsubscribe from future such messages if they want to.\textsuperscript{308}

\textsuperscript{305} Section 2.
16.2 *Definition Of Spam*

The Spam Act refers to spam as "unsolicited commercial electronic messaging".\textsuperscript{309} "Electronic messaging" includes e-mails, mobile phone text messages (SMS), multimedia messaging (MMS) and instant messaging (iM).\textsuperscript{310}

Not all forms of spam are prohibited by the Spam Act. The Spam Act states that "unsolicited commercial electronic messages must not be sent".\textsuperscript{311} Therefore, only commercial spam falls under the Spam Act.

Therefore, the message must be commercial in nature, for example offering a commercial transaction, or directing the recipient to a location where a commercial transaction can take place. Messages without any commercial content that do not contain links or directions to a commercial Web site or location are not covered by the Spam Act.

There are a large number of commercial electronic messages that can be sent legitimately. Commercial electronic messages are only considered to be spam if they are sent without the prior consent of the recipient, as unsolicited messages.

\textsuperscript{307} Section 17.
\textsuperscript{308} Section 18.
\textsuperscript{309} Section 16.
\textsuperscript{310} Section 5.
\textsuperscript{311} Section 16.
The legislation applies equally to both single and bulk email messages that are commercial in nature. The Spam Act makes no reference to bulk messaging, and a single unsolicited commercial electronic message could be spam. The message does not need to be sent in bulk, or received in bulk.

16.3 **Consent**

Under the Australian Spam Act, consent means:\(^{312}\)

"(a) express consent; or

(b) consent that can reasonably be inferred from:

(i) the conduct; and

(ii) the business and other relationships;

of the individual or organisation concerned".

Therefore, the Spam Act follows the "opt-in" principle. Messages should only be sent where the sender has consent from the recipient.\(^ {313}\) The Act has a very limiting premise of no mail without consent. Using the analogy of conventional mail, it would be absurd to say that no one could write you a letter unless you had already given consent to receive it. Yet this is precisely what has been enacted within the Spam Act.

---

\(^{312}\) Schedule 2 clause 2.

\(^{313}\) Section 16 and schedule 2.
Consent may be either express or inferred consent from the person they wish to contact.\textsuperscript{314} Express consent is usually a direct indication that it is acceptable to send the message, or messages of that nature. It may also be possible to infer consent based on a business or other relationship with the person, and their conduct.

16.4 \textit{Identification Of The Sender}

Under the Spam Act, messages must contain clear and accurate identification of who is responsible for sending the message, and how they can be contacted.\textsuperscript{315} Therefore, all commercial electronic messages must show full details of the sender’s identity and physical address.

Identification details that are provided must be reasonably likely to be accurate for a period of 30 days after the message is sent.\textsuperscript{316} This would be a consideration if the business was about to change their address.

16.5 \textit{"Opt-out"}

The Spam Act also contains requirements for an "opt-out" facility in all commercial e-mail, even if the commercial e-mail was requested.\textsuperscript{317} All messages must contain a functional way for recipients to indicate that they

\textsuperscript{314} See further Chapter 8 below for a discussion of express and conferred consent under the Spam Act.
\textsuperscript{315} Section 17.
\textsuperscript{316} It would be useful to include this aspect in South African legislation. See Chapter 8 below.
do not wish to receive such messages in the future and that they wish to unsubscribe.

In terms of the Act, the unsubscribe facility must be reasonably likely to be functional for a period of 30 days after the day on which the message was sent.

Unsubscribe requests must be honoured within 5 working days. The Spam Act states that a request to withdraw consent will be considered to have taken effect after five working days from the date on which the request was sent (for electronic unsubscribe requests) or delivered (in the case of unsubscribe messages sent by post or other means).

16.6 Messages With An Australian Link

Under the Spam Act it is illegal to send, or cause to be sent, unsolicited commercial electronic messages that have an Australian link. A message has an ‘Australian link’ if it either originates or was commissioned in Australia and is sent to any destination, or originates overseas but has been sent to an address accessed in Australia.

---

317 Section 18.
318 Section 18.
319 Schedule 2 clause 6. It would be useful to include this aspect in South African legislation. See Chapter 8 below.
Therefore, it is illegal to send an unsolicited commercial e-mail that is sent:

1. from Australia; or
2. by senders who:
   a) are physically present in Australia; or
   b) are organisations with central management and control (board meetings) in Australia; or
3. to computers in Australia (including the recipient’s personal computer); or
4. to recipients who read the message when they:
   a) are physically present in Australia; or
   b) are organisations carrying on business in Australia;

Enforcement of the penalties relating to overseas spam will be problematic until international arrangements are in place. Nevertheless, the legislation ensures that there is an appropriate enforcement regime in place to deal with overseas spammers as soon as international arrangements are in place. The Spam Act includes provisions that anticipate Australia’s entry into such arrangements with other countries concerned about spam. This will enable regulations to be made giving effect to these agreements once in place.
16.7  Address Harvesting

The Spam Act defines address-harvesting software as:  

"software that is specifically designed or marketed for use for:

(a) searching the Internet for electronic addresses; and

(b) collecting, compiling, capturing or otherwise harvesting those electronic addresses".

Software used to harvest addresses and generate address lists for the purposes of sending spam are illegal under the Spam Act. Businesses are not permitted to use electronic address harvesting software, or lists which have been generated using such software, for the purpose of sending unsolicited commercial electronic messages.

Lists generated manually (for example by reviewing Web sites) are not prohibited under the Spam Act. However, if addressees have included a statement adjacent to their electronic address indicating the addressee does not wish to receive commercial messages, this must be respected.

---

321  This provision is similar to section 90 of the ECT Act. See Chapter 3 above.
322  Section 4.
323  Section 20, 21 and 22.
16.8  **Financial Penalties**

The maximum penalties under the Spam Act are considerable. The maximum daily penalty is Aus $1.1 million for companies, and Aus $220,000 for individuals, and anybody knowingly concerned in a violation is liable. A business that is found to be in breach of the Spam Act may be subject to a Court imposed penalty of up to Aus $220,000 for a single day's contravention. If the business subsequently contravenes the same provision, they may be subject to a penalty of up to Aus $1.1 million.

16.9  **Enforcement**

The Australian Communications Authority (ACA) is responsible for enforcing the provisions of the Spam Act. The legislation gives the ACA the power to issue formal warnings, seek injunctions and seek warrants to investigate and monitor suspected spammers.

Industry codes of practice are likely to be developed by industry organisations such as the Australian Direct Marketing Association (ADMA) and the Internet Industry Association (IIA). The codes are intended to provide relevant and achievable standards and procedures developed by groups representing industry sectors for their member organisations, to assist

---

324 Part 4.
325 Additional information about the ACA's role is available from: [www.aca.gov.au](http://www.aca.gov.au) (29 April 2004).
326 Part 6.
compliance with the Spam Act. These codes will be presented to the ACA for registration.

Under the Spam Act, the ACA is concerned with unsolicited commercial email (and other electronic messages) whether or not the content is itself legal or illegal. However, much email also carries content which is itself illegal under other laws, for example where it is fraudulent, offensive or carries a computer virus. The ACA will be working closely with other regulators and law enforcement agencies on the problem of illegal messages.

The Spam Act specifies a number of options that are available to enforce the legislation, depending on which is the most appropriate response to the contravention that has occurred. The range of possible activities includes formal warnings, infringement notices (similar to a speeding ticket), and court actions.

a) Formal warnings

The ACA may choose to issue a formal warning, rather than issue an infringement notice or initiate a full court proceeding. This would typically be done where the ACA was satisfied that the contravention was largely inadvertent and would not be repeated, or in other cases where a warning would suffice to change the contravening behaviour.

---

327 Section 41.
b) Infringement notices

The ACA may choose to issue infringement notices\(^{328}\) for contraventions of the legislation, instead of initiating a full court proceeding. A person who receives an infringement notice may refuse to pay, but could then be subject to a court action, where, if the contravention was proven, they could be penalised at a higher rate than the infringement notice.

c) Court actions

The ACA may initiate a court action in respect of a contravention of the legislation.\(^{329}\) If a contravention is found to have occurred, the ACA may apply to the court to order the person or organisation involved to pay a penalty, and additionally, to surrender any financial benefit they gained in the course of their contravening activity. Any person who has suffered loss or damages from someone else contravening the Spam Act, or the ACA on their behalf, may apply to the court to make an order for compensation.

16.10 Exemptions

There are exemptions in the legislation to allow political parties, churches and charities to continue to send unsolicited e-mails.\(^{330}\)

\(^{328}\) Section 30 and schedule 3.
\(^{329}\) Part 5.
16.11 *Potential Problems With The Spam Act*

Experts have raised concerns that although the Spam Act is aimed at reducing bulk unsolicited e-mail, it could also target innocent single-message senders, who send a targeted e-mail to a person they had met casually.

While the legislation bans the sending of unsolicited commercial e-mails, it does not include the term ‘bulk’. Critics have suggested that legislation that specifically targets bulk e-mail senders (generally defined as those who send more than 100 messages) would help to overcome the problem of having people who send a single email being netted in the anti-spam enforcement web by differentiating them from serious spammers.\(^{331}\)

The National Office for the Information Economy (NOIE),\(^{332}\) however, argues that the concept of bulk messaging appears to reduce the efficacy and applicability of anti-spam legislation and that the proposed legislation will allow the Australian Communications Authority to ensure any response would be proportional to a breach of the laws. The authorities will also only need to get one example of spam from one person to prosecute, and they will not have to accumulate evidence that there has been more than the minimum...

\(^{330}\) Schedule 1 clause 3.
number to get to bulk (whatever the definition of bulk is) in order to prosecute.

NOIE has argued that spammers would be able to get around any rules defining what constitutes bulk, by sending 99 e-mails, for example, if the law prohibited 100 or more. This, however, could be overcome by the use of clauses such as "substantially the same message".

It has been suggested that a way around the problem may be to exempt senders who can demonstrate a "genuine belief" that the addressee is likely to have an interest in the contents of the message. However, such an approach would be flawed because measuring offences by a person's state of mind would be difficult to prove.

Another fairly serious flaw in the Spam Act is the provisions allowing the sending of factual e-mails. This is potentially a serious loophole. The provisions are beneficial for those organisations that send out newsletters, but they are open to abuse. Spammers would be able to use a factual statement, attach their logo and contact details to it and continue with business as usual.

---

17. **Internet Industry Code of Practice**

Version 5.0 of the Internet Industry Association (IIA) Code of Practice makes the following restrictions on spam in section 10:

a) IIA members and code subscribers must not spam, and must not encourage spam (section 10.7), with exceptions in the case of pre-existing relationships (this does not prevent acquaintance spam).

b) IIA members and code subscribers who do use acquaintance spam must provide recipients with the capability to "opt-out", and must include "opt-out" instructions in the spam (section 10.8).

c) IIA members and code subscribers must not send even acquaintance spam containing prohibited content (section 10.10. Prohibited content is mostly pornographic in nature).

d) IIA member and code subscriber Internet Service Providers should have an Acceptable Use Policy that prohibits spam (section 10.11), and further prohibits services that depend on spam (in other words, ISPs should take action against web sites that use spam, even though they may spam from other sources).

e) ISPs should have a working contact address for spam complaints, such as an "abuse@" e-mail address (section 10.12).

f) ISPs should install relay protection on their mail servers, to prevent spammers from using the relay to evade detection or penalty (section 10.13)

---

18. **Electronic Commerce Guidelines**

On 18 May 2000, the Minister for Financial Services and Regulation launched electronic commerce guidelines for business. The document, "Building Consumer Sovereignty in Electronic Commerce (A Best Practice Model for Business)", is intended to serve both as guidelines for businesses, and for industry codes. This government document clearly states that spam is not acceptable.

Under paragraph 23, for commercial e-mail:

1) Businesses should not send commercial e-mail except:
   
   a) to people with whom they have an existing relationship; or

   b) to people who have already said they want to receive commercial e-mail; and

2) Businesses should have simple procedures so that consumers can let them know they do not want to receive commercial e-mail.

19. **Existing Legislation**

19.1 **The Telecommunications Act**

The Telecommunications Act\(^{335}\) contains additional provisions about commercial electronic messages. Those provisions include Part 6 (industry

---

codes and standards), Part 26 (investigations), Part 27 (information-gathering powers) and Part 28 (enforcement).

19.2 The Privacy Act And The National Privacy Principles

In addition to the requirements of the Spam Act, businesses need to ensure that their practices are in accordance with the Privacy Act and the National Privacy Principles in all activities where they deal with personal information. Personal information includes customers’ contact details.

The obligations under the Privacy Act are still applicable to businesses. In particular, if e-mail is being sent for direct marketing purposes, the business must take steps to obtain consent in advance of that use unless it is impracticable to obtain that consent. To be impracticable ("not capable of being put into practice"), it must be so difficult or unlikely to succeed that there is no point in even making the attempt. It will not be impracticable if the business collected the e-mail address from the individual knowing that one of the uses of the e-mail address would be or may become, direct marketing.

Messages will be prohibited under the Privacy Act, even if they would not be prohibited under the Spam Act, if a sender collects e-mail addresses verbally,

337 Available at www.privacy.gov.au (29 April 2004).
on a web page, or on a form without obtaining consent for the purpose of direct marketing at the time of collection.

The intended effect of the Privacy Act in its current form is to preclude spammers from harvesting email addresses without the consent of their owners. This must in general be consent to the use of the address for spam, as a person who has consented to the collection of their email address for a particular purpose does not thereby consent to it being used for other purposes.

As indicated above however, spammers may be entitled consistently with the National Privacy Principles to send spam to email addresses that were collected for a different purpose if it is impracticable to obtain the recipient's consent to the use of their address for spam. Even if it will always be practical to obtain the recipient's consent, the prospect that spammers might seek such consent by email somewhat defeats the purpose of using the Privacy Act to combat unwanted email. Furthermore, spammers may argue that unless an email address is able to be used to individually identify its owner, it is not personal information at all, or alternatively that those who publish their email address publicly, for example on a Web site, implicitly consent to its collection.
If the Office of the Federal Privacy Commissioner receives a complaint relating to a spammer who is bound by and found to be in breach of the Act, the spammer can be requested to remedy its breach. In the event that the spammer fails or refuses to comply, the complaint can be elevated to the Privacy Commissioner for an enforceable determination to be made. The failure to comply with an enforceable determination is actionable in the Federal Court. To date, no complaint about spam has reached this point.

19.3 *The Trade Practices Act*

The Trade Practices Act\(^{338}\) can be used as a weapon against spam where the spammer is located within Australia. Section 52 of the Trade Practices Act in particular has obvious application in combatting spam that is misleading or deceptive, either in its body or in its headers.

Section 52(1) states:

"A corporation shall not, in trade or commerce, engage in conduct that is misleading or deceptive."

Although the Act has not yet been applied against spam or spammers in Australia, the United States Federal Trade Commission has applied equivalent legislation against United States spammers.

19.4  Corporations Law

The Australian Securities and Investments Commission (ASIC) has taken action against spam that promotes unlicensed investment schemes contrary to the Corporations Law.

In *R v Hourmouzis* 339 the defendant pleaded guilty to interfering with, interrupting or obstructing the lawful use of a computer contrary to section 76E(b) of the Crimes Act 1914 (for sending the spam through open relay mail servers), and to making statements or disseminating information that was false in a material particular or materially misleading and likely to induce the purchase of securities by other persons, contrary to section 999 of the Corporations Law. The United States Securities Exchange Commission also obtained judgment against Hourmouzis in the District Court of Colorado for about US$15,800 under broadly equivalent legislation.

19.5  The Crimes Act

Section 76E(b) of the Crimes Act 1914 imposes a maximum penalty of 10 years imprisonment, and makes it an offence to interfere with, interrupt or obstruct the lawful use of, a computer by means of a carrier (telephone line

---

or ISP) or facility provided by the Commonwealth. In *R v Hourmouzis*, the defendant relayed his spam off the affected third party computer systems.

Therefore, under this section, relay spam is a criminal offence. If you are in Australia and relay spam off 3rd party systems without permission, or even if you are not in Australia and you relay spam off systems in Australia without permission, you can be charged and convicted to up to 10 years imprisonment.

19.6 *The Criminal Code Act*

Many spammers exploit open relay mail servers, in an endeavour to mask their real locations, and also to cast the cost of delivery of the spam onto the owner of the misconfigured server.

This practice may now be in breach of section 478.1 of the Criminal Code Act. It is likely that, by virtue of section 476.3 of the Criminal Code Act, it is even in breach of that provision if the mail server that is abused is overseas (which is very common, as there are many old and misconfigured mail servers in the third world). In simplified terms, liability will attach if the offender institutes or assists in the institution of an unauthorised connection to an open relay server, provided that the connection is either initiated in

---

Australia, or if results of the abuse occur in Australia, or if the offender is an Australian citizen.

Although the legislation is not unambiguous and these provisions have not been tested, it is arguable that the mere sending to an Australian recipient of spam through a compromised open relay server overseas would constitute an offence by the sender, even if the sender had no other connection with Australia. The reverse, namely an Australian spammer sending to overseas addresses through an open relay, is even more likely to be caught by these provisions.

19.7 *The Personal Information Protection and Electronic Documents Act*

Under the Personal Information Protection and Electronic Documents Act, which came into force on 1 January 2001, electronic mail addresses are considered personal information and are subject to the provisions of the Act. In October 2002, the Privacy Commissioner found a number of major organisations that provide communications services at fault for failing to obtain meaningful consent from their customers before using their addresses for secondary purposes, such as commercial solicitation.

---

19.8  *The Privacy Amendment (Private Sector) Act*

The Privacy Amendment (Private Sector) Act\textsuperscript{343} makes certain types of acquaintance spam illegal as of December 2001. Businesses covered by the provisions of that Act must obtain permission from their customers in some situations prior to using their e-mail addresses for anything that can be construed as spam.

20.  **Case Law**

In November 2000, in the case of *R v Hourmouzis*, Australia secured its first conviction related to spamming. Hourmouzis manipulated the share price of an American company by posting information on the Internet and sending spam that contained false and misleading information about the company.\textsuperscript{344}

On 8 and 9 May 1999, Hourmouzis posted messages on Internet Bulletin Boards in the United States and sent more than four million unsolicited e-mail messages to recipients in the United States, Australia and in other parts of the world. The messages contained a statement that share value of the company would increase from the then current price of US$0.33 to US$3.00 once pending patents were released by the company, and that the price

\textsuperscript{344} See ASIC Media release "Two Years Jail – Suspended – For Internet Spammer" available at
would increase up to 900 per cent within the next few months. The effect of the information was that the company’s share price on the NASDAQ doubled, with trading volume increasing by more than ten times the previous month’s average trading volume.

Hourmouzis had purchased 65,500 shares in the company through a stock broking firm in Canada several days before he transmitted the information. He sold the shares on the first trading day after the transmission of the information and realised a profit of approximately A$7,000.

Hourmouzis was prosecuted by the Australian Securities and Investments Commission for distributing false and misleading information with the intention of inducing investors to purchase the company’s stock. He pleaded guilty and was sentenced to two years’ imprisonment on each of three counts, to be served concurrently. The Court ordered that twenty one months of the sentence be suspended upon his entering into a two-year good behaviour bond with a surety of A$500.

In a separate prosecution, Wayne Loughnan, who assisted Hourmouzis in the sharemarket manipulation, was sentenced to two years’ imprisonment, wholly suspended.
PART E: THE EUROPEAN UNION

21. **Introduction**

The European Union does not prohibit spam, but it permits individual member states to do so. Article 13 of the Directive on processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications 2002)\(^{345}\) will guide legislation banning spam throughout the 15 European member countries.\(^{346}\) Member states are required to implement the Directive by enacting national legislation.

22. **Directive on Privacy and Electronic Communications 2002**

As part of the European Commission's 1999 Review of the communications framework, the Directive on Privacy and Electronic Communications\(^{347}\) was adopted to update the existing Telecommunications Data Protection Directive.\(^{348}\)

\(^{340}\)opendocument (30 April 2004).


\(^{346}\) The European Union has 15 member states: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom.

\(^{347}\) (2002/58/EC).

\(^{348}\) (97/66/EC).
The overriding aim of the new Directive is to take account of technological changes and to make the provisions as technology-neutral as possible. The Telecommunications Data Protection Directive relating to the processing of personal data and the protection of privacy in telecommunications sector was repealed with effect from 31 October 2002, and was replaced by the Directive on Privacy and Electronic Communications.

The final Directive on Privacy and Electronic Communications was adopted on 12 July 2002 and required implementation in Member States by 31 October 2003. Final implementing regulations came into force on 11 December 2003.

The Directive primarily requires EU Member States to introduce new laws regulating the use of unsolicited commercial communications; cookies; location and traffic data; and publicly available directories. It also replaces existing definitions for telecommunications services and networks with new definitions for electronic communications and services to ensure technological neutrality and clarify the position of e-mail and use of the Internet.

22.1 "Opt-in"

[^349]: Article 19 of Directive 2002/58/EC.
The new Directive on Privacy and Electronic Communications follows the "opt-in principle". With a limited exception covering existing customer relationships, e-mail marketing is only permitted with prior consent. The Directive prohibits e-mail marketers in the Union from sending their promotions to individuals unless those targeted have expressly asked to receive promotions. In the context of an existing customer relationship, companies may continue to send emails to market similar products on an "opt-out" basis. Member States may also ban unsolicited commercial e-mails to businesses.

Contravention of the Regulations may lead to regulatory investigation and fines, civil damages actions through the courts and, in some cases, criminal liability. In certain circumstances, criminal sanctions may be imposed not only on a company that breaches the Regulations, but also on its directors.

EU Members Austria, Belgium, Denmark, Finland, Germany, Greece, Italy, and Spain, the United Kingdom, as well as European Free Trade Association (EFTA) member Norway have implemented "opt-in" in their national legislation.

22.2 Final Text of Directive 2002/58/EC

Section 40 of the Directive states that safeguards should be provided for subscribers against intrusion of their privacy by unsolicited
communications for direct marketing purposes, in particular by means of automated calling machines, telefaxes, and e-mails.

This section identifies that while these forms of unsolicited commercial communications may be relatively easy and cheap to send, they may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment.

The Directive finds that for such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them.

This section states further that "the single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users".

Section 41 of the Directive states that within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the electronic contact details in accordance with Directive 95/46/EC.
When electronic contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

In terms of section 43 of the Directive, in order to facilitate effective enforcement of Community rules on unsolicited messages for direct marketing, it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.

Section 44 of the Directive notes that certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message, without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments. These arrangements may continue to be useful in certain cases as an additional tool to the general obligations established in this Directive.
In terms of section 45, the Directive is without prejudice to the arrangements which Member States make to protect the legitimate interests of legal persons with regard to unsolicited communications for direct marketing purposes. Where Member States establish an "opt-out" register for such communications to legal persons, mostly business users, the provisions of Article 7 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (Directive on electronic commerce) are fully applicable.

Article 2(h) of the Directive defines "electronic mail" as:

"any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient".

Article 13 of the Directive deals with "unsolicited communications".

Paragraph 1 of Article 13 states:

"the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent".
Notwithstanding paragraph 1, where a person obtains electronic contact details from customers, in the context of the sale of a product or a service, "that person may use these electronic contact details for direct marketing of its own similar products or services".

In these circumstances, customers must clearly and distinctly be given the opportunity to object, free of charge and in an easy manner, to the use of their electronic contact details. Customers must be given this opportunity to object both at the time when the electronic contact details are collected and on each occasion that messages are sent to them.

Paragraph 4 of Article 13 prohibits the practice of disguising or concealing the identity of the sender on whose behalf the communication is made. Paragraph 4 also prohibits the sending of electronic mail for the purposes of direct marketing without a valid address to which the recipient may send a request that such communications cease.

In terms of paragraph 5 of Article 13, "Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected".

The E-Commerce Directive requires the implementation of "opt-out" lists. There are certain labelling requirements, and registration on "opt-out" lists is restricted to natural persons.

The E-Commerce Directive provides for "unsolicited commercial communications" as follows:

"In addition to other requirements established by Community law, Member States which permit unsolicited commercial communication by electronic mail shall ensure that such commercial communication by a service provider established in their territory shall be identifiable clearly and unambiguously as such as soon as it is received by the recipient".

The E-Commerce Directive provides further that:

"Without prejudice to Directive 97/7/EC and Directive 97/66/EC, Member States shall take measures to ensure that service providers undertaking unsolicited commercial communications by e-mail consult regularly and respect the "opt-out" registers in which natural persons not wishing to receive such commercial communications can register themselves".
24. Other Directives

The regulations are to be followed in addition to those in other Directives (for example, Distance Selling, Data Protection and Telecommunications) which provide for "opt-out" as a minimum. Member States may adopt more restrictive provisions if they wish. Service Providers are free to set their own Terms of Service or Acceptable Use Policies as they see fit, and they are not required to carry spam.

PART F : EUROPEAN UNION COUNTRIES

25. Introduction

Several European Union countries have adopted some form of legislation that seeks to regulate spam in terms of the EC Directive on Privacy and Electronic Communications 2002 ("the Directive").

26. The United Kingdom

The United Kingdom Government has introduced anti-spam legislation as part of its implementation of the Directive. The laws came into effect on 11 December 2003, in terms of the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("the Regulations").

---

350 Directive 97/7/EC.
351 Directive 95/46/EC.
352 Directive 97/66/EC.
The Regulations make it an offence for a UK company to send spam messages, unless the recipient is an existing customer or has given their permission to receive such material.\textsuperscript{353}

Firms who contravene the law could face a £5,000 fine for each breach. However, the new legislation covers only personal e-mail accounts. It is still legal for a company to send unsolicited commercial messages to corporate e-mail addresses. According to the Department of Trade and Industry (DTI), this decision was taken so that "legitimate business to business communication" was not hampered. According to the DTI, during its recent consultation on the EU directive, many businesses said they did not want to lose e-mail as a marketing tool.\textsuperscript{354}

26.1 "Opt-in"

The Regulations generally prohibit the sending of unsolicited electronic commercial communications if the recipient has not previously specifically "opted-in" to receive such communications. Typically, "opt-in" consent is obtained by the "ticking" of a box, clicking on an icon or following a specific request for information from the recipient.

\textsuperscript{353} Links to the new Directive, the UK’s implementing Regulations, and other relevant information are set out on the Department of Trade & Industry’s Web site: \url{http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy電子電子電子電子電子電子電子電子電子電子電子電子電子電子電子電子電子電子電子電子電子電子郵件コミュニケーション200258ec.html} (10 May 2004).

