



Australian Government

**Department of Communications,
Information Technology and the Arts**

***Spam Act 2003* Review Issues Paper**

**A legislative review of the operation of the *Spam Act 2003* and related
parts of the *Telecommunications Act 1997***

For Public Consultation

INTRODUCTION.....	4
(i) Overview	4
(ii) Review process	4
The review	5
Structure of the issues paper	5
Making a submission	6
Terminology.....	6
PART A – THE LEGISLATION	8
Chapter 1 – Background and overview	8
1.1 The Current State of Spam.....	8
1.2 Introduction to the <i>Spam Act 2003</i>	9
1.3 Main Features of the Spam Act	10
What is a commercial electronic message?	10
Australian link.....	10
Three main requirements	11
Additional requirements.....	11
Exclusions – ‘Designated Commercial Electronic Messages’	12
Industry codes and standards	12
Enforcement of the Spam Act.....	12
International perspective.....	13
Chapter 2 - The <i>Spam Act 2003</i>	14
2.1 Spam Act - Part 1 - Introduction.....	14
2.1.1 Definition of an ‘electronic message’	14
2.1.2 Definition of a ‘commercial electronic message’	17
2.1.3 Definition of an ‘Australian link’	18
2.1.4 Sending of electronic messages - carriage service providers.....	19
2.2 Spam Act Part 2 - Rules about sending commercial electronic messages.....	19
2.2.1 Unsolicited commercial electronic messages must not be sent	20
2.2.2 The identification requirement.....	22
2.2.3 The unsubscribe requirement.....	24
2.3 Spam Act - Part 3 - Rules about address-harvesting software and harvested address lists	27
2.4 Spam Act – Enforcement - Spam Act - Parts 4, 5, 6, 7 and Schedule 3: Civil penalties, injunctions, enforceable undertakings, formal warnings and infringement notices	28
2.4.1 Enforcement actions under the Spam Act.....	29
2.4.2 Telecommunications Act	32
2.5 Spam Act - Part 7 - Miscellaneous	36
2.5.1 Additional ACMA functions.....	36
2.5.2 Implied freedom of communications	37
2.6 Spam Act - Schedule 1- Designated commercial electronic messages.....	37
2.7 Spam Act - Schedule 2- Consent	40
2.7.1 Express and inferred consent	40
2.7.2 Conspicuous publication.....	41
2.8 Other	42
Facsimile spam.....	42

Chapter 3 - Interaction of the Spam Act with other legislation	43
3.1 Criminal laws	43
3.2 Privacy Act.....	43
3.3 Broadcasting Services Act	44
3.4 Trade Practices Act and State and Territory fair trading laws	44
PART B :THE MULTI-LAYERED STRATEGY	45
Chapter 4 - The role of industry	45
4.1 Industry codes and standards	45
4.1.1 eMarketing code.....	46
4.1.2 Internet industry code	47
4.1.3 Industry standards	48
4.2 Non-regulatory activities	48
4.2.1 Awareness-raising and consumer resources	48
4.2.2 Industry technical measures	49
4.2.3 Protecting industry development	49
Chapter 5 - International Cooperation	50
5.1 The legislation.....	50
5.2 The Australian Government’s international anti-spam agreements.....	50
5.2.1 UK, US and Australia – tripartite MoU on spam – July 2004	51
5.2.2 Australia and Thailand – joint statement on telecommunications and information technology – July 2004	51
5.2.3 London Action Plan on spam – October 2004.....	51
5.2.4 Seoul-Melbourne Multilateral MoU- Asia Pacific region – April 2005	51
5.2.5 Asia Pacific assistance	51
5.3 Involvement with international organisations.....	52
5.3.1 Organisation of Economic Co-operation and Development (OECD)	52
5.3.2 International Telecommunications Union (ITU)	52
5.3.3 APEC Telecommunications and Information Working Group (APEC TEL)	53
5.3.4 International Consumer Protection and Enforcement Network (ICPEN)....	53
5.3.5 Asia-Pacific Telecommunity (APT) and Pacific Islands Telecommunications Association (PITA)	53
5.4 Other international Activities.....	53
Chapter 6 - Information and Awareness Activities	54
6.1 The legislation.....	54
6.2 Government education and awareness.....	54
6.3 Spam Act and Internet security seminars for business	55
6.4 Publications.....	55
6.5 Avenues for complaint.....	56
6.6 Other groups.....	56
Appendix A	57

INTRODUCTION

(i) Overview

In 2003 the Government introduced anti-spam legislation in response to community concerns about the growing spam problem. In the Australian context, spam is defined as unwanted, or ‘unsolicited’ commercial electronic messaging.

The Spam Act 2003 (the Spam Act) provides guidelines for sending legitimate commercial electronic messages and prohibits the sending of unsolicited commercial electronic messages, whether by email, instant messaging, short message service (SMS), or multimedia messaging. Under the Act, messages must be sent with consent - a single unsolicited commercial electronic message is considered to be spam. The Australian Communications and Media Authority (ACMA) is responsible for enforcing the Act.

The legislation forms part of a multi-layered strategy against spam. Domestic legislation and enforcement alone will not provide a complete solution. In addition to the legislation, the strategy consists of education and awareness activities, international cooperation, industry cooperation and technical countermeasures. These elements are designed to complement and reinforce each other. The multi-layered strategy seeks to minimise spam for Australian end-users, reduce Australia as a source of spam and promote Australia’s involvement in worldwide anti-spam initiatives.

The legislation has provided a basis for curbing the activities of major professional spammers in Australia and has decreased the amount of Australian originated spam. It has also enabled the Australian Government to actively participate in international anti-spam agreements and activities.