\textsuperscript{354} See Wearden "UK Anti-Spam Laws Launched" available at \url{http://www.silicon.com/news/165/14/6067.html} (3 October 2003).
A pre-existing customer relationship is the only exception to the requirement for specific "opt-in" provided for in the Regulations. A business may send unsolicited electronic commercial communications without "opt-in" consent if all of the following criteria are fulfilled:

a) The sender has obtained the contact details of the recipient in the course of a sale or negotiations for the sale of a product or service to the individual;

b) The communication is made regarding the sender’s similar products and services only; and

c) The recipient is given a simple means of refusing (free of charge) the use of his or her contact details for the purposes of sending such communications, both at the time of the initial collection of the details, and at the time of each subsequent communication.

Unlike the implementing laws of other Member States, the Regulations only require negotiations (that would normally lead to a sale) to have taken place for the first criterion to be fulfilled.

The communication must concern "the company’s similar products or services only." The Information Commissioner’s guidance to the Regulations limits further marketing under this section to the sort of marketing for products or services that an individual would reasonably expect to receive. Therefore, a link must exist between the product or service that was the
subject of the first sale or negotiation and the unsolicited e-mail. The sending of unsolicited commercial communications by subsidiaries and affiliated companies based on a prior sale or negotiations entered into by another group company does not appear permissible under the Regulations.

26.2 "Opt-out"

Under the Regulations, individuals have the right to "opt-out" of receiving further unsolicited commercial communications at any time. Senders of unsolicited commercial communications are required not to disguise their identity and must provide a valid contact address.

26.3 Corporate Subscribers

The Directive primarily seeks to protect individuals from direct marketing, although it does oblige the Member States to ensure that the legitimate interests of non-individuals, i.e., corporate subscribers, are "sufficiently protected."

Under the Regulations, an "opt-out" right has been provided for corporate subscribers where the recipient’s address contains personal data, i.e., other than where the address starts with "info@" or "the company’s name@," for example.
26.4  *Legacy Provisions*

The new regime will bring about many uncertainties for businesses that have compiled contact registers in accordance with previous legislation. To lessen initial disruptions, the Information Commissioner’s guidance to the Regulations suggests that "legacy" email addresses (i.e., e-mail addresses that were collected prior to the implementation date of the new Regulations) would be usable indefinitely by businesses following the implementation date, provided they were collected in accordance with the legislation in force at that time "and have been used recently".

27.  **Austria**

An amendment to the Austrian Telecommunications Act prohibits both unsolicited commercial e-mail and unsolicited bulk e-mail.

The unofficial translation of the amendment reads as follows:

"Section 101: Unsolicited Calls

Calls - including fax transmissions - for advertising purposes shall not be permitted without the prior consent of the subscribers. The consent of a person authorised by the subscriber to use his line shall be equal to the consent of the subscriber himself. The consent may be revoked at any time; the revocation of consent having no influence on a contractual relationship with the person to whom the consent is given. Sending of
electronic mail as a mass mailing or for advertising purposes shall require the prior consent of the recipient, revocable at any time."

"Section 104:

(3) An infraction subject to a fine of up to 500,000 ATS (EUR 36,330 or USD $37,060) is committed by anyone who ...

23. contrary to section 101 makes unsolicited calls or sends bulk or advertising e-mail."

28. **Belgium**

In Belgium, legislation "Concerning certain legal aspects of Information Society services" provides:\(^{358}\)

"Article 15: Advertising by electronic mail

Section 1. The use of electronic mail for advertising without the prior specific and informed consent of the recipient. The King, together with representatives of the Ministries of Justice and Economic Affairs will determine the forms according to which the consent envisaged in the first part is to be obtained and retained in registries.

Section 2. When advertising by e-mail, the service provider [sender] is to ensure the following:

---

1. supplying clear and comprehensible information concerning the right to refuse such advertising in the future.

2. to indicate an appropriate method to exercise this right efficiently by electronic means.

Section 3. when advertising by electronic mail, it is forbidden

1. to use the electronic address or identity of a third party

2. to falsify or disguise information which makes it possible to identify the origin of the message or its routing.

Section 4. The service provider [sender] must prove that advertising by electronic mail was solicited."

29. **Denmark**

29.1 *Legislation*

Danish law prohibits the sending of unsolicited advertising e-mail and faxes.\(^{359}\)

Under the Marketing Practices Act -Consolidated Act,\(^ {360}\)

"Where a supplier sells goods immovable or moveable property or work or services to customers he shall not be allowed to make calls to anybody using electronic mail, automated calling systems or facsimile

machines for the purposes of such selling unless the particular customer has made a prior request for such calls."

29.2  Case Law

In May 2003, a Danish company was convicted and fined for sending spam. Denmark's government-run Consumer Agency sued Fonn Danmark after it received 50 complaints. The Maritime and Commercial Court in Copenhagen fined the company $2,206 for sending 156 unsolicited commercial e-mails during 2002.\textsuperscript{361}

30.  Germany\textsuperscript{362}

30.1  Legislation

Since February 2001 a special project group for email marketing of the German Multimedia Association has been concerned with developing guidelines. Their definition of "acceptable email marketing" is firmly based on "opt-in".\textsuperscript{363}

\textsuperscript{360} No 699 of 17 July 2000.
\textsuperscript{361} See "Danish Company Fined Over Spam Campaign" available at \url{http://www.nandotimes.com/technology/v-text/story/874440p-6099494c.html} (7 May 2003).
\textsuperscript{363} Available at
30.2  Case Law

The local court in Dachau did not consider unsolicited advertising emails sent to companies to be an unauthorised intrusion. In its judgement of 10 July 2001, the Dachau court rejected the suit of a local software company that demanded compensation from a firm which had sent a 2.5 Megabyte PDF file containing advertising material.

According to the Court, spam along with other advertising is socially acceptable and necessary in order to keep the economy going. The Court argued that advertising e-mails hardly interfere with business operations as opposed to fax and telephone, because unwanted messages can be deleted quickly and without trouble. Therefore, there was no interference with business operations according to section 823 of the Civil Code. The Court, however, did recognise the plaintiff's right to apply for a cease-and-desist order.

31. Finland

Finnish law, in effect from 1 July 1999, prohibits the sending of unsolicited commercial advertisements to private persons and to newsgroups. The

http://www.dmmv.de/de/7_pub/homepagedmmv/themen/emarketing/e-mailmarketing/e_mail_marketing_rechtsinfo.cfm (9 January 2003).


legislation is "opt-in" for individual recipients, and "opt-out" for corporate recipients.

32. **Italy**

In Italy there are 3 laws that prohibit spam:

a) DL 675/1996 on privacy protection: this states that a company must have authorisation from each user whose personal data (like e-mail) they want to use;

b) DL 171/1998 on telecommunications privacy protection (deriving from the European Community directive 97/66/CE): this outlaws all automatic systems to call a user and states that all the expenses of an advertisement must be paid by the company and not the user (for example, faxes and e-mails);

c) DL 185/1999 on customers protection about long-distance contracts (deriving from the European Community directive 97/7/CE): this states that if a company wants to sell something outside a commercial building (for example on the Internet or on the telephone), it must have permission of the user to advertise its products.

Therefore, prior consent is required from the recipient where email is used for advertising purposes. Violations are subject to fines from approximately

---

EUR 500 to 5000, which may be doubled in cases of severe or repeated offences.

33. Norway

The Act on Certain Aspects of Electronic Commerce and Other Information Society Services\(^\text{367}\) came into effect on 1 July 2003. The Act implements the E-commerce Directive\(^\text{368}\) into Norwegian law, and mirrors the Directive in all essential features.

Unsolicited commercial communications by e-mail\(^\text{369}\) are only legal in Norway if the receiver has actively opted to receive them. This also applies to information service providers established in other European Economic Area countries which provide unsolicited commercial communications by e-mail directed towards Norwegian residents.

PART G : JAPAN

34. Introduction

In the Asian region, Japan has the strongest position on spam, prohibiting its transmission unless an "opt-out" facility is provided.


\(^{368}\) (2000/31/EC).

\(^{369}\) Article 7 of the E-commerce Directive.
35. **Legislation**

Legislation on unsolicited email in Japan came into effect on 1 July 2002. The legislation comprises a new law regulating advertisement e-mail and an amendment to a 1976 law governing mail-order business.

In the legislation, spam is defined as mail that is sent for vendors' advertising purposes without recipients’ consent or request.370

The two bills establish "opt-out" as the default model for e-mail marketing, and require marketers to honour recipients' unsubscribe requests from any future mailings. The legislation requires senders of email advertisements to specify that the e-mail is an advertisement and that it has been sent without permission. In addition, senders would have to offer a valid return address and subject line in each e-mail.

The legislation also prohibits sending mail to randomly-generated e-mail addresses.371

---


371 In the United States, spammers typically use "dictionary spamming", for example, agates@microsoft.com, bgates@microsoft.com, etc. "In Japan, where cell-phones (based on i-mode) account a far greater percentage of the country's e-mail accounts than in the U.S., spammers can send mail to specific telephone numbers instead of names". See Saunders "Japan Takes Anti-Spam Steps" available at http://www.internetnews.com/IAR/print.php/1402331 (8 May 2003).
"Violators may face orders from authorities to improve or suspend business. If the senders continue violations despite the orders, individuals may be given prison terms of up to two years or fined up to 3 million yen and companies may face a fine of up to 300 million yen."  

PART H : CHINA

36. Introduction

Internet analysts believe that as much as 60 percent of spam sent to computer users worldwide originates or is routed through servers in China. Spamhaus identified 633 servers at 82 Chinese Internet service providers that send spam.

Many e-mail servers in China are poorly configured and allow spammers to send email anonymously through vulnerabilities known as "open relays". This has encouraged many spammers to set up inexpensive operations in the suburbs of Beijing. According to Spamhaus, China Telecom, one of the largest Internet service providers in China, receives more than 50,000 complaints of spam per day. Because of this, many companies block any incoming e-mail from Asia.

---

372 300 million Yen is approximately $2.5 million.  

373 A London organisation that tracks spammers.  
37. **The Internet Society of China**

The government-owned Internet Society of China (ISC)\(^{375}\) was inaugurated on 25 May 2001. The ISC is a coalition of companies and Internet users. In August 2003, the ISC set up a special task force to fight spam, calling it a threat to the communist country's political and social stability.

In September 2003, the Chinese government, through the ISC, blocked 127 computer servers it believes were being used to send mass amounts of unwanted e-mail.\(^{376}\) Any e-mail from the servers is automatically prevented from reaching the recipient. According to Chinese Internet officials, blocking the servers became necessary after the operators ignored warnings to stop sending spam. The warnings were sent to operators of 225 spam servers worldwide. Many of those servers are believed to have been involved in two cyber-attacks that shut down the ISC's Web site between 21 and 27 August 2003.

According to the ISC, 90 of the blocked servers were based in Taiwan and eight were from China's mainland. The remaining 29 were from outside China, including 16 from the US. One of the servers being blocked is operated by Shanghai Online, one of the country's largest Internet service providers.

---


providers. Many other servers in China have already been blocked by Internet service providers in other countries.

PART I: KOREA

38. Introduction

South Korea has enacted "opt-out" legislation under which senders must include a toll free telephone number where a recipient can call and unsubscribe from the mailing list to prevent further spam mail.\textsuperscript{377}

The law governing the communication networks\textsuperscript{378} also calls for Internet service providers allowing the sending of unsolicited advertising e-mail to include "Advertisement" or "Advertisement for Adults" in the header along with the subject heading of the e-mail. All spam emails will also have to include an extra "@" symbol in the title when sent within Korea.\textsuperscript{379}

Any violations of the new restrictions will be subject to fines of up to W10 million ($8,300).

\textsuperscript{377} It would be useful to include this aspect in South African legislation. See Chapter 8 below.
\textsuperscript{378} The Information and Communications Network Ordinance.
\textsuperscript{379} See further Sang-hun, \textit{The Chosun Ilbo} "Anti-Spam Measures Promised" available at \url{http://english.chosun.com/cgi-bin/printNews?id=200307030015} (22 July 2003). It would be useful to include these aspects in South African legislation. See Chapter 8 below.
The legislation was initially proposed as "opt-in", but was retained as "opt-out" pending further review. The tightened rules require online marketers to register their Internet Protocol addresses when they send commercial e-mails. They also enable regulators to close violating businesses and impose jail terms of up to three years.

39. **Case Law**

39.1 *Fines Imposed*

In the first case where the government imposed a fine against spammers, five spammers were fined 20 million won for sending unsolicited advertising e-mails. The five spammers include Carrot Korea, two Internet adult content providers Banana TV and Dawon Korea, a mid-size online shopping mall Inline Information Technologies, and a business-related Web site MK Husdaq.

Officials stated that "the government will extend co-operation with Internet service providers, e-mail service operators and consumers to effectively curb the inflow of unsolicited e-mails, not to mention the revision of related laws".\(^{380}\)

\(^{380}\) See further Deok-hyun "Unsolicited E-Mail Senders Fined" available at http://www.korealink.co.kr/kt_tech/200204/12002042917210545110.htm (30 April 2004).
39.2  Internet Service Providers

Korea's largest portal and email service provider, Daum Communications, has filed a lawsuit alleging spam-mail damage against three companies, including an education website "K" and adult portal "W." This marks the first e-mail service provider to file a damage suit for spam-mail reasons.

Daum Communications suffered damage because the three firms were sending a total of 6 million junk mails a month, which were backlogging its servers. The company demanded a total of W39 million in compensation from the three, insisting this figure includes the increased spending on equipment Daum had to buy.\(^\text{381}\)

PART J : CONCLUSION

It is important to recognise trends in spam legislation in other jurisdictions so as to ensure a measure of interoperability with those laws. Cross border enforcement against spam will also only be effective if countries adopt similar legislation.

Most spam legislation only prohibits unsolicited commercial e-mail, and does not provide for a blanket prohibition of all forms of spam.

Some countries, including the United States, have adopted the "opt-out" approach in their spam legislation. This means that a spammer can only be prosecuted if they continue sending spam after the recipient has requested that their email address be removed from the spammer's mailing list.

"Opt-in" is the approach that all European countries will adopt under the Directive on Privacy and Electronic Communications 2002. It is also the approach adopted by Australia under the Spam Act of 2003. The "opt-in" approach to spam legislation requires that a sender must first obtain a user's permission before sending a message.

The above comparative study provides useful guidance as to aspects that should be included in South African spam legislation and forms the basis of the content and recommendations contained in Chapter 8 below.
CHAPTER 5
THE INTERNATIONAL NATURE OF THE PROBLEM

1. Introduction

The Internet is a unique international computer-based communications medium that is not constrained by political borders. It constitutes a separate psychological and sociological place. The problem, however, is that this global network must be governed according to the rules of a compartmentalised legal world. This creates difficulties where current private international law is applied to a non-geographical and non-territorial Internet. "Almost every aspect of law is being challenged and many legal frameworks are inadequate to deal with the Internet".  

Part A examines the compatibility of traditional laws, formulated with national borders in mind, when applied to the Internet. Cyberspace knows no physical boundaries, and lawyers are dealing with Internet service providers (ISPs) and networks, as opposed to the notion of provinces and nations.

Part B outlines why the Internet causes problems in the realm of international law. I will examine issues such as jurisdiction, including the concept of "place" on the Internet, uploading and downloading, and the difficulty of determining nationality in cyberspace.
In Part C, I will look at possible approaches that may be adopted where Internet-related disputes arise, such as unifying the choice of law rules, unifying a substantive law of the Internet, and recognising the Internet as a jurisdiction in its own right.

This analysis covers bases of international jurisdiction in cyberspace. It identifies criteria which enable a State to prescribe rules for cyberspace, to subject violators of these rules to the process of its courts, and eventually to enforce these rules. The focus of this analysis is on the competence of the State to exercise its jurisdiction.

Finally, Part D provides a general conclusion for the present Chapter.

PART A : JURISDICTION

2. Introduction

The term ‘jurisdiction’ refers to the limitation on the authority or competence of a State to exercise its governmental functions by legislation, executive and enforcement action, and judicial decrees over persons and property. "Jurisdiction is an important aspect of sovereignty. Sovereignty empowers a State to exercise the functions of a state within a particular territory to the exclusion of other states".383 Therefore, a nation’s jurisdiction generally only

382 Buys Cyberlaw@SA (2000) Preface.
extends to individuals who reside within that country or to the transactions and events that occur within the natural borders of the nation.

International trade, migration, travel, crime, and recently the advent of the Internet, has meant that States have an interest in extending their jurisdiction beyond their territorial borders to cover persons and property in other jurisdictions.

Under international law, a State is subject to limitations on its authority to exercise jurisdiction in cases that involve foreign interests or activities. However, there are no rules that delineate spheres of national jurisdiction, and States have a wide discretion in the matter. Nevertheless, States have an obligation to exercise moderation and restraint in invoking jurisdiction over cases that have a foreign element, and they should avoid undue encroachment on the jurisdiction of other States.

2.1 The Lotus Case

The *Lotus* case sets out the starting point for the basic principles of jurisdiction under international law.

A French ship, the Lotus, collided with a Turkish ship, the Boz-Kourt, on the high seas. The Boz-Kourt sank and several crew members and passengers
lost their lives. The Lotus picked up the survivors and put into port in Turkey. The officer of the watch on board the Lotus at the time of the collision was arrested, tried, and convicted of culpable homicide in Turkey.

France objected to Turkey’s exercise of jurisdiction and the matter was referred to the Permanent Court of International Justice. France argued that only the flag-state had jurisdiction over acts committed on board a vessel on the high seas. Turkey, on the other hand, claimed that it had jurisdiction by virtue of the fact that the effects of the collision had been felt on a Turkish ship, which was viewed as part of Turkish territory.

The Permanent Court of International Justice confirmed the following principles of jurisdiction:

a) A state "may not exercise its power in any form in the territory of another state" – unless there is a permissive rule to the contrary.

b) International law does not prohibit a state "from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad". States have "a wide measure of discretion" to extend the application of their laws and the jurisdiction of their courts to persons, property, and acts outside their territory, "which is only limited in certain cases by prohibitive rules".

384 SS Lotus (France v Turkey) (1927) 4 ILR 153; PCIJ Reports Series A No 10.
c) The territoriality of criminal law, therefore, is not an absolute principle of international law”.

The Court held that Turkey had not violated international law because no rule of international law prohibited Turkey from trying a person for an offence that had produced effects on a Turkish vessel, and hence within Turkey itself.

This decision has been criticised on the ground that it empowers states to exercise jurisdiction over acts occurring outside their territory, except where there is proof of a rule of international law prohibiting such action. States have, however, sought to limit the exercise of extraterritorial jurisdiction in criminal matters to cases in which there is a direct and substantial connection between the state exercising jurisdiction and the matter in question.

It is submitted that the “direct and substantial interest” test is not particularly useful in the context of the Internet, particularly with regard to spam. This is because:

a) The effects of spam may be felt in multiple countries across the globe. Spam is often sent to infinite numbers of recipients, regardless of their location. Spam is also often relayed through multiple service providers, located across the globe, placing a burden on each network that carries the load.

b) The perpetrators involved do not necessarily have to be present in the same physical space, or country. Often spam is commissioned by
individuals or companies in one country, and sent on their behalf by spammers located in other countries, or through servers located in other countries.

2.2 Types Of Jurisdiction

There are three types of jurisdiction generally recognised in international law:\textsuperscript{385}

a) Jurisdiction to prescribe (legislative jurisdiction);

b) Jurisdiction to adjudicate (judicial jurisdiction); and

c) Jurisdiction to enforce (executive jurisdiction).

These distinctions are important in determining the limits of a country’s jurisdiction under international law. Jurisdiction to adjudicate and jurisdiction to enforce usually flow from a country’s jurisdiction to prescribe. Jurisdiction to adjudicate only applies where the country has jurisdiction to prescribe, unless the forum State is willing to apply the law of a foreign state. Similarly, jurisdiction to enforce often depends on jurisdiction to prescribe. The three types of jurisdiction are therefore often interdependent and their scope and limitations are determined by similar considerations.

\textsuperscript{385} Wilske and Schiller "International Jurisdiction In Cyberspace: Which States May Regulate The Internet?" available at
3. **Jurisdiction To Prescribe**

Jurisdiction to prescribe refers to a State’s authority to make its substantive laws applicable to particular persons and circumstances. International law recognises limitations on the authority of States to exercise jurisdiction to prescribe in circumstances affecting the interests of other States.

In principle, a state has legislative jurisdiction to regulate activities within its territory, as well as the conduct of its nationals abroad. However, even the links of territoriality or nationality do not suffice in all instances for the exercise of jurisdiction to prescribe. In certain circumstances a South African court will refuse to exercise jurisdiction over a crime committed within South African territory. For example, foreign diplomats are granted immunity from the jurisdiction of municipal courts, and under article 34 of the Vienna Convention on Diplomatic Relations, diplomats are exempted from most dues and taxes.

Under international law there are six generally accepted bases of jurisdiction or theories under which a State may claim to have jurisdiction to prescribe a rule of law over an activity: subjective territoriality, objective territoriality, nationality, passive nationality, protective principle and universality. These

---


---
are principles are broadly known as the territoriality principle, the nationality principle, the effects principle, and the protective principle.

As a general rule of international law, even where one of the bases of jurisdiction is present, the exercise of jurisdiction must be reasonable. The general mode of international conflict of law analysis is to weigh the interests of competing states in determining whether jurisdiction to prescribe exists. Although subjective territoriality usually trumps other interests, a strong state interest in protecting its nationals can outweigh a weak state interest in prosecuting the crime on its own soil.

3.1 The Territoriality Principle (Subjective Territoriality)

If an activity takes place within the territory of the forum State, then the forum State has the jurisdiction to prescribe a rule for that activity. Most criminal legislation falls into this category. Therefore, a State may assert its jurisdiction over all criminal acts that occur within its territory and over all persons responsible for such criminal acts, whatever their nationality. In South Africa this is the principle basis for the exercise of criminal jurisdiction.


Wilske and Schiller “International Jurisdiction In Cyberspace: Which States May Regulate The Internet?” available at
3.2  *The Nationality Principle*

A forum State may rely on nationality as a basis for jurisdiction. This is where a forum state will prosecute and punish their own nationals for offences committed abroad. Under the law of the Netherlands, for example, a Dutch national is liable to prosecution in Holland for an offence committed abroad, which is punishable under Netherlands law and which is also punishable under the law of the country where the offence was committed.\(^{389}\)

South Africa, like many other common-law countries, will not exercise extraterritorial jurisdiction on grounds of nationality.\(^{390}\) In *S v Mharapara*\(^{391}\) Gubbay JA rejected nationality as a basis for jurisdiction. The Court held:

"There is no rule of international law directing or obliging states to exercise criminal jurisdiction over their nationals for offences committed abroad. International law merely permits every state to apply its jurisdiction against its own citizens even when they are situated outside its boundaries . . . Thus the fact that customary international law is part of the municipal law of a state does not assist, because there is only a permissive principle involved and not a mandatory rule. The permissibility under international law for a state to exercise jurisdiction is not a sufficient basis for the exercise of jurisdiction by a municipal...

---


\(^{390}\) With the exception of treason.

\(^{391}\) 1986 (1) SA 556 (ZS) at 559 E-G.
Court of that state. A municipal Court must be satisfied in addition that the municipal law itself authorises the trial of a national for an offence committed abroad which would be punishable if committed at home”.

3.3 Passive Nationality

Passive nationality is a theory of jurisdiction based on the nationality of the victim. This principle allows a state to exercise jurisdiction over a person who commits an offence abroad which harms one of its own nationals.

Passive and "active" nationality are often invoked together to establish jurisdiction because a state has more interest in prosecuting an offence when both the offender and the victim are nationals of that state. However, passive nationality is rarely used because it is offensive for a nation to insist that foreign laws are not sufficient to protect its citizens abroad. It is also problematic because it is the offender and not the victim that is being prosecuted, and a state needs to seize the actor in order to undertake a criminal prosecution.

In recent years, however, this ground of jurisdiction has been invoked in order to suppress international terrorism.392

392 In 1985 a group of Palestinian terrorists murdered an American national on board an Italian ship, the Achille Lauro, on the high seas. The terrorists boarded the luxury liner as passengers, seized control of the ship, and held its crew and passengers hostage for the release of prisoners in Israel. The United States subsequently enacted legislation to give its courts jurisdiction to try anyone who kills or
3.4 The Effects Principle (Objective Territoriality)

This is sometimes referred to as "effects jurisdiction". It is invoked where the action takes place outside the territory of the forum State, but the primary effect of that activity is felt within the forum State.

The classic example is the case where a gunman standing in State A shoots and kills his victim in State B. The shooting takes place in State A, but the effect (murder) occurs in State B. State B would have the jurisdiction to prescribe under this principle.

3.5 The Protective Principle

The Protective principle expresses the desire of a sovereign to punish actions committed in other places solely because it feels threatened by those actions. Therefore, a state may exercise jurisdiction over aliens who have committed acts abroad that are considered prejudicial to its safety and security.

This principle is invoked where the "victim" would be the government or sovereign itself. For example, in *R v Neumann*, the defendant was an intentionally causes serious bodily harm to a national of the United States outside the United States where the offence "was intended to coerce, intimidate, or retaliate against a government or a civilian population". (Omnibus Diplomatic Security and Anti-Terrorism Act of 1986, Pub L No 99-399 ss 1202(a), 100 Stat 853, 896 (codified at 18 USCA ss 2331 (Supp 1989)). See Dugard *International Law, A South African Perspective* (1994) page 122.
alien resident that was charged with committing acts of treason against South Africa abroad. Murray J held\textsuperscript{394} that as South Africa was a sovereign state, it was "automatically entitled to punish crime directed against its independence and safety". A similar approach was adopted in America, in \textit{United States v Rodriguez},\textsuperscript{395} where the defendants were charged with making false statements in immigration applications while they were outside the United States.

This principle is disfavoured because it can easily offend the sovereignty of another nation. For this reason, both South African common law and statute require aliens tried in this way to have some connection with South Africa, usually in the form of residence.

3.6 \textit{Universality}

This is sometimes referred to as "universal interest" jurisdiction. Historically, universal interest jurisdiction was the right of any sovereign to capture and punish pirates. This form of jurisdiction recognises that a state has jurisdiction to define and prescribe punishment for certain offences recognised by the community of nations as of universal concern, such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and certain acts of terrorism.

\textsuperscript{394} At 1250.
4. **Application To The Internet**

4.1 *The Territoriality Principle*

The territoriality principle is the most common basis for the exercise of jurisdiction to prescribe, and it is generally uncontroversial. This principle would allow a State to order Internet Service Providers (ISPs) who operate within its territory to obey its regulations. It would further allow barring access to certain Web sites from machines operating within the State’s territory.

States rely on their sovereignty to control activities which happen in their territory even if these activities are not limited to the national territory, and even if control might be ineffective. Under international law, States may also incur international responsibility if they allow their territory to be used for unlawful activities directed against other States.

In a case against CompuServe, the Court held that German law was applicable to bar access for German users to certain news groups. The consequence of this was that German law dictated what citizens of other countries could read and view. This was caused by the inability of CompuServe to tailor its services to the laws of each country in which it operated.

---

395 29 F.3d 619 (1st Cir. 1994).
The territoriality principle would not permit extraterritorial application of national law. For example, a country could legally force a local service provider to comply with a regulation banning access of local users to certain content. However, this principle could not be relied on to remove the controversial content from the Internet in general.

The territoriality principle could also not be used to make Internet users responsible for the posting of material that people within other states could access. This is because Internet users have no way of determining the characteristics of their audience or their geographic location.

4.2  The Nationality Principle

The right of a State to regulate the conduct of its citizens or nationals anywhere in the world is also relatively uncontroversial.

In addition to the territoriality principle, ISPs may also be subject to jurisdiction under the nationality principle. For example, the German branch of CompuServe Inc. is chartered as a German company, and it is therefore subject to German law.

4.2.1 Determining nationality in cyberspace

The "law of the flag" from maritime law is difficult to apply in the context of cyberspace law. This is because when we seek to determine the nationality of the "ship" we find that we are unable to locate a tangible ship. The question then arises 'what carries nationality into cyberspace?'.

There is currently no registry in operation that registers files and messages with a particular nationality. Norms therefore have to be developed in order to attribute nationality. The nationality of materials could be determined by looking to the nationality of the person or entity that entered them into cyberspace. Alternatively, one could look to the nationality of the person or entity that controls the relevant material.

Following this analysis, a Web page could be attributed the nationality of the Web page creator, or the person or entity on whose behalf it is maintained. Links to Web pages would follow the same reasoning. The person who creates the link would be subject to their own national laws pertaining to links and to the content that may be uploaded. The person who follows the link is merely a downloader. They will be subject to the jurisdiction of the area where they are physically located at the time they access the content, as well as the laws of cyberspace that govern persons of their nationality. In this way the downloader is not expected to be aware of whether it was legal for the uploader to make the material available. The legality of the uploading would be based only on the uploader’s nationality and physical location at the
time of uploading. Similarly, the uploader’s state could not prescribe laws governing the downloader’s actions.

The following situation illustrates how this approach would work:

Person A, an American citizen, is commissioned to design a Web page for person B, a South African citizen. Person A uploads the Web page from America. The Web page, however, contains content that is prohibited by the Films and Publications Act. Person B could therefore be subject to prosecution by the South African authorities. Person A would also be subject to any American laws regulating uploading. In this way Person B could not avoid the South African laws simply by uploading from another jurisdiction. South Africa could not, however, try to regulate materials that are uploaded outside of its jurisdiction by persons of other nationalities, where there is no link to any South African citizen. It will not be enough that the material is downloadable from within South Africa.

Where the content enters cyberspace through an individual making use of bulletin boards, USENET groups, or e-mail, it will simply be a matter of determining the nationality of the individual person or entity.
4.3  *The Effects Principle*

The effects principle can be invoked when an act committed in one State causes injury in the territory of another State. Jurisdiction is grounded on the fact that the injurious effect occurred in the territory of the State. This principle may be controversial, particularly where the conduct was lawful where it was carried out.

Probably the first cyberspace case where the effects principle was invoked was *United States v. Thomas.*\(^ {398} \) The defendants operated a computer bulletin board system from their home in California containing images depicting bestiality, oral sex, incest, sadomasochistic abuse, and sex scenes involving urination. Access was limited to members who were given a password after they paid a membership fee and submitted a signed application form that requested the applicant's age, address, and telephone number. An undercover agent was accepted as a member and downloaded explicit material in Memphis, Tennessee. The defendants were indicted in a federal court in Tennessee on several criminal violations. The defendants challenged the venue in Tennessee, claiming that the criminal act (the transportation of the material) occurred in California, and not Tennessee. The Court held that "the effects of the Defendants' criminal conduct reached the Western District of Tennessee" and the defendants were accordingly convicted in Tennessee.

---

397 Act 65 of 1996.
It is not clear whether the downloading of files in a certain country makes the sender's activities subject to foreign jurisdiction. However, in the case of *United States v Thomas*, the defendants knew the jurisdiction in which their files were being accessed, and the downloading could not occur without their approval.

The case does not set a precedent for jurisdiction over a sender's activities based on the random downloading of files that happen to be illegal in certain jurisdictions.

*Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.*\(^\text{399}\) is the first published international case addressing multi-jurisdictional issues in cyberspace. A publisher offered and distributed sexually explicit photos through the Internet, from a Web site in Italy. Customers had to subscribe and pay a monthly fee. The publisher was therefore aware that the material was entering specific jurisdictions, including the United States. The court held that distribution of the materials in the United States was a violation of a fifteen-year-old American court order prohibiting the use of the trade mark, "Playboy" in magazines distributed in the United States.

The court analysed the scope of jurisdiction in Internet related matters, and found that:

"The Internet is a world-wide phenomenon, accessible from every corner of the globe. [Defendant] cannot be prohibited from operating its Internet site merely because the site is accessible from within one country in which its product is banned. To hold otherwise "would be tantamount to a declaration that this Court, and every other court throughout the world, may assert jurisdiction over all information providers on the global World Wide Web"."

Although the Court concluded that it could not prescribe conduct on the global Internet, it was entitled to prohibit access to the computer sites in the United States. The defendant was therefore enjoined from offering his magazine to customers residing in the United States.

Therefore, in accordance with international law, a State may limit the domestic effects of a Web site perceived as dangerous to its citizens. However, a State is not permitted to outlaw that activity completely, unless it has jurisdiction based on territoriality, nationality or universality.
4.4  *The Protective Principle*

International law recognises the right of a State to punish a limited class of offences committed outside its territory by persons who are not its nationals. These offences must be generally recognised as criminal by the international community.

This is the case for offences like espionage, counterfeiting of the State's seal or currency, or falsification of official documents. Furthermore, hackers who play "wargames" and intrude in national security data systems, or endanger the systems with worms or through other means, face subjection to the jurisdiction of the affected State.

States are authorised to prescribe rules to outlaw the above mentioned crimes in cyberspace. Expatriated citizens, and even aliens who oppose a certain regime, cannot be sure that participation in public news groups is not subject to regulation of their native State. This does not necessarily conflict with international human rights. On the contrary, Article 20 of the International Covenant of Civil and Political Rights of December 19, 1966 states:

1. Any propaganda for war shall be prohibited by law.

2. Any advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.
4.5  **The Universality Principle**

Universality provides for jurisdiction over a crime which customary or conventional law labels so egregious as to be of universal concern. Unlike the other principles of jurisdiction, universality does not require a direct connection such as the place of the offence, the nationality of the offender, or the effects of the offence on the prescribing State. Universal jurisdiction over the specified offences is a result of universal condemnation of those activities. It criminalises piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and certain acts of terrorism.

Under Article III of the Convention on the Prevention and Punishment of the Crime of Genocide of December 9, 1948, the following acts shall be punishable under the universality principle:

(a) Genocide;

(b) Conspiracy to commit genocide;

(c) Direct and public incitement to commit genocide;

(d) Attempt to commit genocide;

(e) Complicity in genocide.

This section would cover spam that gives rise to "[d]irect and public incitement to commit genocide."

---

5. **Jurisdiction To Adjudicate**

Jurisdiction to adjudicate is defined as a State's authority to subject persons or things to the process of its courts or administrative tribunals, whether in civil or in criminal proceedings, whether or not the State is a party to the proceedings. It requires a sufficient or reasonable relation with the forum State.

In international criminal cases, jurisdiction to adjudicate depends almost exclusively on presence of the accused.

In international civil cases, the principle of "*actor sequitur forum rei*"\(^{401}\) can be regarded as a universally accepted principle.

In the context of the Internet, it is submitted that a State would not have jurisdiction to adjudicate based solely on the existence of a Web site. Therefore, where spam directs recipients to a particular Web site, it would have to be established that the Web site was accessed by citizens of the forum state. The accessibility of a Web site within the state may also be an inadequate basis for jurisdiction. Jurisdiction may be denied where the only contact with the forum state is the location of a database that is used to generate the spam.
6. **Jurisdiction To Enforce**

Jurisdiction to enforce deals with a State's authority to induce or compel compliance or to punish non-compliance with its laws or regulations, whether through the courts or by use of executive, administrative, police, or other nonjudicial action.

Generally, a state may not enforce its rules unless it has jurisdiction to prescribe those rules. The mere existence of jurisdiction to prescribe, however, is insufficient to justify the state to exercise enforcement jurisdiction in another state's territory. Enforcement jurisdiction is linked closely to territory, but its limits are more strictly observed than is the case with jurisdiction to prescribe.

**PART B : THE CONCEPT OF "PLACE" ON THE INTERNET**

7. **Introduction**

It is difficult to give "place" a meaning on the Internet. In reality it makes little difference to users whether an e-mail originates from a next door neighbour or another country completely. It is of little significance to a user that political borders are in fact crossed. A user will visit a Web page on a server in America much the same as they would visit a Web page on a server in South Africa. The Internet ignores political boundaries, and so do its users.

---

401 Plaintiff follows defendant to the defendant's forum.
Although many Internet addresses use a two-letter extension after their domain name to link them to their physical location (for example co.za), it is possible to use a fictitious extension to falsify your true location. There is not necessarily a connection between an Internet address and its physical jurisdiction. A server with a ".co.za" domain name may not necessarily be located in South Africa, and a server with a ".com" domain name may be located anywhere in the world. Users accessing information are therefore often unaware of their ultimate digital destination, or all the countries their communications have travelled through to get there. "Physical borders no longer can function as signposts informing individuals of the obligations assumed by entering into a new, legally significant, place, because individuals are unaware of the existence of those borders as they move through virtual space".  

402

From the point of view of information distribution, on the other hand, all distribution is global. Access to information cannot be restricted to local access, since you generally cannot discriminate as to who can access your information on-line.

Traditional international law takes geographical location into consideration in determining the applicable law and jurisdiction. The problem with international law analysis on the Internet is that there is no "place". As the

---

United States Supreme Court put it, "[t]aken together, these tools constitute a unique medium – known to its users as ‘cyberspace’ – located in no particular geographical location but available to anyone, anywhere in the world, with access to the internet". 403

The United States Courts have adopted two different approaches to choice of law where Internet matters are concerned. One approach is to use the law of the plaintiff’s domicile or principal place of business to govern Internet disputes. In the case of Playboy Enterprises v Chuckleberry, 404 a trade mark case involving an American plaintiff and an Italian defendant, the law of the destination of the Internet transmission was applied. A similar approach was adopted in Compuserve v Patterson 405 (a trade mark dispute), and in U.S. v Thomas 406 (a pornography prosecution).

The opposite approach was adopted in the cases of Religious Technology Center v Lerma, 407 and Religious Technology Center v F.A.C.T.Net, Inc. 408 In these cases, the law of the defendant’s residence was adopted. In other words, it was the law of the place where the Internet transmissions originated that was applied.

405 89 F.3d 1257 (6th Cir. 1996).
406 74 F.3d 701 (6th Cir. 1996).
8. **Uploading And Downloading**

The public interacts with cyberspace either by putting information into cyberspace (uploaders), or by taking information from cyberspace (downloading). It is not necessary for the identities of the parties to be known, and there need not be any specific intent to communicate at all.

Activities of uploaders and downloaders do not necessarily present jurisdictional difficulties. "A state can forbid, on its own territory, the uploading and downloading of material it considers harmful to its interests. A state can therefore forbid anyone from uploading a gambling site from its territory, and can forbid anyone within its territory from downloading, i.e. interacting with a gambling site in cyberspace".\(^{409}\) Therefore, under international law, South Africa has the jurisdiction to prescribe law regulating the content of what is uploaded and downloaded from South African territory.

According to Darrel Menthe,\(^{410}\) a Web page would be ascribed the nationality of its creator. It would thus not be subject to the law of wherever it happened to be downloaded. Where uploading certain material is a crime, it would be an offence committed and consummated in the state where the uploader is located.

---

\(^{408}\) 901 F.Supp. 1519 (D.Colo. 1995).

Jurisdictional problems do, however, arise where states seek to exercise jurisdiction over uploaders outside their own territorial boundaries. In these instances, jurisdiction is founded merely on the fact that the information placed on the Internet was downloadable in the state in question. This is absurd, since it makes all of cyberspace subject to the law of that state. If every state adopted this approach, the result would be that every conceivable body of law would govern internet-related activities. Operating a Web site therefore does not mean that the operator is subject to personal jurisdiction in courts wherever the Web site is accessible.

9. **The Law Of The Server**

Another possible approach to jurisdiction in cyberspace is to treat the location of the server where the Web pages are physically located as the place of the activities.

This approach creates problems, however, where the uploader is in a foreign jurisdiction. When data is sent by an uploader to a server (regardless of the physical distance between them) it can travel in data packets through nodes around the world. It will therefore be sent and received through several

---


411 Judge Jeremy Fogel ruled in a U.S. District Court that Yahoo! Inc does not have to comply with a French order that it keep users in France from seeing Nazi-related content on the Web site. The court ruled that the First Amendment protects content generated in the United States by American companies from being regulated by authorities in countries that have more restrictive laws on freedom of expression.
jurisdictions en route. Territorialisation of cyberspace in this way would create chaos if it meant that an uploader would be subject to the jurisdiction of a state where a randomly assigned routing node held a packet of his data for merely an instant. "One of the challenges we find is that spam is global. A lot of it gets routed through and secure servers. So, as that happens, it outside of any one country's jurisdiction". 412

A further problem with assigning jurisdiction to the state where the server is located arises where the uploader and the server are in different states entirely. In order to apply the law of the state where the server storing the Web page is located, the act of uploading would have to have a substantial effect in the server’s state to warrant awarding jurisdiction.

If jurisdiction is based on the location of the server, the question arises: did the accesor travel to the server, or did the content travel to the accesor? Difficulties would also arise where parts of the Web page are called on from other servers through links.

It would be easy enough for a Web page designer to simply place any illegal materials on servers in other countries. If this content were to be placed on a large number of servers in various countries, however, it would be subject to the laws of all the countries concerned.

412 Enrique Salem, chief executive of Brightmail, in Kapadia "Spam Is Here To Stay"
Perhaps the most serious pitfall with looking to the location of the server is the fact that the uploader and downloader do not necessarily know who the other party is. The interaction between them is often completely random and anonymous. Persons could thus be held liable for criminal activities without knowing what set of laws apply to their actions.

There could not realistically be any meaningful control of material in this way, because individual electrons can enter countries undetected, and the sheer volume of electronic communications crossing territorial boundaries is too great.

PART C : DISPUTES WITH A TRANSNATIONAL CHARACTER

10. Introduction

Traditional international law will have to be adapted to deal with Internet related matters. Often there are no clear "non-virtual world" parallels that can be drawn with the new rules and unprecedented phenomena that have emerged in the on-line world. Asking where activities in fact occurred is possibly not the correct enquiry with disputes of this nature. However, the question is still what law to apply, and which court has jurisdiction.

International law dictates what laws apply, and which courts have jurisdiction in disputes of a transnational character. This, however, is based on the assumption that geographical borders are of primary importance in determining legal rights and responsibilities.

Where Internet law disputes are concerned, there are four potential approaches that may be adopted, namely:

a) unify the choice of law rules;
b) unify a substantive law of the Internet;
c) harmonise the laws of different jurisdictions; or
d) recognise the Internet as a jurisdiction in its own right.

10.1 *Unify The Choice Of Law Rules*  
Choice of law for Internet disputes is an issue that will need to be addressed. Clear choice of law methods will prevent forum shopping, inconsistent obligations, and uncertain courts.

Unifying choice of law methods is the least extreme approach. It involves unifying the rules by which we choose which law will be applicable to Internet-related disputes. Generally applicable rules are articulated to decide which national law will apply when these disputes arise. It could, for instance, be the domicile of either the plaintiff or the defendant that would
govern the matter. Alternatively, the domicile of the party that originates the communication could apply. These rules must be clear and easy to apply. They could be applicable either by convention, or by following the opinion of a special advisory body. A. Gigante has drafted a proposed International Agreement on Internet Law\footnote{Gigante "Ice Patch On The Information Superhighway", Cardozo Arts & Ent. L.J. (1996) volume 14 at page 523.} that lays down a unified rule for choosing law for Internet disputes.\footnote{Gigante "Ice Patch On The Information Superhighway", Cardozo Arts & Ent. L.J. (1996) volume 14 at page 523.}

10.2 Unify A Substantive Law Of The Internet

This approach has the advantage of eliminating choice of law problems altogether, since the parties will simply turn to a separate body of law, namely "Internet law". A further advantage of this approach is that the law would be capable of keeping up with rapid technological advances in this area. It would be able to respond and adapt easily to technical and legal changes. This approach would also create certainty among users, ISPs, and courts, and a single body of jurisprudence will emerge, since all Internet matters will be governed by the same rules.

In order to unify a substantive law of the Internet, we could either draft international treaties or agreements, or we could simply allow courts to develop a "common law" of the Internet.
10.3 Harmonise The Laws Of Different Jurisdictions

International law treaties are the most effective way to harmonise the laws of different jurisdictions. The United Nations Commission of International Trade Law (UNCITRAL) Model Law on Electronic Commerce is an example of an attempt towards the unification of a substantive Internet law. Nations could agree on a set of new rules and common standards of practice with respect to Internet-related issues.

The drawback of this idea, however, is that nations may not be willing to allow disputes involving their citizens to be decided according to a body of law that may conflict in some instances with their own national laws. Economic and political interests are likely to hinder progress in this direction.

10.4 Recognise The Internet As A Jurisdiction In Its Own Right

The Internet has resulted in the total dissolution of geographical boundaries, national borders and communication barriers. "Because the Internet does not map neatly into the jurisdiction of any existing sovereign entity, territorality defined laws and rules are difficult to apply to the Internet and activities of Internet users".\textsuperscript{415}

\textsuperscript{414} For example, in 1994 UNIDROIT issued the General Principles of International Commercial Contracts, available at \url{http://www.unidroit.org/english/principles/pr-main.html} (1 October 2004).

\textsuperscript{415} Almaguer and Baggot "Shaping New Legal Frontiers: Dispute Resolution For The Internet" \textit{Ohio State Journal on Dispute Resolution} (1998) volume 13 at page 712.
If the Internet were to be recognised as a jurisdiction in its own right, Internet disputes could be referred to an international Internet Arbitration Board, or a special court, that deals exclusively with Internet related disputes. Inconsistent obligations and results in Internet cases could be avoided by taking disputes away from regular courts and referring them to special Internet courts.

PART D : CONCLUSION

The solution to effectively combat spam appears to be to harmonise the laws of different jurisdictions. Continuing globalisation of markets, and increased interaction between individuals in different geographical areas has necessitated increased co-operation between governments. Eventually, consistent laws governing the Internet will need to be developed.
CHAPTER 6
CONSTITUTIONAL CONCERNS

1. Introduction

Many of the objections to spam relate to its content. Most users object to receiving email containing sexually explicit material or racist remarks, and are often offended by such messages. Since the potential of the Internet as a mass communication medium is immense, the question that arises is whether governments should attempt to censor and regulate material that is disseminated through the Internet.

This chapter discusses constitutional concerns that may arise in the context of spam. Part A discusses the right to freedom of expression including various instances where the right to freedom of expression must be balanced against competing rights and values.

Part B looks briefly at the right to privacy and discusses United States case law illustrating the restriction on the right to freedom of expression in favour of the right to privacy.

Finally, Part C provides a general conclusion for the present Chapter.
PART A: FREEDOM OF EXPRESSION

2. Introduction

The rights contained in the Bill of Rights must be read, interpreted and understood in the light of other competing and potentially conflicting rights, which are also constitutionally protected, such as the rights to equality, dignity and privacy. There is no hierarchy of rights in the Bill of Rights. Therefore, when a clash occurs between competing rights, the circumstances of each case must be examined.\(^{416}\)

Our courts often refer to foreign comparative law to illustrate the application of legal principles. Section 39(1)(c) of the Constitution supports this approach in providing that "when interpreting the Bill of Rights, a court, tribunal or forum may consider foreign law". A discussion of United States law on the right to freedom of expression has therefore been included to give an indication of the approach adopted by other Western democratic societies.

3. The Constitution

3.1 The Right To Freedom Of Expression

The right to freedom of expression and communication is protected in section 16 of the Constitution of the Republic of South Africa\(^{417}\) (the Constitution).

\(^{416}\) *Van Zyl v Jonathan Ball Publishers (Pty) Ltd* 1999 (4) SA 571 (W).

\(^{417}\) Act 108 of 1996.
Section 16(1) provides that:

"Everyone has the right to freedom of expression, which includes-

(a) freedom of the press and other media;

(b) freedom to receive or impart information or ideas; . . ."

3.2 *Specifically Excluded Forms Of Expression*

Spam that contains propaganda for war, incitement of imminent violence, or advocacy of hatred that it is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm is specifically excluded from constitutional protection in terms of Section 16(2) of the Constitution.

3.3 *Horizontal And Vertical Application*

The traditional approach is that a Bill of Rights has vertical application only, to protect the individual from the abuse of state power: "Traditionally bills of rights have been inserted in Constitutions to strike a balance between governmental power and individual liberty; to constitute a precaution against state tyranny".\(^{418}\)

\(^{418}\) *De Klerk v Du Plessis* 1995 (2) SA 40 (T) at 47.
However, in South Africa, the Constitution has horizontal and vertical application: In *Mandela v Falati*, Van Schalkwyk J held that the constitutional right of freedom of expression had horizontal application.

### 3.4 Limitation Of The Right To Freedom Of Expression

Freedom of expression is recognised as being absolutely central to democracy in most democratic societies. However the right to freedom of expression is not absolute.

In South Africa, the right to freedom of expression is subject to the limitation clause set out in section 36. Under section 36(1), the rights entrenched in Chapter 2 may be limited by law of general application, to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.

When dealing with the criteria prescribed by s 33(1) of the 1993 Constitution, Chaskalson P in *S v Makwanyane and Another* stated:

"The limitation of constitutional rights for a purpose that is reasonable and necessary in a democratic society involves the weighing up of competing values, and ultimately an assessment based on

---

419 1995 (1) SA 251 (W).
421 Corresponding to s 36(1) of the 1996 Constitution.
proportionality. This is implicit in the provisions of s 33(1). The fact that different rights have different implications for democracy and, in the case of our Constitution, for "an open and democratic society based on freedom and equality", means that there is no absolute standard which can be laid down for determining reasonableness and necessity. Principles can be established, but the application of those principles to particular circumstances can only be done on a case-by-case basis. This is inherent in the requirement of proportionality, which calls for the balancing of different interests. In the balancing process the relevant considerations will include the nature of the right that is limited and its importance to an open and democratic society based on freedom and equality; the purpose for which the right is limited and the importance of that purpose to such a society; the extent of the limitation, its efficacy and, particularly where the limitation is to be necessary, whether the desired ends could reasonably be achieved through other means less damaging to the right in question. In the process regard must be had to the provisions of s 33(1) and the underlying values of the Constitution."

Therefore, the right to freedom of expression will have to be weighed against other rights and interests and our courts will have to evaluate the value that is to be placed on freedom of expression and the extent to which other rights and interests should be subordinated.

422 1995 (3) SA 391 (CC) at paragraph 104.
4. **Comparison With The United States**

The First Amendment to the Constitution of the United States of America states:-

"Congress shall make no law ... abridging the freedom of speech".

In the United States, the Bill of Rights has vertical application, and therefore applies to state action only. Therefore, the First Amendment constrains what the state may and may not do, but it does not directly apply to the private sector.

Unlike our Constitution, the Bill of Rights of the United States does not contain a limitations clause, and the First Amendment is therefore not subject to textual limitation. Instead, justifiable limitations upon freedom of speech have had to be fashioned by United States Courts on the basis of implied constitutional purpose and structure.\(^{423}\) Therefore, the First Amendment is similarly not regarded as absolute and it does not afford unlimited protection to freedom of speech.

5. The Right To Freedom Of Expression Under International Law

The right to freedom of expression is recognised under Article 10 of the European Convention on Human Rights: \(^42^4\)

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers...

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society … for the protection of the reputation or the rights of others…".

Therefore, while the Convention recognises the right to freedom of expression, it also recognises that this right carries with it duties and responsibilities, and that the rights and reputation of others also require protection.

6. Commercial Speech

The value of commercial speech and the scope of the constitutional protection that should be afforded to it has vexed our courts. Spammers

present the argument that electronic advertising, like any other form of advertising, is protected commercial speech, implying that it is their democratic right of free speech to send spam. In other words, spammers argue that they have the constitutional right to commercial expression.

However, freedom of speech is not applicable all the time: advertisers are limited in what they can say on billboards and in television advertisements. Advertising by e-mail will have similar rules, since freedom of speech relates to the content of the speech, and not to the method of its distribution.

Generally speaking, when dealing with commercial speech the motive for imparting information is pure economic gain. If advertisers are restrained from imparting this information, their loss is simply a loss of profits. Therefore, restrictions of this kind of easier to justify than other infringements.

South African constitutional jurisprudence has, effectively, confirmed the protection of advertising as a form of commercial speech.

In North Central Local Council And South Central Local Council v Roundabout Outdoor (Pty) Ltd And Others the Court held that since section 16 of the Constitution had been interpreted to include speech

represented in the form of advertising, advertising was a constitutionally protected form of commercial speech.

Further, in *City of Cape Town v Ad Outpost (Pty) Ltd and Others*, Davis J held that it is clear that advertising falls within the nature of expression and thus needs to be protected by section 16(1) of the Constitution. The Court held that:

"The tendency to conclude uncritically that commercial expression bears less constitutional recognition than political or artistic speech needs to be evaluated carefully. So much speech is by its very nature directed towards persuading the listener to act in a particular manner that artificially created divisions between the value of different forms of speech requires critical scrutiny".

The Court held further that it was clear that advertising falls within the nature of expression and hence stood to be protected in terms of section 16(1) of the Constitution. To the extent that its value might count for less than other forms of expression, account of this exercise in valuation had to be taken at the limitation enquiry envisaged in s 36 of the Constitution.

---

426 2002 (2) SA 625 (D) at 633D.
427 2000 (2) SA 733 (C).
428 At page 749.
The Court in *S v Makwanyane and Another*\(^{429}\) highlighted the fact that "different rights have different implications for democracy". There are elements of a right that constitute its core values and others that are at the periphery of protection. The core values require exacting standards before their violation may be justified, whereas the peripheral values are afforded lesser protection.

According to Marcus and Spitz,\(^{430}\)

"Commercial expression has been defined as speech which proposes a commercial transaction. This area of expression relates primarily to commercial advertising of goods or services for profit, but is wide enough to include expression in the context of unlawful competition, including disparagement and economic trade boycotts. Most, but not all, commercial expression is at some remove from the core of freedom of expression and is best located within the protected periphery of the guarantee".

Therefore, while commercial expression is protected under section 16 of the Constitution, it would appear that this form of expression is considered to be at the periphery of the value and may be afforded lesser protection. The limitation enquiry envisaged in section 36 of the Constitution would have to examine the extent to which commercial spam has a lesser value than other

\(^{429}\) 1995 (3) SA 391 (CC) at paragraph 104.
forms of expression, and any restrictions on spamming activities would have to be a reasonable and justifiable limitation on free expression in terms of the limitation clause\(^{431}\) of the Constitution.

6.1 \textit{The United States}

In America a reduced level of constitutional protection is extended to commercial expression. The United States does not, however, afford constitutional protection to false or misleading commercial speech.\(^{432}\)

The United States Supreme Court first extended First Amendment protection to pure economic advertising in the case of \textit{Virginia State Board of Pharmacy v Virginia Citizens Consumer Council}\(^{433}\). The Court stated that the dissemination of commercial information through advertising performs important public interest functions of ensuring the free flow of information indispensable to proper resource allocation in a free market.

\begin{footnotesize}
\begin{itemize}
\item[]\(^{431}\) Section 36.
\item[]\(^{432}\) Chaskalson et al \textit{Constitutional Law of South Africa} (1996) at 20-51.
\item[]\(^{433}\) 425 US 748 (1976).
\end{itemize}
\end{footnotesize}
In *Central Hudson Gas and Electric Corp v Public Service Commission of New York*,\(^{434}\) while the Court recognised the right to freedom of commercial expression, it also considered the limitation of that right:

"The Commission's order restricts only commercial speech, that is expression related solely to the economic interests of the speaker and its audience. The First Amendment … protects commercial speech from unwarranted governmental regulation. Commercial expression not only serves the economic interest of the speaker, but also assists consumers and furthers the societal interest in the fullest possible dissemination of information".

The Court continued:\(^{435}\)

"Nevertheless, our decisions have recognized "the 'commonsense' distinction between speech proposing a commercial transaction, which occurs in an area traditionally subject to government regulation, and other varieties of speech. The Constitution therefore accords a lesser protection to commercial speech than to other constitutionally guaranteed expression. The protection available for particular commercial expression turns on the nature both of the expression and of the governmental interests served by its regulation".


\(^{435}\) At 562.
The Court held\textsuperscript{436} that provided the commercial speech concerns lawful activity which is neither false, deceptive or misleading, regulation of such speech will be upheld if the governmental interest in regulating the commercial speech is substantial, if the regulation directly advances that governmental interest, and if it does so in a manner that is no more extensive than necessary to serve the governmental interest.

"The essential rule that resulted from Central Hudson is that while the government cannot regulate an advertisement's content, it can and does regulate the form in which an advertiser communicates that content to potential customers".\textsuperscript{437}

7. \textbf{Defamation}

Defamation may be defined as the unlawful, intentional publication of defamatory matter referring to the plaintiff, which causes his or her reputation to be impaired.\textsuperscript{438}

\textsuperscript{436} At 564.
\textsuperscript{437} Moorefield "SPAM – It's Not Just For Breakfast Anymore: Federal Legislation And The Fight To Free The Internet From Unsolicited Commercial EMail" Boston University Journal of Science and Technology Law volume 5 at page 10.
The law of defamation seeks to protect a person’s right to an unimpaired reputation or good name by means of the actio iniuriarum. It seeks to find a balance between the individual’s right to reputation or good name with the right of others to freedom of expression.  

This common law right is also entrenched in section 10 of the Constitution, which provides for the right to human dignity. Therefore, notwithstanding the fact that freedom of expression is a fundamental right protected by Chapter 2 of the Constitution, it does not follow that section 16(1) may necessarily be relied upon as a defence in a defamation action. A balancing of these two values would have to take place in terms of the limitation clause set out in section 36.

In Kauesa v Minister of Home Affairs & Others it was held (in relation to the Namibian Constitution) that in so far as the law of defamation infringes freedom of speech and expression, that infringement is reasonable and necessary in a democratic society and therefore constitutional and binding.

A similar conclusion was reached in Mandela v Falati, where Van Schalkwyk J commented that the right to freedom of speech could not be allowed to prevail in every situation in which it came into conflict with the right

---

439 See further Chapter 3 for a discussion of the common law of defamation in South Africa.
440 1995 (1) SA 51 (Nm).
441 1995 (1) SA 251 (W) at 259 F-G.
of human dignity (including the right to an unsullied reputation): to allow freedom of speech to override the right of human dignity in every case would be to abrogate the law of defamation, and would violate the provisions of section 33(1) of the 1993 Constitution.\(^{442}\)

In *Gardener v Whitaker*,\(^{443}\) Froneman J held that since the right to human dignity set out in section 10 of the 1993 Constitution\(^{444}\) had to be interpreted to include the right to one’s good name or reputation, the plaintiff in a defamation action would be relying on a fundamental right in bringing a defamation claim, while a defendant who pleaded section 15 would be relying on the competing fundamental right of freedom of speech in defending the action. Since the Constitution created no hierarchy of rights, but placed the right to reputation on an equal footing with the right to freedom of speech and expression, it seemed reasonable to require the plaintiff who sought to rely on the presence of one fundamental right over another to bear the onus of establishing that the right relied upon by him or her ought in the circumstances to prevail over the competing right of freedom of speech.

In *Khumalo And Others v Holomisa*\(^{445}\) the Court held that “although freedom of expression is fundamental to our democratic society, it is not a paramount value. It must be construed in the context of the other values enshrined in

\(^{442}\) Corresponding to section 36(1) of the 1996 Constitution.

\(^{443}\) 1995 (2) SA 672 (E).

\(^{444}\) Corresponding to section 10 of the 1996 Constitution.

\(^{445}\) 2002 (5) SA 401 (CC) at page 417 paragraph 25.
our Constitution. In particular, the values of human dignity, freedom and equality".

The Court continued: "The law of defamation seeks to protect the legitimate interest individuals have in their reputation. To this end, therefore, it is one of the aspects of our law which supports the protection of the value of human dignity. When considering the constitutionality of the law of defamation, therefore, we need to ask whether an appropriate balance is struck between the protection of freedom of expression on the one hand, and the value of human dignity on the other".\(^{446}\)

On the above it may be concluded that while a spammer has the right to freedom of expression, this freedom does not extend to defamatory statements, and the law of defamation could potentially be invoked where the spam contains defamatory material.

7.1 The United States

In \textit{Cubby Inc v Compuserve Inc},\(^{447}\) CompuServe made a newsletter available to its subscribers called "Rumourville USA", a daily newsletter that provides reports about broadcast journalism and journalists. The newsletter was published by a company called Don Fitzpatrick Associates, and placed on the

\(^{446}\) At page 419 paragraph 28.  
\(^{447}\) Available at \url{http://www.epic.org/free_speech/cubby_v_compuserve.html} (18 May 2004).
CompuServe network by a company called Cameron Communications, Inc. (CCI). CCI was contracted to "manage, review, create, delete, edit and otherwise control the contents" of the Journalism Forum "in accordance with editorial and technical standards and conventions of style as established by CompuServe". Therefore, CCI were contractually responsible for editing and controlling the content of the newsletter.

One of the publications contained false and defamatory statements relating to Cubby. CompuServe did not dispute that the statements were defamatory, but argued that it acted as a distributor, and not a publisher, of the statements, and could not be held liable for the statements because it did not know and had no reason to know of the statements. CompuServe had no opportunity to review the contents of the publication before it was uploaded into its computer data banks.

The Court ruled that CompuServe could not be held liable for information in a newsletter it did not originally publish. The Court held that computer databases are the equivalent of news stands or book stores, whose owners cannot be held liable for the content of the papers they sell unless they know beforehand that the stories are false:

"CompuServe has no more editorial control over such a publication than does a public library, bookstore or news stand, and it would be no more feasible for CompuServe to examine every publication it carries for
potentially defamatory statements than it would be for any other distributor to do so”.

This case is important, because it illustrates that where a spammer sends defamatory material, an action for defamation will lie only against the spammer and not against the ISP that carries the material.

8. **Pornography**

The provisions of the Films and Publications Act\(^4\) prohibit the distribution of child pornography, explicit violent sexual conduct, bestiality, explicit sexual conduct which degrades a person and which constitutes incitement to cause harm or explicit infliction of extreme violence.\(^5\)

The Films and Publication Act was amended by the Film and Publications Amendment Act\(^6\) to bring Internet material within its ambit. The definition of "publication" now includes the words "any message or communication, including a visual presentation, placed on any distributed network, including, but not confined to, the Internet".

---

\(^4\) Act 65 of 1996.  
\(^5\) These types of publications are classified under Schedule 1 of the Act as "XX" publications. Sub-sections 25-30 of Chapter 7 prohibit conduct in relation to publications classified as XX, including distribution, possession and exhibition.  
\(^6\) Act 34 of 1999.
Therefore, spam containing pornographic material, or directing users to pornographic Web sites would fall under the ambit of the Films and Publications Act, and would not be protected under the right to freedom of expression.

9. **Cost shifting**

The right to freedom of expression may be limited in the case of spam on the basis that the exercise of expression involves a shifting of costs onto the recipient.

9.1 *State of Missouri v. American Blast*

In the case of *State of Missouri v. American Blast* the Court held that a law limiting junk faxes did not infringe the First Amendment.

The State of Missouri sued American Blast Fax, Inc. and Fax.com, Inc. for violating statutory restrictions on unsolicited fax advertising. The fax companies argued that this was an unconstitutional restriction on their freedom of speech. On appeal, the court concluded there is a substantial governmental interest in protecting the public from the cost shifting and interference caused by unwanted fax advertisements, and the means chosen

---

451 United States Court of Appeals for the Eighth Circuit - Nos. 02-2705/2707.
452 Missouri alleged that they had violated the provisions of the Telephone Consumer Protection Act of 1991 making it unlawful "to send an unsolicited advertisement to a telephone facsimile machine".
by Congress to address these harms directly and materially advances the governmental interest.

Part of the decision was an acceptance that the junk-fax law fairly attempted to fight the practice of "cost-shifting," in which the cost for advertisements is borne by the recipients in the form of tied-up phone lines, paper, ink, and toner.

Because anti-spam activists make similar arguments for restricting unsolicited email advertisements, many see the approval of the fax law as support for anti-spam forces. Anti-spam activist Ray Everett-Church said the ruling "reinforces the argument that ... federal regulations banning unsolicited e-mail could be held constitutional". 453

PART B : THE RIGHT TO PRIVACY

10. Introduction

As discussed above, the rights contained in the Bill of Rights must be read, interpreted and understood in the light of other competing and potentially conflicting rights, which are also constitutionally protected. The right to freedom of expression must therefore be balanced against other competing rights and values, including the right to privacy.
11. The Constitution

11.1 The Right To Privacy

Section 14 of the Constitution guarantees a general right to privacy by providing that:

"Everyone has the right to privacy, which includes the right not to have

e) their person or home searched;

f) their property searched;

g) their possessions seized; or

h) the privacy of their communications infringed".

In terms of section 39 of the Constitution, when interpreting the Bill of Rights, the values which underlie an open and democratic society based on human dignity, freedom and equality, should be promoted. This is analogous to the test in the law of delict of ascertaining the boni mores or legal convictions of the community.

454 The South African law of privacy is more fully discussed under Chapter 3 above.
11.2 *Balancing Of Fundamental Rights*

The constitutional right to privacy is, like its common law counterpart, not an absolute right. It may be limited in terms of a law of general application and has to be balanced with other rights entrenched in the Constitution. Consideration must be given to other competing interests and protecting the rights, freedoms and interests of others. The right to privacy may conflict with the right to freedom of expression, and this will involve a balancing of fundamental rights.

Marcus and Spitz\(^ {455} \) pose the questions:

"To what extent may private property owners exercise their common-law right to determine what forms of expression are permissible on their property? Conversely, do speakers have any right to express themselves on private property without the consent of the owner?"

12. *Privacy Under International Law*

International law recognises the importance of the protection of privacy. The right to privacy is found in Article 12 of the Universal Declaration of Human Rights of 1948,\(^ {456} \) Article 17 of the International Covenant of Civil and

\(^ {455} \) Marcus and Spitz in Chaskalson et al *Constitutional Law of South Africa* (1996) at 20-55.

Political Rights, and Article 8(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

It is interesting to note that the African Charter on Human and People's Rights does not make any reference to privacy rights.

The Organisation for Economic Co-operation and Development ("OECD") has also published Guidelines on the Protection of Privacy and Transborder Flows of Personal Information. These guidelines represent an international consensus on how best to balance effective privacy protection and management with the free flow of personal data. The Guidelines set out core principles and play a major role in assisting governments, business and consumer representatives in their efforts to protect privacy and personal data, and avoid unnecessary restrictions to trans-border data flows, both online and offline. The Guidelines also serve as the foundation for privacy protection at a global level.

---


13. **The United States**

Several United States cases have held that there is no First Amendment right to send bulk e-mail.

13.1 *Rowan v U.S. Post Office Dept*

In *Rowan v U.S. Post Office Dept*,\(^{461}\) the United States Supreme Court observed that:

"Nothing in the Constitution compels us to listen to or view any unwanted communication, whatever its merit. The ancient concept that 'a man's home is his castle' into which 'not even the king may enter' has lost none of its vitality. We therefore categorically reject the argument that a vendor has a right under the Constitution or otherwise to send unwanted material into the home of another. If this prohibition operates to impede the flow of even valid ideas, the answer is that no one has a right to press even 'good' ideas on an unwilling recipient. That we are often 'captives' outside the sanctuary of the home and subject to objectionable speech and other sound does not mean we must be captives everywhere. The asserted right of a mailer, we repeat, stops at the outer boundary of every person's domain."

\(^{461}\) 397 U.S. 728 May 4, 1970.
In upholding a Postal statute that allowed a homeowner to instruct the Postmaster to order the sender of unwanted mail to remove the recipient’s name from a mailing list, the Court held that the "right to communicate must stop at the mailbox of an unreceptive addressee". The Court held that the government may help individuals stop junk mail by putting in place regulations that assist them, as long as the choice of which mail to stop is left to the individual and not government.

This case may similarly applied in the case of spam to reject the argument that a spammer has a right to send unwanted material to others and to support the notion that spammers may be directed to remove user addresses from their mailing lists.

13.2  *CompuServe Inc. v Cyber Promotions*

*CompuServe Inc. v Cyber Promotions* was one of the earliest cases in which an ISP alleged trespass against a spammer. CompuServe informed the defendant, Cyber Promotions, that it was prohibited from sending its e-mail advertisements to CompuServe’s subscribers. Cyber Promotions instead increased the number of e-mail advertisements that it sent to CompuServe customers. CompuServe then attempted to block Cyber Promotions from sending the e-mail

---

advertisements, but Cyber Promotions responded by changing its methods and continued to gain access to CompuServe’s equipment and subscribers.

CompuServe sought an interdict against Cyber Promotions, alleging that Cyber Promotions’ actions constituted trespass. Cyber Promotions on the other hand argued that they had the right to send the electronic mail to its subscribers.

The Court disagreed with Cyber Promotions and granted relief to CompuServe. The Court held that trespass is "intentionally using or intermeddling with the chattel in possession of another", whereby intermeddling is "intentionally bringing about a physical contact with the chattel".

The Court held that a physical dispossession is not required in a showing of trespass. The Court found that there was liability simply because the actions of Cyber Promotions, through its mass electronic mailings, "demand[ed] the disk space and drain[ed] the processing power of plaintiff’s computer equipment" thereby prohibiting its availability to CompuServe’s subscribers.

463 CompuServe is one of the larger ISPs.
Therefore, the Court held that:

"Defendants’ intentional use of plaintiff’s proprietary computer equipment exceeds plaintiff’s consent and, indeed, continued after repeated demands that defendants cease. Such use is an actionable trespass to plaintiff’s chattel. The First Amendment to the United States Constitution provides no defense for such conduct."

13.3  *Cyber Promotions Inc. v America Online Inc*

In *Cyber Promotions Inc. v America Online Inc*\(^{464}\) the Court similarly held that spam is not protected under the First Amendment:

"Cyber has no right under the First Amendment to the United States Constitution to send unsolicited e-mail".

The Court held that Cyber Promotions had alternative ways of sending advertising to AOL members, including non-Internet avenues, such as United States mail and traditional marketing media.

**PART C : CONCLUSION**

The sending of spam involves a weighing up of fundamental rights and values, and any limitation on the right to freedom of expression would have to be considered in terms of the limitations clause of the Constitution. It is

\(^{464}\) 96-2486, November 4, 1996.
submitted, however, that as the Court held in the *Cyber Promotions*\textsuperscript{465} case, there are numerous other methods of communication available, including non-Internet avenues, such as traditional "snail mail" and other traditional marketing media, and therefore restrictions on spamming activities may be easily justifiable.

\textsuperscript{465} 96-2486, November 4, 1996.
1. Introduction

A number of alternatives to legislation have been suggested to combat the problem of spam. However, all of these alternatives have proven to be somewhat ineffective in practice. It appears that the solution to the spam problem lies in the co-ordination of these alternatives.

"Microsoft firmly believes that spam can be dramatically reduced, and that the solution rests squarely on the shoulders of industry and government. There is no silver-bullet solution to the problem. Rather, we believe that fully addressing this problem for the long-run requires a co-ordinated, multi-faceted approach that includes technology, industry self-regulation, effective legislation, and targeted enforcement against the most egregious spammers."  

In terms of technology, the industry is developing better filters and is investing heavily in research and development. Filtering technologies are being developed that are easier for consumers to use and are more effective in determining which e-mail messages are spam and which are desired.

---

466 Microsoft "Letter From Bill Gates To The U.S. Senate Commerce Committee Regarding Spam Hearings" available at
communications. This differentiation will greatly reduce the risk of falsely misidentifying legitimate email as spam. Lessig\textsuperscript{467} also suggests that the "architecture" of cyberspace - its code - may act as a kind of regulator.\textsuperscript{468} However, technology is not the only answer. Effective and complementary self-regulation efforts by the industry are also essential.

Self-regulation efforts by the industry would involve the advertising industry and Internet Service Providers. Specifically, independent authorities around the globe could develop industry best practices.

In order for technology and self-regulation efforts to be successful, they need to be supported by strong legislation that prohibits spam, especially fraudulent and deceptive spamming practices, and empowers consumers without threatening legitimate e-commerce. This is discussed in chapter 3 of this report.

Finally, consumer awareness will play an important role in complementing the various approaches to eliminate spam.

\textsuperscript{467} Lessig \textit{Code} (1999) at page 6.

\textsuperscript{468} In other words, the hardware and the software that make up cyberspace may be designed to enable better regulation of behaviour in Cyberspace, for example by creating architectures of identification and authentication.
This Chapter discusses the current and proposed solutions to the spam problem. It focuses specifically on self regulation, technology and consumer awareness. Legal countermeasures are discussed above in Chapter 3.

Part A deals with self-regulation, and the role of the advertising industry and the role of Internet Service Providers is explored. In examining various technical approaches in Part B, individual user solutions and third party solutions are discussed, including filters and blacklists. Government intervention is proposed along the lines of the United States FTC email address. The implementation of various header labels is also discussed. In Part C, the role of consumer awareness in protecting against spam is emphasised. Finally, Part D provides a general conclusion for the present Chapter.

PART A: SELF REGULATION

2. Introduction

In the early stages of the Internet, social pressures were predominantly used to control Internet abuses. Internet governance as a whole was largely informal, and informal rules of Internet etiquette or “netiquette” and acceptable use policies prohibited or discouraged abuses of Internet

---

resources. The social stigma attached to spam was enough to discourage Internet users from engaging in such an activity. 470

As commercial activities have become generally accepted on the Internet and have overtaken the volume of academic and research usage, industry groups representing marketers and ISPs have attempted to address the spam problem with self-regulatory efforts. Industry stakeholders have been encouraged to deal with spam through voluntary industry-wide codes and practices. Various advertising and marketing associations have established codes and guidelines dealing with Internet use for the distribution of promotional materials. ISP associations have also developed voluntary codes based on good practices.

3. The Role Of The Advertising Industry

"Advertising may be described as the science of arresting the human intelligence long enough to get money from it." - Unknown 471

3.1 Introduction

Advertising plays a valuable role as a source of information for the consumer. Without advertising consumers would not know what was available or where

470 Spam did not represent a significant problem until the mid-1990’s, although it was recognised as a potential problem in 1978 when a marketer at the Digital Equipment Corporation (DEC) spammed ARPAnet users about new DEC products. See Chapter 2 above.

471 Unlimited Freedom of Speech home page available at
to get it. Advertising plays an important role in the development of new technology, new ideas and new products. Advertising also tends to keep prices down by stimulating competition.

Advertising is so common that it has become the background noise to our lives. However, in their effort to get us to buy their products and services, advertisers are becoming more and more intrusive. There is growing resentment that consumers are being targeted by advertising for products they don’t want and don’t need.

The Internet has become a popular advertising medium for the obvious reason that over 20 million people can be reached via the Internet. It allows for the full range of advertising techniques to be transmitted through a faster and more efficient means of reaching a larger consumer base than alternative and conventional methods.

The Internet has also become popular because the bulk of the cost of advertising on the Internet is borne by the recipient of advertising material, and not by the advertiser himself. Computer technology allows for the collection and collation of information about the individual consumer and can


Forrester Research forecasts that traditional US companies will spend $63 Billion annually by 2005 on Internet advertising, compared to the $11 Billion spent in 2002.
assist marketers reach their target market. However, for all these reasons, this medium of advertising is also open to abuse.

Since most of the costs of Internet advertisements are shifted onto the recipients, many advertisers engage in mass spamming. This use of the Internet to send large volumes of email in a totally indiscriminate fashion to promote products and services has infuriated many consumers, forced employees in organisations to waste time deleting junk email, strained the facilities of Internet service providers, and hurt the business of legitimate Internet marketers. Computer technology is used to randomly target consumers, irrespective of whether these consumers fall within the advertisers' target market. "Spam has become a symbol of consumer frustration with cannon-blast marketing that intrudes in their lives and offers them little in the way of incentives".474

Response rates for spam are negligible compared to other forms of direct marketing. "It is a singularly ineffective method of direct marketing, but for the fact that few of the costs involved are incurred by the spammers themselves".475 Spam is making legitimate commercial communication through email increasingly difficult because of its volume and consumers'

negative attitude towards spam. However, while spam continues to be a nuisance, it cannot be ignored that a targeted email message can be very effective. E-mail can be a valuable marketing tool where it is used correctly.

3.2 The Control Of Advertising

It is necessary to control unacceptable advertising, because a few offenders can hamper the functioning of the market system, harm or insult consumers, and reduce the overall credibility of advertising. Regulation is essential because it gives advertising credibility and the reputation necessary in order to fulfil its marketing function.

The legal framework that exists in South Africa to control advertising is a mixture of the common law and legislation, with substantial reliance being placed on the self-regulatory system based on the South African Code of Advertising Practice (the Code) administered by the Advertising Standards Authority (ASA).

According to Michael Judin, "the Advertising Standards Authority self-regulates one of South Africa's most dynamic industries with a living, breathing code that is updated on an annual basis. This has set a very good

---

476 According to the Interactive Advertising Bureau, an online trade association, Internet advertising revenue in the United States totalled $1.5 billion for the first quarter of 2002, declining 6.5 percent from the fourth quarter of 2001, and down 18 percent from the first quarter of 2001. See Hansen and Olsen "Spam: It's More
precedent for self-regulation, and I believe that in this way, we could have positive and informative control of spam". 477

3.2.1 Forms Of Advertising Regulation

There are three possible forms of regulating advertising, namely:

a) Self-discipline:

This is where there are no formal controls. Advertisers are restrained by their competitors who may run better advertisements and by consumers who will refuse to be misled by misleading advertisements. Honest traders will be governed by their own consciences, by ethical business practices or by their fear of earning a bad reputation. However, this form of advertising regulation does not adequately control the abuses of advertising.

b) Statutory regulation:

In South Africa a number of statutes have been introduced which are designed to protect consumers as well as to protect honest business people from the disreputable practices of their competitors. Unfortunately, these statutes despite their criminal penalties do not act as adequate deterrents.

c) Self-regulation:

This is where the industry itself assumes responsibility. This is control by one’s peers, and in the field of advertising, the sanction is to withhold the right to advertise. A fully developed system of self-control offers pre-advertising advice to practitioners, monitors advertisements in various media, deals with competitor and consumer complaints, penalises bad behaviour and publicises decisions.

This is usually faster and less expensive than government regulation and the industry believes that it will be more effective in identifying genuine abuses as it "takes a thief to catch a thief". The industry expects its members to adhere to the spirit rather than the letter of the self-imposed rules and not to circumvent them by dubious ingenuity.

In order for self-regulation to be effective, voluntary controls and statutory regulation must be complementary. The Code states that advertising content should not violate any of the laws of the country.

---

3.3 *The Advertising Standards Authority*

In 1969 the advertising industry in South Africa assumed responsibility for monitoring itself. The industry voluntarily formed the Advertising Standards Authority (ASA) as a self-regulatory industry body charged with setting, implementing and maintaining standards within the industry.\(^{478}\) The ASA membership is fully representative of the media, marketing, advertising and communications industry.

The ASA adopted a code of conduct known as the ASA Code of Advertising Practice (the Code) based on the British Code of Advertising Practice and the International Code of Advertising Practice, prepared by the International Chamber of Commerce.

The Code prescribes the professional conduct of its members and encapsulates the good morals of the industry.\(^{479}\) It is reviewed annually and amended from time to time to meet the changing needs of the industry and of our society.

---

\(^{478}\) The ASA is an independent body set up and paid for by the marketing communications industry to regulate advertising in the public interest through a system of self-regulation. It is a section 21 company registered according to the company laws of South Africa. The ASA works closely with government, statutory bodies, consumer organisations and the industry to ensure that the content of advertising meets the requirements of the Code.

The Code is designed to protect consumers and to ensure fair play among advertisers. It ensures that certain standards of fair dealing and honest trading are met and sets out certain criteria for professional conduct for those involved in the industry. In addition the Code is a source of reference for the public as it sets out the ethics and limitations accepted by those using or working in advertising.

The primary object of the Code is the regulation of commercial advertising. It therefore applies to all advertisements for the supply of goods or services or the provision of facilities by way of trade, and also to advertisements other than those for specific products which are placed in the course of trade by or on behalf of any trader.480

The Preamble to the Code states:481

"All advertisements should be legal, decent, honest and truthful;

All advertisements should be prepared with a sense of responsibility to the consumer;

All advertisements should conform to the principles of fair competition in business;

No advertisement should bring advertising into disrepute or reduce confidence in advertising as a service to industry and to the public”.

480 Section i – Introduction; Paragraph 2.1 Scope
The Code defines an "advertisement" as:482

"any visual or aural communication, representation, reference or notification of any kind – which is intended to promote the sale, leasing or use of any goods or services; or which appeals for or promotes the support of any cause."

The Code further defines electronic media as advertising published by way of electronic means, and includes, *inter alia*, broadcast media.483 This definition could be extended to include e-mail advertising, and thus spam.

The general principles and rules of the Code that may be applied in the context of spam include:

"No advertising may offend against good taste or decency or be offensive to public or sectoral values and sensitivities, unless the advertising is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom".

"Advertisements should contain nothing that is likely to cause serious or wide-spread or sectoral offence. The fact that a particular product, service or advertisement may be offensive to some is not in itself

---

481 Section i – Introduction; Paragraph 1 Preamble
482 Section i – Introduction; Paragraph 4 Definitions
483 Section i – Introduction; Paragraph 4 Definitions
sufficient grounds for upholding an objection to an advertisement for that product or service. In considering whether an advertisement is offensive, consideration will be given, inter alia, to the context, medium, likely audience, the nature of the product or service, prevailing standards, degree of social concern, and public interest". 484

"Advertisements should not be so framed as to abuse the trust of the consumer or exploit his lack of experience or knowledge or his credulity". 485

"Advertisements should not without justifiable reason play on fear".

"Advertisements should not contain anything which might lead or lend support to acts of violence, nor should they appear to condone such acts".

"Advertisements should not contain anything which might lead or lend support to criminal or illegal activities, nor should they appear to condone such activities".

484 Section ii – General; Paragraph 1 Offensive Advertising
485 Section ii – General; Paragraph 2 Honesty
"No advertisements shall contain content of any description that is discriminatory, unless, in the opinion of the ASA, such discrimination is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom".

"Gender stereotyping or negative gender portrayal shall not be permitted in advertising, unless in the opinion of the ASA, such stereotyping or portrayal is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom".\(^{486}\)

"Headlines to advertising should not mislead in any way and it shall not be acceptable to contend that a misleading impression conveyed by a headline has been corrected in the body copy of the advertisement".\(^{487}\)

"Advertisements should be clearly distinguishable as such whatever their form and whatever the medium used. When an advertisement appears in a medium which contains news, editorial or programme matter it should be so designed, produced and presented that it will be readily recognised as an advertisement.

\(^{486}\) Section ii – General; Paragraph 3 Unacceptable Advertising \url{http://www.asasa.org.za/section_ii__general_48.html} (6 April 2004).

\(^{487}\) Section ii – General; Paragraph 4.2.6 Truthful Presentation \url{http://www.asasa.org.za/section_ii__general_48.html} (6 April 2004).
"In print media, wherever there is any possibility of confusion, the material in question should be headed conspicuously with the words ADVERTISEMENT or ADVERTISEMENT SUPPLEMENT, and should be boxed in or otherwise distinguished from surrounding or accompanying editorial matter”. 

"In Electronic Media particular care should be taken to clearly distinguish between programme content and advertising. Where there is a possibility of confusion, advertising should be clearly identified in a manner acceptable to the ASA”.  

3.3.1 Sanctions Imposed By The ASA

The ASA attempts to prevent unacceptable advertising from appearing by offering a pre-clearance service to any advertisers who wish to ensure that their adverts conform with the principles contained in the Code. In terms of the Independent Broadcasting Authority Act, electronic media owners are obliged to pre-clear their advertising.

---

The primary sanction agreed to by the industry is the withholding of advertising time and space. If the ASA rules that the advertising is unacceptable it cannot be used or, if already part of a marketing campaign, it must be amended or withdrawn. In many instances advertisers will voluntarily agree to amend or withdraw an offending advertisement. Where they fail to co-operate with the ASA, all ASA media members are requested not to accept further advertising from the advertiser in question until the matter has been satisfactorily resolved.

In addition, if an advertiser habitually contravenes the Code or appears to be ignorant of its provisions, the ASA will issue a media alert that no advertising be accepted from that particular advertiser unless the advertiser has obtained pre-publication clearance from the ASA. The ASA cannot however impose these sanctions if the offender is not a member.

In traditional media the threat of withdrawal of advertising privileges has generally proved to be effective. The sanctions imposed by the ASA however are not applicable to the Internet, and the ASA would therefore not have effective control over spam. The guidelines of the Code would also only be useful to legitimate Internet marketers.
3.4 *The European Advertising Standards Alliance*

The European Advertising Standards Alliance (EASA), based in Brussels, brings together advertising self-regulatory bodies across Europe and further afield in the ever-expanding global self-regulatory network. South Africa became part of the Alliance in 1995.\(^{490}\)

3.5 *The Marketing Federation Of Southern Africa*

The Marketing Federation of Southern Africa (MFS A)\(^ {491}\) was formed in October 2002 as a result of an amalgamation of the former Association of Marketers, the Direct Marketing Association and the Institute of Marketing Management.

The Association of Marketers (ASOM) was established as an industry association to lobby for the industry and to take measures to enhance the professional standing of the marketing sector.\(^ {492}\)

The Direct Marketing Association (DMA) was established to represent the collective interests of operators in one of the fastest growing sectors of the


\(^{492}\) In 1976 it set up the well-known Loerie Awards to promote high quality advertising on South Africa’s commercial television. In 1999 ASOM launched the Raptor Awards programme to recognise excellence in sponsorship as a means of achieving marketing objectives in a wide range of sectors.
discipline thus representing marketers and suppliers in direct mail, DRTV, e-marketing, SMS, telemarketing, response print and broadcast advertising.\textsuperscript{493}

The Institute of Marketing Management (IMM) grew out of the Sales Manager’s Association of South Africa (SMASA), which was set up in 1949 by members of the Incorporated Sales Management Association of Great Britain (ISMA) as a non-profit professional organisation.\textsuperscript{494}

The MFSA sets the framework for excellence in marketing practice; it directly promotes excellent marketing practice through its advisory services publications and incentive awards; it monitors ethical standards in the marketing industry; and it sets and monitors standards in educating and training marketing professionals and practitioners.

The MFSA has various articles on e-mail advertising available on its Web site to guide advertisers on how to use email advertising correctly.\textsuperscript{495} These guidelines\textsuperscript{496} will form the basis of a green paper process to arrive at an...

\textsuperscript{493} In 1998 the DMA established the Assegai Awards programme to promote growth and reward excellence in direct marketing campaigns.

\textsuperscript{494} In the late 1950s, a diploma in marketing for the sector was introduced by SMASA as a result of an arrangement with ISMA. This was the start of marketing education in the country. In 1960, SMSA changed its name to the Institute of Marketing Management, which was committed to upgrading and upholding the standard of expertise in marketing.

\textsuperscript{495} For example "How To Use E-Mail To Fire Up Sales (Without Getting Flamed)" available at \url{http://www.dma.org.za/articles/levison-e-mail_mktg.htm} (12 October 2003).

\textsuperscript{496} A copy of these guidelines is available at \url{http://www.spamsummit.co.za} (10 September 2004).
industry-approved Code of Conduct for commercial e-mail usage, to be administrated by the MFSA.

The MFSA should consider self-regulation and require its members to subscribe to an e-mail best practice guide. It should work with the South African Internet Service Providers’ Association (ISPA), and possibly compile a white-list of its members who have subscribed to its code of conduct and whose IP addresses can be trusted for purposes of bulk e-mailing.

3.6 **Legislation**

Advertising may also be regulated by legislation. Such legislation may be aimed at protecting intellectual property rights, such as trade marks or Copyright, or prohibiting or controlling certain business practices (such as gambling legislation), or regulating advertising within a particular industry (such as the Internet gaming industry). There are also common law restrictions on advertising related to unlawful competition.

3.7 **The Harmful Business Practices Act**\(^{497}\)

The Harmful Business Practices Act is the principal Act controlling misleading and false advertising. This Act was introduced in 1988 in order to facilitate effective consumer protection and to replace the Trade Practices Act. It

\(^{497}\) Act 71 of 1988.
provides for the prohibition of certain business practices that may be regarded as "harmful to consumers".

The Act provides for the establishment of a Business Practices Committee which has the power to investigate business practices and to recommend that they be declared harmful.

The Business Practices Committee reports to the Minister of Trade and Industry who is empowered to declare by notice in the Government Gazette that a practice is unlawful. The Minister may also by notice in the Government Gazette direct any person who uses or has used any advertising or type of advertising which is connected with a harmful business practice to refrain from using that advertising.

The Act also provides for certain criminal penalties for persons who fail to comply, and a term of imprisonment may also be imposed.

Unfortunately, the Business Practices Committee has been under-utilised. The committee does not see its role as superseding any self-regulatory scheme which may operate to maintain standards in a particular industry. Self-regulation in industry is viewed as one of the primary mechanisms for the handling of harmful business practices.
In the field of advertising there is close co-operation between the Business Practices Committee and the ASA. Although the committee has various investigatory powers, it is essentially an advisory body. Through such informal intervention the committee frequently secures the voluntary compliance of a business in altering its business practice.

Where appropriate, the Business Practices Committee will consult bodies such as the ASA or the Competition Board. The Business Practices Committee may also recommend that the Minister take appropriate action as provided for in the Act.

3.8 The United Kingdom

3.8.1 The United Kingdom Advertising Standards Authority

Marketers in the United Kingdom are obliged to adhere to the Committee of Advertising Practice Code (CAP Code).\footnote{The new CAP Code is available at http://www.asa.org.uk/the_codes/downloads/Bcasp_11.pdf (27 March 2004).} The CAP Code is a set of rules produced by the United Kingdom’s Committee of Advertising Practice governing the content of non-broadcast marketing communications, sales promotions and direct marketing communications. It is administered by the Advertising Standards Authority. Although lacking the force of legislation, the CAP Code should be followed by all businesses and there are penalties available for non-compliance.
The most recent edition of the CAP Code takes account of, and refers to, emerging new media and has been substantially redrafted to clarify many sections so that marketers have a better idea of the rules they are required to follow to ensure that their marketing is legal, decent, honest and truthful. The new rules came into force in March 2003 and they significantly affect direct marketing by e-mail and SMS text messaging.

Under the new set of rules, immediate disclosure is required if e-mails contain direct marketing. Legitimate unsolicited e-mail marketing communications must be clearly identifiable as such without the need for recipients to open them.

The CAP Code states that marketers:

"should ensure that marketing communications are designed and presented in such a way that it is clear that they are marketing communications. Unsolicited email marketing communications should be clearly identifiable as marketing communications without the need to open them."

This echoes a legal requirement introduced by the provisions of the Directive on Privacy and Electronic Communications passed by the EU in 2002 (the E-commerce Regulations of 2002). However, there has been little or no
guidance under either the CAP Code or the E-commerce Regulations on how to identify marketing communications as such.

Under the new rules, explicit consent is required for marketing by e-mail or SMS unless marketers are offering similar products to existing customers:

"The explicit consent of consumers is required before marketing by e-mail or SMS text transmission, save that marketers may market their similar products to their existing customers without explicit consent so long as an opportunity to object to further such marketing is given on each occasion".

This is also in compliance with the provisions of the E-commerce Regulations of 2002.

3.8.1.1 Sanctions for non-compliance

Although breaking the CAP Code is not a criminal offence, a range of sanctions operate to ensure compliance with the CAP Code:

a) Upheld cases of non-compliance often receive extensive adverse media coverage. This not only informs the public that a marketer has misled or caused offence but also acts as a deterrent to other companies.

b) It is a prerequisite for membership of the trade and professional associations in CAP to comply with the CAP Code, so publishers and media owners may refuse further space for an advertisement that breaks the Code. CAP sends out an "Ad Alert" to its members to warn them of those companies that have chosen not to co-operate with the ASA. Advertising space can then be denied until the required changes have been made.

c) The trade and professional associations in CAP may remove concessions or incentives associated with membership of that association, or withdraw commission paid on placing advertisements. This could significantly increase the costs associated with a campaign to the point of jeopardising it.

d) The ASA can refer a marketer, agency or publisher to the Director General of Fair Trading at the OFT under the Control of Misleading Advertisements Regulations 1988. The OFT can obtain an order through the courts to prevent advertisers from using the same or similar claims in future marketing communications.
3.8.2 Case Law

3.8.2.1 The Training Guild

The United Kingdom’s ASA published its first ruling under the new rules on e-mail marketing in terms of the new edition of the CAP Code on 10 September 2003.500

The landmark decision confirms that companies need to check for explicit consent before using a marketing list for an e-mail campaign, even if the company believes in good faith that the list comprises only those who opted to receive marketing. The decision also clarified what is necessary to identify a marketing communication.

The matter involved a Southampton seminar provider called "The Training Guild" that had sent e-mails about a seminar to a mailing list that had been supplied by a third party. It sent messages headed "Business Seminars – Telesales & Selling Skills Made Easy" which, when opened, promoted "a selling sales course for non-aggressive people". A recipient on this list laid a complaint with the ASA under two new provisions of the CAP Code.

The complaint was first, that the e-mail did not make clear in its subject field that it was a marketing communication; and secondly that The Training Guild did not get explicit consent to send e-mail to the complainant.

The ASA decided that the subject line was clearly identifiable as a marketing communication but it considered that The Training Guild "had not got explicit consent to send the e-mail to the complainant".

In its decision, the ASA also acknowledged that the advertisers had bought a list of e-mail addresses of people who had opted to receive information about business development topics by e-mail in good faith. The ASA nevertheless considered that "it was the advertisers' responsibility to ensure that recipients on the list had given their explicit consent to receive such e-mails".

Ultimately, the ASA was lenient in its punishment, simply advising the organisation to take more care in its targeting of marketing emails in the future. Failure to comply would result in sanctions.

3.8.2.2 Phone Direct

In October 2003 the United Kingdom’s ASA reprimanded a telephone company for breaching the CAP Code by sending commercial e-mail that did
not identify itself as a marketing communication until opened by the recipient.  

A company called “Phone Direct” advertised its international telephone call rates by email. The addressee field read “Friends Group” and the subject field read "FW: Useful information this time of year".

The content of the e-mail read like typical spam:

"Hiya, With most of you all going on holiday soon, I just thought this website my boyfriend e-mailed me about would be useful! Looks like you can save loads on international phone calls. Helen X".

An apparently forwarded message in the e-mail read:

"Hi Helen, I have just been told about this website where it tells you how to make cheap phone calls, it looks pretty good and we don't even need to register with them. I will be able to call you every day when you are on holiday as it will only cost me the same as ringing you when you are here! The website is here: http://www.pd-dial.com Anyway, must get on with more work, take care babe Steve".

See further Out-Law.Com "Misleading E-Mail Headers: ASA Warns Marketers"
Complaints were made to the ASA on the basis that the e-mail did not make it clear that it was a marketing communication. The nature of Phone Direct’s e-mail was not apparent from the subject header. The ASA therefore concluded the Phone Direct’s e-mail was misleading because neither the format nor the content identified it as a marketing communication. The ASA’s report does not address the fact that the e-mail was unsolicited.

3.9 **The United States**

3.9.1 The Direct Marketing Association

The Direct Marketing Association (DMA) in the United States is a trade association that represents users and suppliers in the direct, database, and interactive marketing field.\(^{502}\) Members of the DMA are required to abide by the DMA’s Privacy Promise\(^{503}\) and are prohibited from sending unsolicited commercial email messages to addresses that appear in the DMA’s email Preference Service database.\(^{504}\)

The DMA acquired the Association for Interactive Media (AIM) in 1998. AIM also opposes unsolicited bulk commercial e-mail.\(^{505}\)

\(^{502}\) The DMA has approximately 4700 members that include direct mail, catalogue and telemarketing companies.


\(^{504}\) Available at [http://www.e-mps.org](http://www.e-mps.org) (13 April 2004).

The DMA acquired the Internet Alliance in 1999. Under the Internet Alliance’s "spamming guidelines", marketers should not collect e-mail addresses in online forums for the purpose of sending unsolicited email unless they are permitted to do so by the forum.\textsuperscript{506}

3.10 Canada

The Canadian Marketing Association (CMA)\textsuperscript{507} was established in 1967 by 21 companies involved in the direct marketing industry in Canada. It has grown to become the largest marketing association in Canada with a membership of 800 companies, representing 80% of the industry. Some of these companies focus solely upon marketing, including the reaching of consumers through "Internet, television, telephone, radio and addressed advertising mail".

In the late 1970s, the federal Department of Consumer and Corporate Affairs (CCA) encouraged the CMA to establish a self-regulatory program to deal with customer complaints about direct marketers. At the beginning of 1978, a complaint resolution program called Operation Integrity was implemented,

\textsuperscript{506} See the Internet Alliance "IA Addresses Unsolicited Bulk E-mail" available at http://www.internetalliance.org/policy/spamming_guidelines.html (14 April 2004).

\textsuperscript{507} The CMA was formerly known as the Canadian Direct Mail/Marketing Association and then the Canadian Direct Marketing Association. In 1998 it became the Canadian Marketing Association. The CMA Web site is available at http://www.thecma.org (23 March 2004).
which included a code of conduct which CMA members are required to follow.

The CMA’s consumer protection rules have seen a number of changes in response to issues which caused consumer concern. In January 1993 privacy policies were introduced in response to growing concerns about the handling of personal information by marketers.

In 1998 member organisations were forbidden from sending unsolicited commercial e-mail and had to further restrict their information handling practices as the Internet became an increasingly common marketing medium.

Members of the CMA, who abide by an industry Code, will only solicit customers with whom they have an existing relationship. The CMA also manages an e-mail preference program that allows consumers to have their name and address removed from marketing lists.
3.11  *Legitimate E-mail Advertising*

"Advertising just doesn't work as well as it used to - in part because there's so much of it, in part because people have learned to ignore it, in part because the rise of the Internet means that companies can go beyond it".  

Electronic mail has dramatically changed the relationship between consumers and the suppliers of products and services. It allows companies to quickly inform customers of new products and services. It has also become one of the most cost-efficient ways of providing customer support and assistance. Permission-based Internet marketing, through e-mail advertisements, could become one of the most important commercial Internet applications.

The biggest problem with mass-market advertising is that it fights for people's attention by interrupting them. A 30-second advertisement interrupts a television programme, a telemarketing call interrupts a family dinner, and a print advertisement interrupts a newspaper article. The interruption model is not effective when there is an overflow of interruptions. A new model of advertising has therefore been built around permission, where consumers volunteer attention and agree to learn more about a company and its products.

---

509  An example of this is where consumers give a company permission to send them advertising messages in return for the chance to win prizes.
In the same way, email marketing can be highly effective when it is done appropriately. It can be particularly effective when marketers have obtained the permission of consumers and are able to target messages to those who have expressed an interest in a particular product or service.

Jupiter Communications estimates that commercial e-mail market will soar to an estimated $7.3 billion and that online consumers could receive up to 1,600 commercial e-mails per year by 2005.510

3.12 "Opt-In" Lists

Permission-based or "opt-in" e-mail is becoming more popular. However, companies must be acutely aware of customer sensitivity toward unsolicited e-mail, and must develop their "opt-in" list very carefully from both on-line and traditional sources. There are thousands of lists available on the Internet for as little as $11, but lists like these are often spam lists and consist merely of names that have been harvested without the recipients' consent.

A safe and reputable option is to generate a list by inviting Internet users to "opt-in" to lists pertaining to topics of interest and allowing members to "opt-out" at any time. Companies should balance the importance of mailing against the potential nuisance to the customer. Every message should run

through a "headline test" to determine if it is newsworthy enough to merit a new communication.

3.13  Limitations Of Industry Codes And Self Regulation

Informal approaches such as social pressure and industry self-regulation have generally had little effect on spam. Rules of netiquette generally lack enforcement mechanisms and ISPs are not able to impose their acceptable use policies upon spammers attempting to send spam messages to their subscribers.

Self regulation and industry codes generally rely on the honest desire on the part of industry participants to be seen to be responsible to ensure compliance. The threat of legislation, coupled with the need to protect a substantial investment, may also lead to the adoption of voluntary codes. In the case of spamming, however, the notion of responsibility does not come into play. Spammers also have no investment to protect since they expect to have their ISP service terminated at some point. Spammers therefore have no incentive to adhere to any industry code of practice, and there are no real consequences to a spammer who refuses to comply with a code of practice.
4. The Role Of Internet Service Providers

4.1 Introduction

Apart from the senders and recipients of unsolicited communications, Internet service providers ("ISPs") which typically manage consumers' e-mail through their servers are part of the "spam chain" and therefore have an important role to play.

For ISPs, quality of services is key to attracting and retaining consumers. In response to consumer complaints about spam, many ISPs have taken steps to curtail this practice. Most ISPs reserve the right to terminate service to any subscriber who uses their facilities to transmit spam. ISPs also use, or provide subscribers with, technological tools to filter unwanted communications.

It is arguable that there are further steps that could be taken to ensure that a zero-tolerance policy is effectively enforced industry-wide, through domestic and international co-operation. Internet users should be clearly advised of the possible consequences of e-mail abuse, such as a denial of service by other service providers.

4.2 Chapter XI of the ECT Act

The Department of Communications has invited comments on proposed guidelines for the recognition of Industry Representative Bodies in terms of
Chapter XI (Limitation of Liability of Service Providers) of the ECT Act. The guidelines address minimum requirements for Best Practice Codes of Conduct, Checklists of Adequate Criteria, and Monitoring and Enforcement procedures.

Section 5 of the guidelines contain minimum requirements for a code of conduct for ISPs. Section 5.8 of the guidelines provides:

"5.8.1 Members 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.

5.8.2 Members must provide a facility for dealing with complaints about spam originating from their networks and must react expeditiously to complaints received.

5.8.3 Members shall contractually require their clients to guarantee that they will not send or promote the sending of spam."

4.3 Terms Of Agreement

The majority of ISPs and email service providers have adopted strict anti-spam policies to control people's behaviour in using email. Almost all ISPs have their users agree to what they call a "terms of service" contract, which normally includes an agreement not to abuse bulk email in one form or another. In their terms of service contract, they maintain the right to

terminate the account of any subscriber who engages in abusive e-mail practices.

ISPs also use special servers for users who have not yet agreed to the contract. These measures are to ensure that people don't send bulk e-mail unless they can be held accountable for abuse of it, while not blocking individual mail in any way. However, spammers appear to have very little difficulty in obtaining new accounts when they are cut off by a service provider as a result of e-mail abuse. ISP need to work together to share information so that they can keep tabs on roving spammers and shut them down more effectively.

4.4 Free Trial Accounts

Most ISPs use free trial (or "throwaway") accounts to market their services. These free trial accounts can often be signed up for online and the ISP has no way of enforcing any terms of service over free trial users. In most cases the ISP doesn't even have valid contact information on a free trial user.

While most ISPs require users to supply their credit card details to open a trial account, stolen credit card numbers can be used because the trial account is only valid for one month. Users of free trial accounts are therefore not easily held accountable for violations of their terms of service and the only recourse available to the ISP is to disconnect them. After disconnection,
the user can simply get another free trial account, at the same ISP or another
one.

ISPs should be encouraged to restrict the access of trial accounts by giving
these accounts a lower level of service than established customers. In
particular, ISPs should place limitations on the use of bulk email until the
user becomes an established customer who has signed a terms of service
contract.

Microsoft has also introduced a "human verification" test in an attempt to
prevent spammers from using automated programmes to sign up for
hundreds of free Hotmail accounts to send spam. The test involves entering
information from a displayed graphic that contains a word rendered in
distorted text placed on a busy background. The theory is that automated
spam software can't decipher the text, but humans can.\(^\text{512}\)

\section{4.5 Throttle Relays}

ISPs should only grant "open" access to e-mail ports on the Internet to users
who have agreed to a terms of service contract and a code of email ethics.
All other users, including anonymous mailers, should only be allowed to send
e-mail via special relaying servers. Those wishing to send bulk mail, such as
the operators of mailing lists, would have to agree to a code of e-mail ethics.

\(^{512}\) Delio "Spammers Top Microsoft Hitlist" \textit{Wired News} available at
Relay servers, either present at the ISP or on the Internet, are able to put a "throttle" on e-mail volume. These throttle relays only allow a low volume of messages for each user, IP address or network of addresses. I.e. the server would allow users on any given network or computer the ability to only send a few messages per minute, per hour or per day. The threshold volume allowed would be enough to handle the needs of people sending ordinary person to person e-mail, but bulk e-mail would not be possible, since the throttle would slow down, or eventually stop, any mass messages from a machine or network. A small volume of spam could get through, but it would not be possible to generate a significant volume of spam because of the limit on the volume to that of an individual mailer.

Throttle servers deal with the threat of "open relays" which are commonly used by spammers, since the throttle is based on the number of recipients of messages, rather than the number of message connections. A person attempting to mail a message to an open relay with 1 000 recipients would get cut off or throttled immediately.

Parties wishing to send anonymous mail, through services called re-mailers would also relay through the throttle servers. Therefore, anonymous bulk e-mail would not be possible, except by arranging for another party who has signed the code of ethics to act as a gateway. That party would take

http://www.wired.com/news/print/0,1294,61742,00.html

513 Today most ISPs and ordinary users already use throttle servers.
responsibility for abuse by the anonymous party. There are services which have offered anonymous e-mail for a small fee. However, if you abuse them, they cancel the access, costing you the fee. For example, companies like Zero Knowledge sell anonymous Internet access, but delete accounts when they are abused. This puts a financial cost on abuse, helping to solve the problem.

If an ISP cannot or will not put a throttle on its users that can't be held accountable, sites that wish to can put a throttle on the entire site. There are various technical ways to achieve this. It is possible to redirect\textsuperscript{514} all traffic from such ISPs to a set of connected throttle servers. Instead of blocking all

\textsuperscript{514} One way to arrange this redirect is with a "MX" (Mail Exchanger) record trick. The domain naming system allows any site that receives mail to specify a prioritized list of sites which accept mail for it. Senders of mail are expected to connect to the highest priority [lowest number] site which is up and running. Usually the highest priority site is the "real" site and others are backup sites. A site wishing to stop spam coming to it would create a special, lowest-score "MX" record for their mail domain, pointing to the throttle server. It would contain a special flag to indicate that it is an MX to a throttle.

If a site that doesn't know about the MX trick tries to send mail to the site, it would instead mail the throttle server. This is not a problem, because at worst their person to person mail is delayed a few minutes. If a sender is, however, part of the group who have agreed to be accountable for spam they would be able to mail through directly and would not have to go through the throttle server. They can do this by having a special mail sending agent (like Sendmail) which knows to skip any "MX" with the magic throttle server name. Alternatively, the throttle server itself could also simply refuse connections from them, and immediately they will try to send the mail to the 2nd tier, which is actually the real destination.

The low-accountability sites would have to use the throttle relays, and they would not be able to bypass them like the high-accountability sites because the non-throttle sites won't take their traffic directly at all, using techniques like blacklists or whitelists. However, these blacklists don't actually block any legitimate e-mail, since you would only encounter them if you deliberately ignore the regular rules for an MX list.

access from those ISPs or dial-ups, the throttle server will only block the bulk mail access.

The throttle servers do not need to be fast. They can run on old hardware or spare capacity because it is their job to be slow. The throttle servers would delay all mail for at least a minute or two in a queue, and would summarise mail volume from various sources on a multicast stream, itself pulsing out the data every minute so all throttles can know what all the others know. This stops spammers from trying to distribute their load among all the known throttle servers. The "live delay" on the queue would mean that if they hit the volume threshold, their mail would be stopped or slowed down.

In effect, high priority is given to short single messages and low priority is given to volume traffic that is overloading the servers. Ideally, the system would detect duplicates (bulk mail) and deliver the first couple, and put the rest into a very slow queue and mail a warning (like the "unable to deliver mail, still trying" message) back to the sender. In this way non-duplicates would not be slowed down very much. Duplicate detection also does not have to be intelligent. It mainly has to look for an above normal volume of messages from any given IP address or address block.
4.5.1 Advantages Of Throttle Relays

Throttle relays are generally very effective in solving the spam problem. They only involve contracts and not new laws. They have an advantage over legislation in that they work internationally, and in many cases ISPs are already using relay servers for all users.

The relay servers do not need to be particularly fast or powerful since their goal is to slow down mail. This in turn means that they can be relatively inexpensive. Because they are slow, it is a strong incentive for people to formally agree to an anti-spam terms of service contract. There are also methods to ensure that the relay servers are not overwhelmed with the mail volume.

By not dealing with individual mail at all, and allowing relay servers to be open again, throttle servers also have the important benefit of not punishing innocent users by blocking legitimate mail in an attempt to stop spam.

4.5.2 Disadvantages Of Throttle Relays

Throttle relays mean that it is not possible to run a mailing list until you have agreed to the anti-spam rules or are somehow accountable for abuse, and that mailing lists with a truly anonymous host will have a problem operating. However, mailing lists run by a known user who protects the identity of the
real sender are still able to exist. This is almost always the case in any event.

The throttle servers must be able to communicate with one another to exchange throttling data. IP multicast with encryption can do this efficiently. Since it is acceptable for these servers to delay all mail a few minutes, a resynchronisation of throttle volume data every few minutes would be sufficient to stop abusers who attempt to round-robin around the throttle servers.

This system creates a potential problem for users of ISPs that both won't sign the anti-spam pledge and are hosts for lots of spammers. If the ISP itself gets their mail volume throttled, their mail will get very slow. If the ISPs spammers use the same IP address as their ordinary users (i.e. they are both using the ISP's mail relay), all their mail will become unusably slow. The ordinary users could, however, terminate their account and sign up with another server that is not throttled.

This system will not stop spam sent in very small volumes, but these single e-mails are not likely to fill users mailboxes to the point that they are unusable or overload servers.
4.6 Example Of A Terms Of Service Contract

MWEB’s "Terms and Conditions of Use" provides an example of a comprehensive Terms of Use contract that caters specifically for spam. Section 8, entitled "User Etiquette and Abusive Behaviour", provides:

"1. You hereby agree to adhere to generally acceptable Internet and e-mail etiquette. In this regard, without being limited to the examples listed below, you agree not to:

1.1 engage in any abuse of e-mail or spamming, including (without being limited to) the posting or cross-posting of unsolicited articles with the same or substantially the same message to recipients that did not request to receive such messages;

1.2 take any action aimed at deceiving or misleading any person, attempt to impersonate or misrepresent your affiliation to any person or forge headers or otherwise manipulate identifiers in order to disguise the origin of anything posted or transmitted through the service;

1.3 use the service to post or transmit anything which is defamatory, discriminatory, obscene, threatening, abusive, harassing, harmful, hateful or which carries child pornography, religious or racial slurs or threatens or

---

encourages bodily harm or the like or which may violate any person's personality rights;

1.4 use the service to make fraudulent offers to sell or buy products, items or services or to offer or solicit for any type of financial scam such as "pyramid schemes" and "chain letters";

1.5 use the service in a manner that may infringe the intellectual property rights (for example copyright or trade marks) or other proprietary rights of others, including (without being limited to) the transmission of pirated software;

1.6 use the service in any manner which could damage, impair, overburden or disable the service or interfere with any other party's use or enjoyment of the service;

1.7 use the service to post or transmit anything which contains viruses or any other destructive features, regardless of whether or not damage is intended;

1.8 cancel any Usenet post other than your own;

1.9 repeatedly post gratuitous off the topic postings;

1.10 gather e-mail addresses and/or names for commercial, political, charity or like purposes or use the service to collect or attempt to collect personal information about third parties without their knowledge or consent; and
1.11 violate the privacy of any person or attempt to gain unauthorised access to the service or any other network, including (without being limited to) through hacking, password mining or any other means; and/or

1.12 use the service to engage in any illegal or unlawful activity.

2. Should you engage in any one or more of the above practices, which shall be determined in MWEB's sole discretion and which decision shall be final, then MWEB shall be entitled, without prejudice to any other rights it may have, to:

2.1 without notice, suspend your access to the service;

2.2 terminate this agreement with immediate effect;

2.3 bill you for any costs incurred by MWEB, including (without being limited to) bandwidth, administration costs, downtime, usage of MWEB's name or registered domain names and CPU cycles; and/or

2.4 notwithstanding MWEB's privacy policy, disclose any information relating to you, whether public or personal, to all persons affected by your actions."
Spam academic Brad Templeton\textsuperscript{516} has proposed the following Terms of Service contract:

a) SUBSCRIBER (or any party given access via SUBSCRIBER's contract with ISP) will not use ISP's facilities to send a "mass e-mailing" to parties who have never had voluntary personal interaction with SUBSCRIBER. A "mass e-mailing" shall be the ordering of an e-mail message (or group of related messages) to more than 25 people who themselves have not had personal interaction with one another.

b) SUBSCRIBER shall further not perform such a mailing through any facility so that replies will come to an email address served by ISP, or refer to any web page, FTP site or other resource served directly by ISP.

c) In the event that SUBSCRIBER violates the above clauses, SUBSCRIBER's Internet service may be terminated immediately, without refund or further access to any associated services, such as received e-mail, files on ISPs machines or servers. In addition SUBSCRIBER shall be liable to ISP for the full costs, plus 200% incurred by ISP in dealing with the consequences of such a mass e-mailing, including but not limited to system loads, system failures, and staff time and overtime related to complaints and other problems. In addition, SUBSCRIBER shall be liable for a minimum of $10 per address in the mailing.

\textsuperscript{516} Available at \url{http://www.templetons.com/brad/spam/block.html} (5 April 2004).
d) SUBSCRIBER warrants that SUBSCRIBER, nor any party he or she represents or will allow access to ISP's facilities, is not at present nor has at any time in the past been subject to discipline from another Internet service provider or related company for violation of contractual terms regulating bulk emailing. SUBSCRIBER agrees that a violation of this clause shall cause SUBSCRIBER to be liable to ISP for $10,000, plus court costs in obtaining payment of this liability.

4.7 Why Enforcement By ISPs Has Failed

Internet Service Providers continue to stop service to spammers. Unfortunately, the ISP only knows they have a spammer connected once the spam has already been sent, and all that the spammer loses is their service fees. This is still good value to the spammer for sending millions of copies of an advertisement all over the Internet.

Once an ISP has terminated service to a spammer, the spammer has a vast array of other ISPs to select from. The type of spammer that does this is called a "whack-a-mole" spammer, because as soon as one ISP disconnects the spammer they pop up elsewhere, and eventually they resurface at the original ISP using different credit card details or a prepaid account. The whole exercise becomes an electronic version of the arcade game of the same name. Whack-a-mole spamming is the standard mode of operation for low budget spammers, and it makes ISP based enforcement impossible.
On the above it is submitted that South African ISPs cannot effectively prevent spam without supporting legislation.

4.8 ISP Liability

An important question is whether ISPs can be liable for negligence if they fail to adhere to the standard of care legally required of them. In terms of South African law, if a reasonable person in the position of an ISP would foresee the reasonable possibility of its conduct injuring subscriber/s and causing loss; would take reasonable steps to guard against such occurrence; and fails to take such steps, the ISP is negligent.

In this sense, an ISP could be liable for negligent conduct due to their failure to guard against the foreseeable harm of spam, for example by not taking technical steps to deal with the problem. Such steps could include the technical approaches detailed below, such as enforcing e-mail ethics in their terms of service contracts, implementing subject line blocking, the use of blacklists and reverse domain name look-ups to establish whether a sender is real. ISPs could also assist subscribers to manage the spam problem, for example, by making spam filtering software and blacklists available to them.

517 Kruger v Coetzee 1966 (2) SA 428 (A).
The type of loss that is foreseeable would include a situation where a virus attached to a spam e-mail deletes all the subscriber’s data on his computer’s hard-drive.

PART B : TECHNICAL APPROACHES

5. Introduction

For most Internet users, the first line of defense against spam normally consists of self-help and other technical mechanisms. These methods are usually employed by individual users and Internet service providers. Lessig\(^{519}\) comments that the architecture of cyberspace could be designed to enable better regulation, for example by creating architectures of identification and authentication.\(^{520}\)

In *CompuServe Inc. v Cyber Promotions Inc*\(^{521}\) the Court held that “the implementation of technological means of self-help, to the extent that

\(^{519}\) Lessig *Code* at page 30 – 35.

\(^{520}\) Internet architects could update the e-mail system to make it possible to verify the sender of e-mail messages through authentication schemes. Microsoft has attempted to make such an architectural design an Internet standard through their Sender ID technology that seeks to cut down on junk mail by making it difficult for spammers to forge e-mail headers and addresses. However, *Wired News* reports that America Online has announced that it will not be supporting Microsoft’s Sender ID technology. Internet engineers rejected a preliminary proposal from Microsoft to introduce its technology as an Internet standard, due to the software giant’s patent claims. AOL said that its objections had nothing to do with Microsoft’s patent but rather it had been concerned at the “lack of acceptance for Sender ID among the free and open source online community”. See *Wired News* “Spam-Busting Plan Can’t Buy A Pal” available at http://www.wired.com/news/technology/0,1282,64989,00.html?tw=wn_tophead_7 (25 September 2004).

reasonable measures are effective … should be exhausted before legal action is proper”.

6. **Filtering And Blocking**

The rapid growth in the volume of spam has lead to an increased demand for filtering and blocking technologies. Filtering technologies for individual users have been available for many years, and new services offered on the market are being aimed at service providers and organisations. However, effective e-mail filtering services can entail considerable added costs for service providers and individual consumers.

Some products claim an 80 percent success rate in intercepting spam. However, while certain keywords and features make it relatively simple to intercept spam, spammers have shown themselves to be resourceful in getting through security firewalls and filters. Spammers continue to come up with new and ingenious ways to bypass filters by misspelling words, sending e-mails from what appears to be yourself, and putting messages in the subject lines that make people think the mail is from a friend.

At the same time, companies\(^{522}\) are trying to help consumers, businesses and Internet service providers to combat spam by coming up with new technologies. “Spammers are clever people and there is clearly an arms

---

\(^{522}\) For example, Brightmail Inc and McAfee.
race between spammers and people trying to prevent spam that just constantly escalates".  

7. Individual User solutions

7.1 Identify And Delete

The easiest approach for individual users is usually just to ignore and delete unwanted messages. Users may try to recognize unwanted messages based upon an unfamiliar sender address, or a subject line that contains an obvious solicitation, and delete them without wasting time opening and reading them.

This may seem practical, but there are a number of problems with this approach. First, how many times should users have to "just hit delete" every day? Simply ignoring and deleting unwanted messages ignores the escalating problem of spam. The damage from spam to the individual comes from the cumulative effects of spam, not from isolated incidents.

Secondly, by the time a user has deleted the message, most of the damage has been done. The ISP has incurred the cost of facilities to cope with the volume of spam and passed them on to the user. The user has had to spend time downloading useless messages, which may be charged by either time

---

or data. If their e-mail program notifies them of new messages, their flow of work has been interrupted, costing them time and productivity.

Thirdly, "just hit delete" does nothing to discourage vendors from further advertising by spam.

7.2 User Filters

Most modern e-mail software, such as Microsoft Outlook, includes automatic filtering capabilities which are specifically designed to identify and delete spam. Most filtering techniques involve rejecting messages that appear to be spam. Messages can be filtered based upon the headers of a message or its full text. Various blacklists and spam archives can also be used to help identify spam. It is also possible to reject all messages except those that can be recognized as legitimate.

Telkom Internet, one of South Africa’s largest ISPs with more than 100 000 users, offers its clients a free service that filters spam and provides free anti-virus software. Telkom Internet operates a blocking system through qmail scanner, which provides plug-in anti-virus and anti-spam capabilities to the Telkom Internet mail system. Virus definitions are automatically updated every 12 hours from the global threat database, or manually at any time if a new threat is identified. Telkom Internet does not quarantine or attempt to disinfect any message found to have a viral payload. If the sender is identifiable, a non-delivery message detailing the reason will be returned. If the sender-ID is false, the message will be suppressed.
SpamAssassin. The SpamAssassin filtering system checks the content of each message received using constantly updated spam identification rules which pinpoint features associated with spam. The filter will assign a score to the message, with the default value for spam set at level 6. If any message accumulates a spam filter score above 6, it is 99% likely to be a spam message.  

The problem with filtering techniques is that they often result in legitimate messages being mistakenly identified as spam. They may also block legitimate users of anonymous and pseudonymous re-mailers, free Web-based e-mail services like Hotmail, and e-mail "greeting card" services.

Spam may be temporarily placed in a lower priority channel. However, prioritization of incoming messages does not address the bandwidth and storage capacity problems caused by spam, and it is still necessary to periodically review these messages.

Filtering algorithms cannot detect all spam, and spammers have an incentive to structure their messages in a way that defeats automated filters, such as using false domain names or generic or personalized subject lines. Filters that work on a key word basis to block spam depending on how frequently

---

525 See further Meyer "Are You Also Sick Of ‘Spam’?" The Star, Tuesday 15 July 2003 page 12.

526 For example, Hotmail uses an inbox filter which places e-mail addressed to the user in the "BCC" header into a bulk mail folder for the user to sort through.
certain words appear are also not very effective because spammers misspell words or write shorter e-mails so there are not as many occurrences.

8. Third Party Solutions

8.1 Filters

Filtering by ISPs and third-party proxy filtering services like Brightmail can be more effective than end user filtering. For example, an ISP can block all traffic originating from a known spammer and may cooperate with other ISP's in identifying spammers. Individuals can also have their incoming e-mail routed through a third-party proxy service\(^{527}\) that attempts to filter out spam.

The advantage of using filtering by ISPs and third-party proxy filtering services is that they are more likely to stop spam before it reaches the user's e-mail inbox.\(^ {528}\) The collaborative filtering employed by these approaches can also be more effective than individual filtering since it permits identification of multiple identical copies of a message that otherwise might not be obvious as spam.

\(^{527}\) For example, Brightmail Inc. See Free Brightmail available at http://www.brightmail.com/individual (25 March 2004). Brightmail plants decoy e-mail addresses in various places on the Internet to be "harvested" unwittingly by spammers. The company's spam-filtering rules are based largely on messages received at these decoy addresses.

\(^{528}\) Online services are increasingly touting antispam features to differentiate their products from rivals amid fierce competition for subscribers. As of May 2003 Microsoft was blocking 2.4 billion e-mail messages targeting its MSN and Hotmail subscriber in-boxes every day. See further CNET News.com "Microsoft Unveils Antispam Tools" available at http://www.news.com.com/2100-1025_3-1000417.html?part=dht&tag=nhl (22 July 2003).
Even when filtering is performed by a destination operator rather than by end users, it is still an inefficient solution since the destination operator and intermediate networks still must devote bandwidth and storage capacity to receiving the message.

8.1.1 Pattern And Bayesian Filters

Many mail tools can filter out mail or redirect it based on analysis. Some filters search for known patterns or the names of known junk mailers. Other filters simply look for generic items uncommon in regular e-mail such as mail not directed at the user, or subject lines in all upper case.

Although these filters can be relatively effective, they do not offer a long-term solution. The filters can always be circumvented, and it becomes a war of escalation between the filter designers and the spammers. The patterns in most products can be decoded and the mailers simply learn not to use them.

Filters also do not assist in reducing server load. False positives often block legitimate mail and these filters will often block mail containing information about spam. They are sometimes put in place without recipient's knowledge, and users often don't receive notification that messages have been blocked. These filters also have the drawback that they are content based rather than volume based.
8.1.2 Domain Filters

Many mailers now refuse mail from domains that don't exist. These domain filters have proved to block a large amount of spam, however they have encouraged spammers to forge real people's domains. Domain filters also eliminate the ability to send legitimate anonymous e-mail.

8.2 Blacklisting

Several technological measures have been developed to enable destination operators to refuse delivery of spam. Many databases, sometimes referred to as blacklists or "blackhole lists", list Internet hosts frequented by spammers. These databases can be used to identify and refuse delivery of selected incoming messages. Many are publicly available online, and Internet service providers and individuals can subscribe to the list and use it to block all incoming messages that originate from addresses on it.

529 The term "blackholing" means denying delivery of any e-mail, or other data, coming from a certain Internet host, without returning a bounce message. The destination operator blocks the data coming from the blacklisted ISP and the data disappears without a trace, falling into a "blackhole". See Jargon 4.2, at http://www.science.uva.nl/-mes/Jargon/b/blackhole.html (25 March 2004).

"Like black holes, they are powerful and poorly understood - and escaping their grasp can be impossible. This has made them one of the most effective yet controversial weapons in the crusade against unsolicited e-mail".  

Individual blacklisting also helps ISPs identify potential subscribers who have been terminated by other ISPs for spamming.

It is arguable that the practice of blacklisting does more harm than good because legitimate e-mail is often lost in the process. If you have a black list that stops 100 percent of spam and 75 percent of legitimate mail, you have solved the spam problem, but you have created another problem.

There is a constant battle to keep such lists up to date, and the system is somewhat wasteful. There is a significant risk of blacklisting innocents, or those using the same ISPs as innocents. Some list operators use a "guilt-by-association" approach that places an entire ISP or hosting service on a blacklist merely because one of its users is a spammer.

---

For example, various organisations were placed on the Mail Abuse Prevention System (MAPS) list because of complaints that their Internet service provider, Media3 Technologies, refused to cut off service to companies suspected of doing business with spammers. MAPS blacklisted a group of Media3’s addresses, and ISPs using the MAPS list blocked e-mail coming from those addresses. Blacklist operators call this “collateral damage”, admitting that it is an unfortunate side effect. However, where users don’t realise that their outgoing e-mail messages are being blocked, this “collateral damage” can seriously hinder someone’s ability to communicate via the Internet.

Another problem that unintended victims of blacklists frequently encounter is that the people who compile the lists often keep a low profile. As a result, it is difficult for people whose service providers get blacklisted to appeal. Often, the only option for someone who gets blacklisted is to change ISPs. Blacklists could also be used by individuals or political groups to stifle opposing views, since many operators rely at least in part on customer complaints to compile their lists. Blacklists therefore have the potential to become tools for people's personal vendettas.

System administrators, fighting to prevent spam from crippling their networks, are more supportive of blacklists. They have to respond to complaints when their customers are inundated with spam, and they have to bear the expense
of the extra bandwidth and computer space needed to house the volumes of unwanted e-mail.

For network administrators, the lists are more useful than spam filters because they block offending e-mails before they reach the network. Blacklists are a more efficient option than e-mail filters, which can keep most offensive email out of recipients’ inboxes, but only after those emails have entered a company’s network. By the time the filter does its job, the recipient has already paid the price of handling the message.

Large e-mail hosts such as America Online, Microsoft and Yahoo can afford to develop their own blacklists, but smaller organizations typically rely on lists published by groups like MAPS, Spamhaus and SpamCop.

8.3 *Whitelisting*

Mailer programs using whitelisting filters learn all contacts of a user and let mail from those contacts through directly. Mail from strangers is redirected to other folders or challenged using the challenge and response technology described below. Whitelisting is relatively effective since they have a lesser chance of blocking legitimate e-mails, and they can be used in conjunction with other tools. They do, however, make anonymous and first contact messages difficult and there is often a delay in receiving mail from new contacts. Mailing lists must also be individually whitelisted.
8.4  Close "Open relays"

Open relays allow third parties to route their email through servers of other organisations, disguising the real origin of the e-mail.

United States regulators have identified 1000 potential open relays, 90 percent of which were in 16 countries, namely the United States, China, South Korea, Japan, Italy, Poland, Brazil, Germany, Taiwan, Mexico, Britain, Chile, France, Argentina, India, Spain and Canada. These open relays may exist on servers operated by governments, schools, businesses or any organisation with a server, or central computer.

Many of the open relays are on older servers with weaker security settings and may not be left open intentionally. According to Australia's Internet Industry Association, open relayed mail servers are proliferating worldwide, particularly in non-English speaking countries, because mail server systems are supplied with open relay enabled by default. A lack of documentation in the appropriate language meant that this is often left on. 14 United States and international agencies have drafted a letter, which was translated into eleven languages, urging the organisations to close their open relays to help reduce spam.

---

8.5 Turning Off Images Within E-mails

Microsoft's MSN 8 and Hotmail subscribers can elect to turn off images within e-mails. Images may conceal so-called "Web beacons" that confirm a particular e-mail address is in use. That's important to spammers, who frequently use dictionary attacks that blanket domains with thousands of random variations in the hopes of hitting a handful of targets. Beacons can be triggered when images appear in a preview window, meaning recipients do not need to open the file to be painted as a target.

8.6 Challenge-Response Technology

When an e-mail is sent to a "challenge-response" user, an e-mail is sent back asking the sender to verify that they are a life person. If the sender verifies that they are a life person by replicating a word and picked are displayed on the screen, the original e-mail is allowed through. The system automatically recognises future e-mails from the same sender, so the verification only needs to be performed once. Without verification, the e-mail is not delivered. Users are also able to automatically clear the e-mail addresses of friends, family members and other associates in their electronic address book, so those people would not receive the challenge e-mail.

Some networks already employ challenge-response technology when someone seeks to open an e-mail account. Microsoft is seeing progress in attacking Hotmail account hijacking, as a program aimed at hindering
spammers from using the service to ply their trade proves its worth. Microsoft has seen a 20 percent drop in new account registrations since it inaugurated its human interactive proof (HIP) program in December 2002. HIP aims to stop robots from creating accounts by requiring applicants to complete steps that are difficult for a machine to accomplish. Microsoft said the drop-off in sign-ups shows that fewer spammers are securing accounts.\(^5\) A variation of the system can also be used when an account holder is sending high volumes of e-mail.\(^6\)

The problem with this technology is that it is doubtful whether consumers will accept a process that add another step to e-mail delivery. It could also slow delivery of some e-mail, for example where a sender has walked away from their computer after sending an initial message and does not notice that a challenge has come back until much later. Senders may also not respond to the challenge email, or they may think that the challenge e-mail itself is spam.

Spammers could also start disguising emails as challenge e-mails to get people to open the messages. If large numbers of people begin to use the


system, user address books will be a target of hackers seeking to obtain lists of approved addresses.

Users would also have to use special email addresses when registering to purchase goods online, because vendors often send sales confirmation notices by computer.

9. Other Solutions

9.1 Hiding From Spammers

Spammers frequently compile mailing lists by "harvesting" e-mail addresses from Web pages, Usenet newsgroups, chat rooms, and public directories. Internet marketers can get e-mail addresses when people make their email addresses public by placing advertisements, inquiring about offers or participating in newsgroups or chat-rooms, or placing their email addresses on their Web site. Address lists are also created by stealing e-mail addresses from Internet mailing lists.

Internet users can reduce the amount of spam that they receive by making it harder for spammers to learn their e-mail addresses. Address concealment has become a common practice, but it may be impractical for Internet users who want to remain open to other communications.

537 In the same way an unlisted telephone number can help reduce telemarketing solicitations.
A more common technique is to disguise, or "munge", your address so that the correct address can be determined by other individuals, but not by address-harvesting software.

Internet users can also maintain multiple e-mail accounts and use web-based response services as methods of concealing their e-mail addresses from spammers, while still providing other people with a means of contacting them. Free e-mail services such as Hotmail are frequently used to obtain secondary or disposable addresses.

Another measure that has been used to combat address harvesting is the posting of Web pages containing very long lists of bogus e-mail addresses intended to frustrate harvesters by filling their lists with invalid or non-responsive addresses.

9.2 Opting Out

Some users reply to spam with an "opt-out" request, asking the sender not to send any further messages and to remove their e-mail address from its mailing list. Spam messages commonly include "opt-out" instructions, including an e-mail address or web page addresses (URLs) for submitting opt

---

out requests. These e-mail addresses and URLs often are invalid, or merely serve to confirm the validity of the address.

Individual "opt-out" requires each spammer to maintain their own list of removal requests and to honour those requests. This means that you would have to reply to every individual spammer and ask them to remove you from their lists. This would take even more time than just deleting the e-mail.

Opt out requests are relatively effective in other forms of direct marketing, such as direct mail and telemarketing, because the incremental cost of subsequent communication (including labour costs and printing and postage or telephone charges) discourages marketers from engaging in further communications with persons who have submitted "opt-out" requests. Since spam does not involve an analogous incremental cost, there is no incentive to respect "opt-out" requests, and it requires effort to remove a single address from a spammer's list.

9.2.1 Opt out lists

Consumers in America are calling for a "do not spam list", similar to the "do-not-call list"\textsuperscript{539} that has been created for telemarketing, to curb the number of

\textsuperscript{539} According to a survey conducted by an online research firm, Insight Express, of 300 consumers who have signed up to have telemarketing calls blocked, more than 8 in 10 respondents stated they wanted to see the government create the same sort of device to prevent unsolicited commercial e-mail from reaching their mailboxes. According to the respondents, spam is a bigger nuisance than telemarketing
marketing e-mails they receive. However, the Information Technology Association of America said such a law would be hard to implement and possibly counter-productive. This is because spam e-mailers are often located offshore, beyond the reach of US law enforcement, and within the US, the nearly instantaneous nature of the Internet itself makes spam easy to do but hard to trace.\textsuperscript{540} A "do not spam" registry could also fall into the hands of spammers, becoming a ready source of active e-mail addresses.

Various opt out lists have been operated over the past few years. There have been several "opt-out" lists calling themselves "global opt-out lists" or "global remove lists". Such lists are completely voluntary, and there is no incentive for spammers to use them. Few spammers even claim to use such lists, and fewer still actually do use them.

Almost all "opt-out" lists are currently operated by spammers. One major "opt-out" list, the IEMMC "opt-out" list, was put together by some of the largest spamming companies on the Internet at the time. Evidence showed over time that even some of the people involved in forming the list were not using it.

intrusions as, on average, consumers report receiving 16 times more spam than they do telemarketing calls. See further Mark "Do Not Call List Sparks Call For Similar Spam Plan" available at \texttt{http://www.clickz.com/news/article.php/2229621} (30 March 2004).
It is not in the spammer's interest to remove addresses from their lists - it is only in their interest to add addresses. Some people have supplied brand new e-mail addresses to these "opt-out" lists and soon after that have received spam from those addresses.

Even when a spammer decides to use an "opt-out" list, they have to decide which one to use. There are many lists to choose from, and the list administrators are generally not willing to cede any of their perceived power by combining their services. As a result, even where a spammer uses such a list, it will not clean their database of everybody who thinks they have opted out with the "global remove list". Few, if any, users are registered with all of these opt out lists.

"Opt-out" lists have therefore been discredited as being ineffective for stopping spam, and sometimes even for resulting in new spam.

9.3 Reporting And Retaliation

Another category of technical responses involves complaints and other retaliatory actions directed at spammers.

Users who receive spam may try to trace the message and complain to their ISP or the spammer's service provider. However, tracing spam can be extremely difficult. Spammers often forge message headers and omit other contact information such as telephone numbers and physical addresses.

Retaliation can go beyond the complaint stage. Some users have taken to more serious efforts, including methods that are illegal or which break Internet "rules". Spammers and their service providers have been subjected to flames, reputation attacks, invasions of privacy, email bombs and other denial-of-service attacks, and even threats of violence and property damage. "Canter & Siegel of CyberSell (the "Greatest Spammers of all Time") and Jeff Slanton (the "King of Spam"), have lived to regret their abuses of net educate. In retaliation, much of their personal information has leaked onto the Internet, and their e-mail boxes are often flamed, once to the tune of 30,000 times in one day". Such extreme retaliatory acts may be


542 See Howe Free On-Line Dictionary of Computing available at http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?flame (25 March 2004) defining "flame" as "An electronic mail or Usenet news message intended to insult, provoke or rebuke, or the act of sending such a message" or "To speak incessantly and/or rabidly on some relatively uninteresting subject or with a patently ridiculous attitude or with hostility towards a particular person or group of people".

543 This practice refers to sending, or urging others to send, massive amounts of electronic mail to a single system or person, with intent to crash or spam the recipient's system". See Howe Free On-Line Dictionary of Computing available at http://foldoc.doc.ic.ac.uk/foldoc/foldoc.cgi?mailbomb (25 March 2004)

somewhat effective in deterring spam, but they are often illegal and are not ideal solutions to the problem.

9.4  Digital Signatures

A digital signature that verifies the sender can be useful for non-anonymous mail. Digital signatures can be used for reliable whitelisting and blacklisting. In addition, the signature can come with a digital certificate stating the sender has agreed to a certain code of e-mail ethics.

Recipients could insist on such a certificate. Or the simple fact that the sender, and their ISP can be reliably identified may be enough to make people willing to give e-mail access, and divert non-signed mail.

Anonymous mail would be hampered by this scheme. Anonymous mailers must find some way to assert they are not abusing the system or recipients may delay, redirect or filter their mail. Valid methods include the use of re-mailers that protect the sender's identity but assured non-abuse.

9.5  E-Stamps And Pay Per View

It has been suggested that all e-mail messages should include some form of electronic payment. Recipients and destination operators could refuse to
accept messages not accompanied by sufficient payment, and recipients could choose to return the payment upon verifying the legitimacy of a message. Payments could be very small payments of a fraction of a cent per message, just enough to discourage large bulk mailings, or they could be substantial enough to compensate recipients for the time and resource costs that they incur and they could possibly even provide funds for other purposes.\textsuperscript{546}

Such a system works regardless of borders, and allows anonymous mail without abuse. However, it requires a substantial build-up of technical infrastructure and the redesign of mail systems.

9.6 Network Solutions

In the early days of the Internet, the computers that directed traffic were configured to relate communications without discrimination. As networks have evolved and multiplied this function is no longer required and many providers have configured their facilities accordingly. Spammers have found ways of identifying and using facilities that are not configured appropriately and to use them as relays for distributing the communications. For example,

\textsuperscript{546} A digital signature is a type of passport on the Internet that can be used to authenticate information about a user, including your name, country of citizenship, etc.

a spammer in South Africa could use an improperly configured server in Asia to relay spam to South African customers.

The Internet service industry and information technology suppliers therefore have a role to play in developing and implementing best practices for configuring network facilities to curtail abuse such as indiscriminate bulk e-mail.

Some service providers have already taken steps to curtail this abuse by refusing to accept communications traffic from improperly configured servers or from countries where a large number of facilities can be used for relaying inappropriate communications.

9.7 FTC E-mail Address

The Federal Trade Commission (FTC) in the United States encourages consumers to report spam and has established an e-mail address, uce@ftc.gov, where Internet users can forward offensive junk e-mail. According to the FTC, the address gets over 70,000 such e-mails a day. The FTC uses the unsolicited emails stored in its database\textsuperscript{547} to institute legal proceedings against persons who send spam in the United States. In March

\textsuperscript{547} The FTC has the most complete spam database in the world consisting of over 20 million messages. The collection is sorted into "libraries" viewable by date received or subject matter. The spam can also be searched and sorted using keywords. See further Wired News "FTC: Where Spam Goes To Die" available at http://www.wired.com/news/politics/0,1283,55972,00.html (22 July 2003).
and April 2002, the FTC shut down several Internet marketing operations that used spam.\textsuperscript{548}

The FTC can only legally pursue cases where there are clear instances of spam being used to perpetuate a scam or conduct fraudulent business activities. “The test is: Does the spam make a representation, an offer of some sort of product or service? Is that representation false? And would an average consumer believe that the representation was true?” Their mandate doesn't let them prosecute spam in general; they have to prosecute for things like fraud and deception.

It is submitted that the creation of a body to perform a similar role in South Africa would be beneficial to individual users and ISP’s. No organisation would want to be the subject of a test case and the law enforcement agencies have other competing priorities. These databases can also be useful for tracking spammers and for compiling statistics.

9.8 \textit{Require “ADV” Label In Header}

In theory, it would seem to be more efficient to require that spam include an affirmative statement indicating that the message is spam, rather than to require legitimate messages to include the negative statement that it is not spam. For example, it could become a requirement that “ADV” is added to

\textsuperscript{548} See further \textit{Wired News “Hypocrisy In Anti-Spam Land?”} available at
the start of a subject line to indicate that the message is an advertisement. Users could then customize their spam filters to either accept “ADV” labeled mail or automatically delete it.

The flaw in this solution is that legitimate marketers would probably be the only ones to use the labels. Spammers would have an incentive to lie in order for their messages to get through. Blocking of unlabeled messages would also be impractical until labeling became universal, and changes in most existing e-mail client software would be required to reach this stage. It would also make e-mail more restrictive than paper mail, since there is no similar requirement for paper mail. Definitional questions regarding what constitutes spam or other classifications subject to mandatory labeling would also be problematic.

9.8.1 Other Descriptive Labels

Another possible solution is to define a way to describe attributes of bulk e-mail, and e-mail from unknown parties. This method can be used to define a protocol to enable email servers to express what sort of mail they will accept, or tags to attach to e-mail describing how it is sent. This is a long term solution since it requires changing e-mail agents as well as e-mail sending tools.

The proposed tags would:

a) label the number of recipients of a message; and

b) flag the relationship between the sender and recipient (known or stranger; solicited or unsolicited; bulk or non-bulk).

Preferably the tags would be used in a protocol allowing mail servers to filter mail according to the attributes above. However, because most mail is relayed through several sites, it is not usually possible for the mail server that first receives a message to know the policies of the final recipient. As such, the tags would also need to exist within e-mail headers directly.

In their most basic form, mail transport agents and clients could be programmed to filter or redirect mail that had certain attributes. Mail would go into different destination mailboxes or "mail folders" based on these and other attributes.

This ability is already common in mail tools. Many mail tools have put in pattern based filters that can redirect or delete mail that contains certain "spam signature" strings in the text or subject. Should such protocols be defined and come into use, we can expect mail tools to very quickly adopt them with nice user interfaces.

\[549\] For notes on how protocol formalities might be implemented see Templeton "Bulk E-Mail Protocols And Tagging" available at http://www.templetons.com/brad/spam/tag.html (6 April 2004).
9.8.2 "Opt-Out" Protocols

These tags could form the basis of an "opt-out" protocol. If users wish to place a "no soliciting sign" on their mail server, they need a protocol to say in formal computer language what mail is welcome and what is not. The mail protocol could be extended to allow the recipient to express their preferences before mail is even sent. This is primarily in the interests of efficiency, to avoid having the recipient’s mail server take the load of receiving messages that are undesired and will be discarded anyway.

When servers "bounce" mail that was blocked due to tagging decisions, this bounce could be taken as an instruction to not send any more mail of the type bounced.

9.8.3 Making Labels Effective

The difficulty that arises with implementing a tagging system is how to make people who are already abusing e-mail put tags on their messages that may cause their messages to be declared 2nd class. With paper mail, senders are happy to put bulk-rate postage on their mail, thus tagging it as bulk, because they save money. This incentive is not present for e-mail tags.
There are several potential solutions to this problem:

a) Insisting on tags

Bulk-tags could become successful if recipients insisted that all mail they receive is tagged, and diverted all untagged mail to a low-priority folder. Users would also be able to divert mail tagged in ways they don't wish to receive.

This would require spammers to be honest, but spammers would have an incentive to lie in order for their messages to get through.

b) Voluntary Use

Many spammers would be happy to comply with a tagging system. In an effort to gain some respect, several spammers have proposed tagging systems of their own, including content-based ones. This because some spammers genuinely want to make a serious business out of bulk email, and they believe this will assist them.

c) Universal Use

Tags would be successful if they become popular enough that they were attached to almost all mail. In this event, people would be able to bounce or redirect mail that that does not have a tag attached to it.
A simple tag would have to be permitted for "small volume" person to person and small group e-mail mail. Email programmes could be programmed to add this special tag without any effort by the user. Only bulk mailing programs (programs that explode to mailing lists) would need to worry about the fine points of the attributes being tagged.

Again, this does not address the problem of people who would deliberately lie on their tag.

d) Trademark Protection

A tagging scheme could be enforced by placing a valid trade mark on the name of the tag, and allowing the mark to be used only by those who follow proper standards of email ethics. Use without following the rules would be a violation, which could result in litigation.

e) Tagging laws

Already some legislatures have proposed laws requiring tags, such as "advertisement" in the Subject line. A law which requires an honest bulk-tag on bulk mail from strangers, or which simply clarifies that lying on such a tag is fraudulent could be effective.
9.8.4 Electronic Seal Of Approval

The idea of a self-governing organisation that could issue an electronic seal of approval for "legitimate" senders of commercial e-mail has been supported by several of the big Internet e-mail account providers, particularly Microsoft. The proposal is that companies could forgo other labels, such as ADV labels, if they join a "trusted sender" program that mandated email marketing rules, such as ensuring that consumers are removed from mailing lists if they request it.

An independent third party would issue an electronic seal of approval for "legitimate" senders of commercial e-mail, thereby making it easier for computer users to filter out mail from unsavoury or fraudulent spammers. The self-regulation plan creates a grievance process for individual consumers who might otherwise have trouble getting the attention of law enforcement authorities when marketers continue to target them. The proposal establishes a complaint mechanism that the self-policing group must follow.\(^550\)

10. Limitations Of Technical Approaches

Unfortunately, none of the filtering and blocking technologies are perfect. Most of them cost money to implement on a widespread basis, interfere with some legitimate message traffic, allow some spam through, and fail to

eliminate many of the costs imposed by spam. Advances in filtering and blocking technology thus far seem to have been matched by advances by spammers in circumventing such measures.

While technological measures are the most flexible approach to spam, spammers have consistently succeeded in adapting their techniques to circumvent advances in anti-spam technology.\textsuperscript{551} Therefore, technical approaches are unlikely to eradicate spam completely, partly because of the time and resources that spammers devote to their activities and partly because of the inherent openness of the Internet and e-mail protocols.

Another problem with technical approaches is the harmful effects that they can have on legitimate communications. Up to 10 percent of legitimate e-mails are never received because of automatic volume, content and black-list based filtering tools.\textsuperscript{552} Blocking e-mail traffic from a spam-friendly site often means blocking a great deal of legitimate e-mail as well. Closing down an open relay that has been used for sending spam as well as for legitimate purposes can be inconvenient for many users. Blacklists only capture 10 percent of spam and often eliminate valid e-mails as well.

\textsuperscript{551} A study by ZDNet's eTesting Labs found that even the best filter available still let more than a quarter of the spam through. See http://www.theregister.co.uk/content/archive/11416.html (1 April 2004).

The costs of implementing technical mechanisms is also of great concern. These costs are often passed on to users and are ongoing because of the need to constantly update technical solutions.

Finally, technical approaches have been criticized for a lack of transparency and accountability. For example, blacklist maintainers do not disclose the criteria that they use for blacklisting and wrongly accused spammers usually have no way of contacting blacklisters to be cleared.

PART C: CONSUMER AWARENESS

11. Introduction

On an individual level, education and sound responsible e-mail use is probably the best protection against spam. Irrespective of how many laws are enacted or how many regulations are imposed, the Internet will always present enforcement challenges. For this reason, well informed consumers will remain a key element in the orderly development of the Internet and its use. Users should not open spam emails, they should not click on boxes requesting further information, and they should never accept what is on offer via spam e-mail.

In the United States, the FTC has focused on consumer education to combat spam. It has released a "dirty dozen" list of the top "spam scams" being sent around the Internet. The FTC has also created its own web sites that lure
consumers in with get-rich-quick offers, but then within a few clicks explains the dangers of pursuing these often shady business opportunities. 553

12. Consumer Complaints

Initially, spam was reacted to with ire by recipients, and this has helped significantly to deter legitimate companies away from using junk e-mail. Consumer reactions to spam has led many ISPs to change their policies, and it has made legitimate companies very wary of engaging in this type of activity. Consumer complaints have also made legitimate companies fairly good about working list-removal.

Consumer complaints, however, have the negative effect of placing a severe burden on ISPs handling valid complaints and invalid complaints. The forging of email also often results in complaints being lodged against the wrong person.

Often spam comes from places that the recipient has previously had contact with, such as web sites they gave their e-mail address to or companies they have done business with. Consumers should be encouraged to complain directly to these companies, because revolt and anger by customers is far more effective than anger at strangers. Companies should be pushed to

disclose what they will do with any data they collect from a customer/user, and be forced to adhere to that disclosure.

13. **Consumer Responsibility**

Many products and services on the Internet are provided with no charge to users. However, consumers should bear some responsibility for verifying what conditions may be attached to these free products and services. Most Web sites contain privacy policies that will explain how personal information provided by customers will be protected or used for other purposes.

Consumers should also be aware that certain areas of the Internet, for example newsgroups, have very little or no security. Consumers should be aware that they may be exposing their e-mail address to public view.

**PART D: CONCLUSION**

It is submitted that spam can only be defeated by a combination of legal measures, informal measures, technical measures and consumer education. The above Chapter therefore discusses various alternative solutions that are available to supplement the law.

In terms of technology, filtering technologies are being developed that are easier for consumers to use and are more effective in determining which e
mail messages are spam and which are desired communications. These technical measures are supplemented by informal measures, including self-regulation efforts by the industry and social norms. Finally, consumer awareness will play an important role in complementing the various approaches to eliminate spam.
1. Introduction

Part A of this Chapter outlines the need for direct anti-spam legislation in South Africa. At the SA Spam Summit, held on 22 October 2003, the Department of Communications stated that it "is likely to amend the ECT Act, taking into consideration the fact that at the time at which the legislation was developed spam did not represent the current challenges."\(^{554}\) The Department of Communications, however, recognised that the current spam provisions in the ECT Act have served to create awareness of the problem.

According to Ant Brooks, regulatory chairman of the Internet Service Providers Association ("ISPA"), ISPA has been asked by the Department of Communications to propose legislation for combating spam.\(^{555}\) Part B of this Chapter suggests various clauses that will need to be addressed in the legislation.

Part C provides a general conclusion for the present Chapter.

PART A: GENERAL INTRODUCTION

2. Introduction

Simple and direct legislation is required to effectively stop the South African contribution to the problem of spam. While we need to accept that there is some spam activity which originates outside our borders that we will not be able to control, we cannot avoid the responsibility to eliminate our own spam output.

The Internet is an international medium, and we can only control activities that take place within South Africa. However, as more jurisdictions enact spam legislation, spam legislation in general will become more effective and pressure can be applied on countries that have not enacted spam legislation.

Legislation in South Africa would have a positive effect on the spam problem, even without equivalent legislation in other jurisdictions. Legislation could eliminate the South African contribution to the problem, and prevent South African interests from using offshore facilities for spam.\textsuperscript{556} There are many South African spammers, and there are also many foreigners who send spam from South Africa out to the rest of the world. Therefore, efforts to

\textsuperscript{556} Thereby closing the back door to spammers attempting to avoid the legislation.
control the problem in South Africa could also bring about an appreciable
difference in the volume of spam globally. 557

Legislation in South Africa could also serve as an impetus for other countries
to implement similar legislation. While South Africa looks to other countries
to see what they are doing, many other countries, including major world
powers and other African countries, similarly examine what South Africa has
done when considering their own policies. If legislation is passed in South
Africa, it would also give South Africa leverage in the international arena to
courage other governments to follow suit so that we can start moving
towards a global solution.

Anti-spam lobbyists hope that Australia’s "opt-in" legislation banning the
sending of unsolicited junk electronic mail will put pressure on other countries
in the Asia-Pacific region to adopt similar measures. 558 According to Josh
Rowe, 559 "the more countries that put in this kind of "opt-in" legislation, where
people have to give permission to receive email, the more it pushes out
countries who don’t have that legislation and it kind of puts them into the
Third World of the Internet".

557 Crabb "Legislation Will Outlaw Junk E-Mails" The Age 24 July 2003 available at
558 Adams “Nations Move Closer To Anti-Spam Legislation” The Age 22 July 2003
available at
559 A founding member of the anti-spam group Coalition Against Unsolicited Bulk E-
mail (CAUBE.AU) and Australia’s representative at the recently formed Asia-Pacific
Coalition Against Unsolicited Commercial E-mail (APCAUCE) forum.
3. **Issues To Be Addressed**

The core issues that will need to be addressed in spam legislation include the definition of spam, "opt-in" rather than "opt-out", the penalties that should be in place for people breaking anti-spam laws, the issue of whether spammers should be open to civil actions and what types of business-to-customer e-mails should be exempt.

Direct legislation is required which:

a) bans the practice of transmitting spam;

b) bans the sale of tools designed for transmitting spam;

c) provides a right of action to the recipient, together with suitable damages;

   and

   d) provides a right of action to ISP's, together with suitable damages.

---

**PART B : FRAMEWORK FOR ANTISPAM LEGISLATION**

4. **Introduction**

Suggested clauses to be inserted into specific anti-spam legislation are outlined below. The commentary in these sections may be included in a guide document to be published in conjunction with the legislation.\(^{560}\)

---

5. **Purpose**

The purpose of the legislation should be:

a) to provide strong, effective and sensible solutions to limit the growth of spam and give users meaningful control over their inboxes;

b) to prohibit a person or entity from bulk e-mailing, or causing to be bulk e-mailed, documents consisting of unsolicited material; and

c) to provide safeguards for users against intrusion of their privacy by unsolicited communications by means of e-mail.

6. **Definition Of Spam**

Spam should be defined as "unsolicited, bulk, e-mail". This definition should not be restricted to "unsolicited, bulk, commercial, e-mail".561

7. **Definition Of E-mail**

Under the ECT Act, 'e-mail' is defined as:562

"electronic mail, a data message used or intended to be used as a mail message between the originator and addressee in an electronic communication".

---

561 The advantages and disadvantages of UBE versus UCE are discussed in Chapter 2 above. As discussed in Chapter 3 above, section 45 of the ECT Act only provides for unsolicited commercial communications.

562 Section 1.
It may be useful to expand this definition along the lines of the Australian Spam Act 2003\textsuperscript{563} and the proposed California Act.\textsuperscript{564}

The Australian Spam Act defines an electronic message as follows:

“(1) For the purposes of this Act, an electronic message is a message sent:

(a) using:

(i) an Internet carriage service; or

(ii) any other listed carriage service; and

(b) to an electronic address in connection with:

(i) an e-mail account; or

(ii) an instant messaging account; or

(iii) a telephone account; or

(iv) a similar account.

Note: E-mail addresses and telephone numbers are examples of electronic addresses.\textsuperscript{565}

(2) For the purposes of subsection (1), it is immaterial whether the electronic address exists.


\textsuperscript{564} Senate Bill No 186 (2003) available at http://www.spamlaws.com/state/ca1.html (18 September 2004). This Act was superseded by the enactment of Federal legislation.
(3) For the purposes of subsection (1), it is immaterial whether the message reaches its intended destination".

The California Act provides:

"(f) "Electronic mail" or "e-mail" means an electronic message that is sent to an e-mail address and transmitted between two or more telecommunications devices, computers, or electronic devices capable of receiving electronic messages, whether or not the message is converted to hard copy format after receipt or is viewed upon transmission or stored for later retrieval. "Electronic mail" or "e-mail" includes electronic messages that are transmitted through a local, regional, or global computer network.

(g) "Electronic mail address" or "e-mail address" means a destination, commonly expressed as a string of characters, to which electronic mail can be sent or delivered. An "electronic mail address" or "e-mail address" consists of a user name or mailbox and a reference to an Internet domain".

566 The inclusion of telephone numbers as an example of an electronic address will become more important as the use of cell-phones as an e-mail account increases. See the discussion on Japan in Chapter 4.
8. **Establish "Opt-In" Rather Than "Opt-Out"**

Cross-border enforcement against spam will only be effective if countries adopt similar legal requirements. "Opt-in" is the approach that all European countries will adopt under the Directive on Privacy and Electronic Communications 2002.\(^566\) It is also the approach adopted by Australia under the Spam Act of 2003.\(^567\)

It is also not practical to require multinational companies to operate on an "opt-out" basis when sending emails to people in South Africa and an "opt-in" basis for when sending e-mails to people in other countries.

Under the "opt-in" approach, bulk e-mails should only be sent with the recipients' prior affirmative agreement. This will require that prior explicit consent is obtained before such communications are addressed to them.

There should be an exception for previously existing business relationships, whereby in the context of an existing customer relationship, companies may continue to send e-mails to market similar products on an "opt-out" basis.

---

\(^{566}\) Directive 2002/58/EC. See further Chapter 3.

9. **Consent**

Under the Australian Spam Act, consent means:

"(a) express consent; or

(b) consent that can reasonably be inferred from:

(i) the conduct; and

(ii) the business and other relationships;

of the individual or organisation concerned".

9.1 **Express Consent**

Express consent from an addressee is where that person has specifically requested messages to be sent to them. Examples include where the recipient has subscribed to an electronic advertising mailing list; or where the recipient has deliberately ticked a box consenting to receive messages.

9.2 **Inferred Consent**

Inferred consent is where the person a sender wishes to contact has not directly instructed the sender to send them a message, but it is still clear that there is a reasonable expectation that messages will be sent.

It may be reasonable to infer consent after considering both the conduct of the addressee and their relationship with the sender. For example, if the
addressee has an existing relationship with the sender and has previously provided their address then it would be reasonable to infer that consent has been provided. Inferred consent would probably apply to a regular customer, but not to a once off customer.

According to the Australian Communications Authority, other examples of where consent may be inferred include:

a) when purchasing goods or services an addressee has provided their electronic address in the general expectation that there will be follow-up communications;

b) when an addressee has provided their address with the understanding that it would be used in day-to-day transactions (such as online banking or business), and may be used for additional communications (for example notification of related services or products);

c) online registration of a product or a warranty;

d) when an addressee has conspicuously published their electronic address. In such a case the Spam Act permits commercial electronic messages to be sent to the addressee, if the message relates to the addressee’s published employment function or role. If a plumber advertises their email address, it is acceptable to send them offers of work or of plumbing supplies, but not to send an offer unrelated to their work, such as cheap

---

568 Schedule 2 clause 2.
569 See The Australian Communications Authority "Spam Act 2003: A Practical Guide For Business" available at
pharmaceuticals. If the published address is accompanied by a statement saying that it should not be used for such messages, such as the words "no spam", then it cannot be used to infer consent to a message being sent;

e) similarly, when an addressee has provided a business card containing their electronic address, it would be a reasonable expectation on both sides that relevant messages should be sent to that particular electronic address. For example, if the business card was provided for work purposes then it would not be reasonable to infer that the addressee consented to receiving messages from you which are unrelated to their work.

Therefore, consent may not be inferred from the mere fact that an electronic address has been published.

9.3 Existing Relationships

It is possible for senders to infer consent based on the status of their relationship with the addressee, as long as it is consistent with the reasonable expectations of the addressee, and their conduct. An existing business or other relationship may, for example, be a relationship that was initiated by a commercial activity (including provision, for a fee or free of
charge, of information, goods, or services) or other communication between
the sender and potential addressee.

According to the Australian Communications Authority, the following
examples might suggest that a business, or other, relationship exists from
which a sender may reasonably infer consent:

a) persons who have purchased goods or services which involves ongoing
   warranty and service provisions;

b) shareholders;

c) magazine and newspaper subscribers;

d) subscribers to a service;

e) registered users of online services;

f) utility or rate payers (i.e. in a business relationship with utility
   company/government body);

g) subscribers to information/advisory services;

h) financial members of a club;

i) professional association members;

j) members of frequent flyer or buyer clubs;

k) bank account holders;

---

See The Australian Communications Authority "Spam Act 2003: A Practical
Guide For Business" available at
practical_guide.pdf (29 April 2004).
l) superannuation subscriber;

m) employers and employees; or

n) contractors.

Consent will not always be inferred where there is a pre-existing relationship between the sender and a potential addressee. For example, it would not be reasonable to infer that a person consented to receiving electronic messages simply because of a transaction along the lines of any one-off purchase. Transactions such as the purchase of a t-shirt or groceries from a shop, attendance at a concert, performance or movie, would not be a valid basis for inferring consent, or assuming that there is a pre-existing relationship.

9.4 Contact Lists

Since spam must only be sent with consent, it is immaterial when the contact list was gathered, or how it has been used. What is important is that the sender has either express or inferred consent to contact each addressee on the contact list. If there is any uncertainty about the consent of the potential addressee, senders must seek confirmation from that addressee that commercial electronic messages may be sent to them.
A ‘double opt-in’ process\textsuperscript{571} (sometimes also referred to as a ‘closed-loop confirmation’) can be used to validate that an addressee has consented to receiving commercial electronic messages and provides proof that the consent of the addressee has been obtained. A double "opt-in" process, whether it is an automated system or a manual procedure, is recommended where it is difficult to validate whether the potential addressee has actually consented. These instances can occur when dealing with online subscriptions, requests from third parties and other occasions where consent has not been given at the time of a personal communication or transaction.

Section 45(1)(b) of the ECT Act, provides that the sender must provide the consumer "with the identifying particulars of the source from which that person obtained the consumers' personal information, on request of the consumer". This section provides important consumer protection by assisting consumers to trace the source from which their information was obtained, and should be inserted into the new Act.

\textsuperscript{571} With a typical double opt-in process, the business receives a message saying that an electronic address should be added to their contact list for commercial messages or company newsletters. The business sends a message to that address, requesting confirmation that messages should be sent there in future. The message also contains a notification that they will only be added to the contact list if they send a positive confirmation within 14 days. After 14 days, if there has been a positive confirmation, the address is added to the contact list. If there has been a negative response, or if there has been no response, the address is not added to the contact list for future messages.
10. **Accurate Sender Information**

Electronic messages must include clear and accurate information and contact details about the individual or organisation responsible for sending the message.

To facilitate effective enforcement, the use of false identities or false return addresses or numbers must be prohibited.

This information must be valid for at least 30 days after the message is sent.

11. **Functional Unsubscribe Facility**

Section 45(1)(a) of the ECT Act, which provides that the sender must provide the consumer "with the option to cancel his or her subscription to the mailing list of that person", should be expanded.

Senders must be required to establish a toll-free telephone number and a valid return email address that a recipient may contact to notify the sender not to e-mail any further unsolicited documents.

---

572 See the discussion on Korea in Chapter 4.
All messages must contain an "opt-out" facility, for recipients to indicate that they do not wish to receive such messages in the future and that they wish to unsubscribe, even where the e-mail was requested.

The unsubscribe facility must be reasonably likely to be functional for a period of 30 days after the message was sent.\(^{573}\)

Where a recipient has sent an unsubscribe request, this request must be honoured within a definite period, and the e-mailing of unsolicited documents to a person who has requested not to receive them must be prohibited. The Australian Spam Act provides that the withdrawal of consent takes effect after 5 business days.\(^{574}\)

12. **Identification As Unsolicited**

Messages should be clearly and unambiguously identifiable as spam as soon as they are received by the recipient. For example, messages may be required to contain headings such as "Advertisement" or "Advertisement for Adults."\(^{575}\)

\(^{573}\) Similar to section 18 of the Australian Spam Act.
13. **Tools Designed For Transmitting Spam**

Tools designed for transmitting spam must be prohibited.

Messages must not be sent to a non-existent electronic address unless the sender has reason to believe that the electronic address exists. In other words, "dictionary spamming" and sending mail to other randomly generated e-mail addresses must be prohibited.

Address-harvesting software is a computer program that is designed to automatically collect electronic addresses from the Internet. The software searches public areas such as Web pages, newsgroups, chat rooms and other online directories to compile or ‘harvest’ lists of addresses.

Address-harvesting software and harvested-address lists are often used for legitimate purposes such as collecting data for research, marketing or maintaining Web sites; but they are also often used to create distribution lists for sending spam.

Address-harvesting software must not be supplied, acquired or used, and an electronic address list produced using address-harvesting software must not be supplied, acquired or used.

---

574 Schedule 2 clause 6.
575 See Chapter 4 – Legislation enacted in South Korea.
The Australian Spam Act defines address-harvesting software as:  

"software that is specifically designed or marketed for use for:

(a) searching the Internet for electronic addresses; and

(b) collecting, compiling, capturing or otherwise harvesting those electronic addresses".

The Australian Spam Act defines a harvested address list as:

"(a) a list of electronic addresses; or

(b) a collection of electronic addresses; or

(c) a compilation of electronic addresses;

where the production of the list, collection or compilation is, to any extent, directly or indirectly attributable to the use of address-harvesting software".

14. **Multiple E-mail Addresses**

The registering of multiple email addresses for the purpose of unsolicited bulk e-mail must be prohibited.

15. **Penalties**

Penalties for contravention of the legislation must include fines, civil actions for damages and interdicts, and criminal liability. Individuals as well as ISPs

---

Section 4.
should have the right to bring civil actions against spammers for interdicts and damages.

16. **Jurisdiction**

Under the Australian Spam Act it is illegal to send, or cause to be sent, unsolicited commercial electronic messages that have an Australian link. A message has an ‘Australian link’ if it either originates or was commissioned in Australia and is sent to any destination, or originates overseas but has been sent to an address accessed in Australia.

The Australian Act suggests that exemptions may include instances where the sender did not know; and could not, with reasonable diligence, have ascertained that the message had an Australian link. A person who wishes to rely these exemptions bears an evidential burden in relation to that matter.

It is submitted that section 90 of the ECT Act goes further than this provision and should be imported directly into the new legislation.

17. **Review**

Government should be compelled to regularly review the effectiveness of the legislation. In the United States of America, in terms of the CAN SPAM Act,  

---

Section 7.
the FTC is required to report back to Congress within two years on the
effectiveness of the law and the need, if any, for modifications.\textsuperscript{578}

\textbf{PART C : CONCLUSION}

South Africa has a responsibility to eliminate our own spam output through
specific anti-spam legislation. This legislation should provide a definition of
spam, and it should adopt the "opt-in" approach.

The legislation must ban the practice of transmitting spam, and the sale of
tools designed for transmitting spam. The legislation must also provide a
right of action to the recipient and to ISP’s, together with suitable damages.

The commentary on the application of the various sections provided above
should be included in a guide document to be published in conjunction with
the legislation.

\textsuperscript{578} See Chapter 4.
ADAMS D

"Nations Move Closer To Anti-Spam Legislation" *The Age* 22 July 2003
available at

"New Spam Laws A Little Hit And Miss" available at

AGRE P

"How To Complain About Spam, Or, Put A Spammer In The Slammer"
available at http://dlis.gseis.ucia.edu/people/pagre/spam.html

ALMAGUER AE & BAGGOT RW

"Shaping New Legal Frontiers: Dispute Resolution For The Internet" *Ohio

ANSTEY G


ASARAVALA A

"With This Law, You Can Spam" available at

"FTC Says No To Antispam Registry" *Wired News* available at
ASHFORD W

"Legitimate Marketers Slam Spam" available at

ASIC

"Two Years Jail – Suspended – For Internet Spammer" available at
http://www.fido.asic.gov.au/fido/fido.nsf/byid/1B1AC613B3225EA5CA256B0B02B5940?opendocument

BAILEY S

"The Rise Of E-Mail Marketing" available at

BANFIELD R

"Where To For Internet Advertising?" available at

BASELEY WD

"Address Munging FAQ: Spam-Blocking Your E-Mail Address" available at
http://members.aol.com/e-mailfaq/mungfaq.html

BOBERG PQR

BORTZ T AND LOUW L

"The Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002" available at http://www.werksmans.co.za

BRINKMAN L


BURCHELL J


BURNS Y


BURNSTEIN M


BUSINESS DAY


BUYS R

"The Use Of E-Mail Blocking Software Will Soon Be Illegal In South Africa"

CHANG R

"Could Spam Kill Off E-Mail?" Medill News Service available at
http://www.pcworld.com/resource/printable/article/0,aid,113061,00.asp.

CHASKALSON M, KENTRIDGE J, KLAAREN J, MARCUS G, SPITZ D &
WOOLMAN S


CHELLAM R

"Singapore Gets Behind Drive To Can Spam" available at
http://www.business-
times.asia1.com.sg/sub/premiumstory/0,4574,86574,00.html?

CHISSICK M AND KELMAN A

London.

CNET NEWS.COM

"Microsoft Unveils Antispam Tools" available at

CNN

"First Four Charged Under 'Can Spam' Law" available at
COOLTECH.IAFRICA.COM


COALITION AGAINST UNSOLICITED BULK E-MAIL, AUSTRALIA (CAUBE.AU)


COHEN T


CRABB A


CRANOR L and LAMACCHIA B


DE JAGER C AND SMITH E

DELO M

"Breaking News: Most Spam Is Bogus" Wired News available at

"Spammers Top Microsoft Hitlist" Wired News available at

DEOK-HYUN K

"Unsolicited E-Mail Senders Fined" available at
http://www.korealink.co.kr/kt_tech/200204/t2002042917210545110.htm.

DEVENISH GE

A Commentary on the South African Bill of Rights (1999) Butterworths:
Durban.

DE WAAL J, CURRIE I, ERASMUS G


DE WET P

"Big Brother Employers Outlawed" available at

DIROM P

"Employers' Rights To Monitor Employee Email Under United States Law"
available at
http://www.murdoch.edu.au/elaw/issues/v8n4/dirom84_text.html#t47
DUGARD J


DU PLESSIS JR AND KOK L


EBERSOHN G


ELECTRONIC COMMERCE IN CANADA


"Are Unsolicited Email Messages Illegal In Canada?" available at [http://strategis.ic.gc.ca/SSG/1/sh50527e.html](http://strategis.ic.gc.ca/SSG/1/sh50527e.html).


EUROCAUCE

Bibliography

FALK JD

"The Net Abuse FAQ Revision 3.2" available at

FEDERAL TRADE COMMISSION OF THE UNITED STATES

"FTC Announces First Can-Spam Act Cases" available at

FINDLAW.COM

"What Is "Spam" And How Can It Be Avoided?" available at
http://www.findlaw.com/business_commercial/business_operations/source/faq
s/faq445.

"You’ve Got Spam" available at

FLETCHER T

"May I Read Your E-Mail? Please…” available at
=0&CTRL=S.

FOLEY K

"E-Mail: The Wonder Tool" available at
FOSTER E

"Viral Marketing Goes One Step Too Far – To A Place Where Friends Spam Friends" available at
http://www.infoworld.com/articles/op/xml/00/02/07/000207opfoster.xml.

FREE BRIGHTMAIL


FROOMKIN


GATES B

"Letter From Bill Gates To The U.S. Senate Commerce Committee Regarding Spam Hearings" available at
http://www.microsoft.com/presspass/misc/BillgSpam05-21-03.asp.

"On Spam: Wasting Time On The Internet (3/25/98)" available at

GEOCITIES CANADA

"Freedom Of Speech And The Limits" available at

GEREDA S

GIGANTE A


GUEDES G

"Industry Concedes Spam Is Here To Stay" *ITWeb* available at

"The Proudly South African Spammer Is Born" available at

HAHLO HR AND KAHN E


HAMBRIDGE S


HANSEN E AND OLSEN S

"Spam: It’s More Than Bulk E-Mail" available at

HAWKEY S

"Culture Jammers" available at

HAZEN MUELLER S

"Should I Hit "Remove"?" available at
http://www.spam.abuse.net/overview/remove.shtml.
"What Is Spam?" available at

HILLER J AND COHEN R


HISE P

"Mom Spam: The Cyber-Scourge Of Families Everywhere" available at

HOAXBUSTERS


HOFFMAN P

Internet Mail Consortium Report: "Unsolicited Bulk E-Mail: Definitions And

HORMEL FOODS CORPORATION


HOWE D

"Free Online Dictionary Of Computing" available at
http://wombat.doc.ic.ac.uk/foldoc/foldoc.cgi?

INDUSTRY CANADA

"Internet And Bulk Unsolicited Electronic Mail (SPAM)" available at http://e-
INTERNATIONAL LAW OFFICE

"New E-Commerce Act Mirrors Directive" available at

http://www.internationallawoffice.com/Ld.cfm?i=45338&Newsletters__Ref=7038.

JAPAN TODAY NEWS

"Law On Unsolicited E-Mail Takes Effect" available at


JAQUES R

"Three In Five E-Mails Will Be Spam In 2004" available at


JOHNSON DR AND POST DG

(1996) volume 1367 page 4, available at


JOUBERT WA (founding editor)

The Law of South Africa(1997) First re-issue volume 19 Butterworths:
Durban.

JUNNARKAR S

KADOw

Kadow’s Internet Dictionary available at
http://www.msg.net/kadow/answers/s.html

KAPADIA R

"Spam Is Here to Stay" available at

KINGDON J

"How To Complain To The Spammer's Provider" available at
http://spam.abuse.net/spam/howtocomplain.html

KRIM J

"Self-Policing Added To Spam Bill" Washington Post 18 September 2003

LEMKE T

"China Blocks 127 Spam Servers" The Washington Times available at

"Valid E-Mail Thrown Out With Trash" The Washington Times available at

LESSIG L

LEVINE J

"Why Is Spam Bad?" available at

LLOYD IJ


MACAVINTA C

"Report: FTC Should Slam Spam" *CNET News* available at

MACKENZIE K

"Spam Crackdown Goes Global" available at

MAIL ABUSE PREVENTION SYSTEM


MARK R

"Bush Signs Can Spam Bill" available at

"Do Not Call List Sparks Call For Similar Spam Plan" available at

"Welcome To Spam Week" available at
MCCURLEY K


MCGUIRE D


MCKERRON RG


MCQUOID-MASON DJ


MENTHE D

"Jurisdiction In Cyberspace: A Theory Of International Spaces"

METCALFE B


http://www.infoworld.com/cgi-bin/displayNew.pl/?metcalfe/bmOl2O97.htm:

MEYER T


MICHALSON L

"The Law Vs The Scourge Of Spam" available at


MILTON JRL


MIYAKE K

"Spam-Blocking Law Proposed In Japan" available at


MOOREFIELD G

"SPAM – It's Not Just For Breakfast Anymore: Federal Legislation And The Fight To Free The Internet From Unsolicited Commercial E-mail" *Boston University Journal of Science and Technology Law* volume 5 page 10.
MORRISSEY B

"The Threat Of Eternal Spammation" available at

MSN.CO.ZA

"About Junk E-Mail" available at

MWEB

"Terms and Conditions of Use" available at
http://www.mweb.co.za/policies/subscriber_terms.asp

NAE-SUN P

"Daum Files Suit Against Spam-Mail Senders" Chosun.com : available at

NANDOTIMES.COM

"Danish Company Fined Over Spam Campaign" available at

NATIONAL OFFICE FOR THE INFORMATION ECONOMY (NOIE)

"Spam" available at

NEETHLING J, POTGEITER JM & VISser PJ

NELSON R

"The Definition Of E-Mail Spam" available at

NEWS24.COM

"Americans Want Spam Ban" available at

"127 Spam Servers Blocked" available at

OPPERMAN D AND GOODBURN D

"Licence To Bug Only In Exceptional Circumstances" Business Day Monday 8 March 2004.

OUT-LAW.COM

"First UK Ruling Under New Rules On E-Mail Marketing" available at

"Misleading E-Mail Headers: ASA Warns Marketers" available at

RICH LL


SANG-HUN T


SAUNDERS C


SCOTT I


SILICON.COM


SMITH R

"Corporate Crime In The Digital Age" available at
http://www.lawbookco.com.au/academic/Corporate-Misconduct-

SNYMAN CR


SORKIN DE


SPAMHAUS PROJECT

"The Definition Of Spam" available at
http://www.spamhaus.org/definition.html

STEIN P, PATEL S AND TSHEPE D


STRASSEL K

"Web Censorship In Germany" Wall Street Journal 13 May 1998 available at

STREET FL AND GRANT MP

TAYLOR W

"Permission Marketing" available at

http://www.fastcompany.com/magazine/14/permission.html.

TEMPLETON B

"Bulk E-Mail Protocols And Tagging" available at


"Commentary On Ad-Hoc Working Group On UCE" available at


TECHSMART

"SA Spam Summit An Unequivocal Success" Issue 6/1.

THE ADVERTISING STANDARDS AUTHORITY OF SOUTH AFRICA

Web site available at http://www.asasa.org.za

THE ADVERTISING STANDARDS AUTHORITY OF THE UNITED KINGDOM

ASA "CAP Code" available at


THE ASSOCIATION FOR INTERACTIVE MEDIA

"Responsible E-Mail Marketing: Resolutions Hailed At Net.Marketing Conference In Seattle" available at

THE ASSOCIATION OF LAW SOCIETIES OF THE REPUBLIC OF SOUTH AFRICA


THE AUSTRALIAN COMMUNICATIONS AUTHORITY


THE CANADIAN MARKETING ASSOCIATION

Web site available at _http://www.the-cma.org_.

THE DIRECT MARKETING ASSOCIATION OF THE UNITED STATES

DMA Privacy Promise Member Compliance Guide available at _http://www.the-dma.org/library/privacy/privacypromise.shtml_.

THE EUROPEAN ADVERTISING STANDARDS ALLIANCE

Web site available at _http://www.easa-alliance.org_.

THE INTERNET ALLIANCE

"IA Addresses Unsolicited Bulk E-mail" available at

_http://www.internetalliance.org/policy/spamming_guidelines.html_.

THE MAIL ABUSE PREVENTION SYSTEM

Web site available at _http://www.mail-abuse.org/dul_.

THE MARKETING FEDERATION OF SOUTHERN AFRICA

Web site available at _http://www.mfsa.co.za_.

THE SPAMHAUS PROJECT


THE STAR

"Are You Also Sick Of ‘Spam’?" 15 July 2003.

THE WASHINGTON TIMES


THIS DAY

"Drowning In Spam" 23 October 2003.

THORNTON L


UHLIG R

"We Can’t Stop E-Mail Spam, Says MP" available at http://www.telegraph.co.uk
UNIDROIT

General Principles of International Commercial Contracts, available at

UNLIMITED FREEDOM OF SPEECH

Web site available at

VAN DER MERWE CG

"Neighbour Law" Law of South Africa (1997) First Reissue volume 27
Butterworths: Durban.

VAN DER WALT JC

"Oorlas: Grondslag van Aanspreeklikheid?" Tydskrif Vir Hedendaagse

WEARDEN G

"UK Anti-spam Laws Launched" available at

WERKSMANS ATTORNEYS

"Business Guide to Internet Law" available at
WILSKE S AND SCHILLER T

"International Jurisdiction In Cyberspace: Which States May Regulate The Internet?" available at
http://wwwlaw.indiana.edu/fclj/pubs/v50/no1/wilske.html.

WIRED NEWS

"FTC: Where Spam Goes to Die" available at

"Hypocrisy in Anti-Spam Land?" available at

"Spam-Busting Plan Can't Buy a Pal" available at

ZDNET ETESTING LAB

<table>
<thead>
<tr>
<th>TABLE OF CASES</th>
</tr>
</thead>
</table>

**AUSTRALIA**

*R v Hourmouzis* Unreported, County Court of Victoria, 30 October 2000.

**INTERNATIONAL COURT OF JUSTICE**

*SS Lotus (France v Turkey)* (1927) 4 ILR 153; PCIJ Reports Series A No 10.

**SOUTH AFRICA**

*Bamford and 4 others and Energizer (SA) Limited* [2001] 12 BALR 1251 (P).

*Berstein v Bester NO* 1996 (2) SA 751 (CC).

*City of Cape Town v Ad Outpost (Pty) Ltd and Others* 2000 (2) SA 733 (C).

*Cronje v Toyota Manufacturing* (2001) 22 ILJ 735 (CCMA).

*De Klerk v Du Plessis* 1995 (2) SA 40 (T).

*Delanga v Costa* 1989 (2) SA 857 (A).

*Dorland and another v Smits* 2002 (5) SA 374 (C).

*East London Western Districts Farmers' Association v Minister of Education and Development Aid* 1989 (2) SA 63 (A).


*Financial Mail (Pty) Ltd And Others v Sage Holdings Ltd And Another* 1993 (2) SA 451 (A).
Gardener v Whitaker 1995 (2) SA 672 (E).


Jacqueline Bamford and 4 others and Energizer (SA) [2001] 12 BALR 1251 (P).

Kauesa v Minister of Home Affairs & Others 1995 (1) SA 51 (Nm).

Khumalo And Others v Holomisa 2002 (5) SA 401 (CC).

Kruger v Coetzee 1966 (2) SA 428 (A).

Mandela v Falati 1995 (1) SA 251 (W).

Mistry v Interim Medical and Dental Council of South Africa 1998 (7) BCLR 880 (CC).

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

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

O’Keeffe v Argus Printing and Publishing Co Ltd and Another 1954 (3) SA 244 (C).

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

R v Neumann 1949 (3) SA 1238 (SCC).

Rand Waterraad v Bothma en ’n Ander 1997 (3) SA 120 (O).
Regal v African Superslate (Pty) Ltd. 1963 (1) SA 102 (A).

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

S v Mharapara 1986 (1) SA 556 (ZS).

Three Rivers Ratepayers Association And Others v Northern Metropolitan 2000 (4) SA 377 (W).

Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk 1979 (1) SA 441 (A).

Van Zyl v Jonathan Ball Publishers (Pty) Ltd 1999 (4) SA 571 (W).

UNITED STATES OF AMERICA


CompuServe Inc v Cyber Promotions Inc 962 F Supp 1015 (SD OH 1997).

Compuserve v Patterson 89 F Supp 3d 1257 (6th Cir. 1996).


Hotmail Corp v Van$ Mony Pie, Inc 1998 WL 388389, 47 USPQ 2nd (ND Cal. 16 April 1998).

Jacobellis v Ohio 378 US 184 (1964) 197.


United States v Thomas 74 F Supp 3d 701 (6th Cir. 1996).

United States v Rodriguez 29 F Supp 3d 619 (1st Cir. 1994).

<table>
<thead>
<tr>
<th>AUSTRALIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crimes Act 1914.</td>
</tr>
<tr>
<td>Personal Information Protection and Electronic Documents Act 5 of 2000.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AUSTRIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecommunications Act TKG, BGBI 188/1999.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CANADA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competition Act, RS 1985, c. C-34.</td>
</tr>
<tr>
<td>Personal Information Protection and Electronic Documents Act, RS 2000, c.</td>
</tr>
<tr>
<td>C-6.</td>
</tr>
</tbody>
</table>
BELGIUM

Concerning certain legal aspects of Information Society services.

DENMARK


ITALY

Privacy Protection DL 675/1996.


JAPAN

The Law on Regulation on Transmission of Specified Electronic Mail.

Amendment of Commercial Transactions Act.

KOREA

Information and Communications Network Ordinance.

NORWAY

Act on Certain Aspects of Electronic Commerce and Other Information Society Services.

SOUTH AFRICA


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

Telecommunications Act 103 of 1996.

Films and Publications Act 65 of 1996.

Film and Publications Amendment Act 34 of 1999.

UNITED KINGDOM


UNITED STATES OF AMERICA

California Act Senate Bill No 186 (2003).

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 S. 877.

United States Constitution.
### TABLE OF REPORTS AND CONVENTIONS

#### AFRICA


#### AUSTRALIA

Internet Industry Association (IIA) Code of Practice Available at

Minister for Financial Services and Regulation electronic commerce guidelines
for business: "Building Consumer Sovereignty in Electronic Commerce (A
Best Practice Model for Business)".

#### EUROPEAN UNION


European Convention for the Protection of Human Rights and Fundamental
Freedoms (ETS no: 005) open for signature November 4, 1950, entry into
force September 3, 1950, available at
http://www.hrcr.org/docs/Eur_Convention/euroconv.html

Convention on Cybercrime available at
Convention on Cybercrime Explanatory Report available at


Distance Selling Directive (97/7/EC).

Data Protection Directive (95/46/EC).


**UNITED NATIONS**

UNIDROIT General Principles of International Commercial Contracts,

United Nations Convention on the Prevention and Punishment of the Crime of

United Nations Commission of International Trade Law (UNCITRAL) Model
Law on Electronic Commerce

International Covenant of Civil and Political Rights, adopted and opened for
signature, ratification and accession by General Assembly resolution 2200A


Universal Declaration of Human Rights of 1948 Universal Declaration of
Human Rights, adopted and proclaimed by General Assembly resolution 217
A (III) of December 10, 1948, available at

http://www.un.org/Overview/rights.html
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
("OECD")


http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1_1_00.html

SOUTH AFRICA