To date, the Spam Act has been well received, from consumers and industry alike. The legislation has provided an avenue for the e-marketing industry to send legitimate consent-based commercial electronic messages. It has also been recommended as a template for other countries seeking to address spam.¹

(ii) Review process

This legislative review is concerned with the operation of the Spam Act and the parts of the *Telecommunications Act 1997* (the Telecommunications Act) that support its operation.

¹ Spamhaus, 19 July, 2004- article, ‘Follow Australia’ www.spamhaus.org/news.lasso?article=154

The review

According to section 46 of the Spam Act, the Minister for Communications, Information Technology and the Arts must cause a review of the legislation to be conducted and tabled in Parliament by April 2006.

The review must consider the operation of the Spam Act as well as the relevant parts of the Telecommunications Act that provide ACMA with the necessary enforcement powers. These provisions also provide a framework to enable the development of industry codes relating to the sending of commercial electronic messages.

The Minister has directed the Department of Communications, Information Technology and the Arts to initiate a public consultation process as part of the review.

Structure of the issues paper

This issues paper poses questions throughout to assist individuals and organisations to develop submissions. A summary of questions raised are provided at Appendix A.

Part A provides a discussion on the Spam Act, and the relevant parts of the Telecommunications Act, by considering the operation of each part of the legislation in detail.

- **Chapter 1** begins with an introduction to the legislation, including an overview of the main features of the Spam Act and the current status of spam.
- **Chapter 2** is dedicated to reporting on the operation of the major provisions of the legislation.
- **Chapter 3** discusses the intersection of the operation of the Spam Act with other Australian legislation.

Part B deals with the operation of the legislation in the context of the multi-layered strategy:

- **Chapter 4** addresses the role of industry in developing guidelines and standards to ensure compliance with the Spam Act. It also considers the extent to which industry has also made available spam-related information and product resources to consumers.
- **Chapter 5** reports on how the legislation has enabled the Australian Government to enter into international arrangements with other countries to extend the relevance of the legislation overseas.
- **Chapter 6** discusses the provision of information by government bodies and industry regarding the legislation and mechanisms established that allow spam to be reported.

Making a submission

The Department of Communications, Information Technology and the Arts is seeking written submissions on the issues raised in this paper.

Questions appear throughout the paper as boxed text.

Interested stakeholders are invited to provide written comment in answer to these questions, or provide a more general response on the operation of the Spam Act, as preferred.

Submissions should identify the name of the party making the submission, the organisation they represent (if relevant), as well as contact details.

Please forward submissions to:

Manager, Online Policy
Department of Communications, Information Technology and the Arts

By mail: GPO Box 2154
CANBERRA ACT 2601

By email: spam.comments@dcita.gov.au

By fax: 02 6271 1098

Those making submissions should be aware that submissions will be made publicly available on the Department's website. The Department reserves the right not to publish any submission, or part of a submission, which in the view of the Department contains potentially defamatory material.

All submissions will be treated as non-confidential information unless specifically requested. Email disclaimers will not be considered sufficient confidentiality requests. Note that submissions or comments will generally be subject to freedom of information provisions.

Enquires about issues raised in this paper may be directed to telephone 02 6271 1259 or by email to spam.comments@dcita.gov.au.

The closing date for comments and submissions to the Department is **Wednesday, 1 February 2006**.

Terminology

On 1 July 2005 the Australian Communications Authority (ACA) merged with the Australian Broadcasting Authority to become the Australian Communications and Media Authority (ACMA). For ease of understanding, ACMA will be used for the ACA in most cases in this paper.

Spam Act 2003 Review—Issues Paper

In 2004 the area responsible for drafting the Spam Act within the National Office of the Information Economy (NOIE) was absorbed into the Department of Communications, Information Technology and the Arts (DCITA). For ease of understanding, DCITA will be used for NOIE in all cases except those relating to specific NOIE titled publications.

PART A—THE LEGISLATION

Part A provides an introduction to the legislation including an overview of the main features of the Spam Act. It also reports on the operation of the Spam Act, and relevant parts of the Telecommunications Act, in sequence.

Part A also contains a discussion on the intersection of the Spam Act with other Australian legislation.

Chapter 1—Background and overview

1.1 The Current State of Spam

Australia's spam legislation was introduced in response to concerns about the impact of spam on the effectiveness of electronic communication and the costs imposed on end-users.

ACMA's active enforcement of the Spam Act sends a clear message that breaches of the legislation will not be tolerated. Prior to the introduction of the legislation, a substantial proportion of spam received in Australia came from local businesses marketing their products. Australian businesses have been adjusting their practices and policies to comply with the Spam Act through compliance with a code of practice for e-marketers. The development of industry codes of practice are provided for under the legislation in recognition of the essential role that industry plays in managing levels of spam.

The majority of spam received in Australia comes from overseas. ACMA is using a network of international regulators to share intelligence on spam campaigns and network security threats. ACMA has used its relationships developed under the 'Seoul-Melbourne' Asian region agreement on spam to assist in shutting down compromised systems that are hosting child pornography and fraud operations.

At the time the legislation was being drafted, the percentage of email that was identified as spam was between 20-30 per cent². Spam is still a global problem and continues to concern end users, employers, Internet Service Providers (ISPs) and legitimate e-marketers. The annual cost to business is estimated at over \$1000 per employee per year, due to lost productivity and additional IT resources required to deal with spam and its flow-on effects. Estimates of global spam vary, but it is generally reported as accounting for between 60-80 per cent of all global email.³

² B.1, Regulation Impact Statement *Spam Bill 2003 Explanatory Memorandum*, p 7

³ Symantec Internet Security Threat Report Trends for January 05–June 05, p 5; and Postini, www.postini.com/stats

Although spam is increasing as a percentage of global email, technological filtering has improved and is proving effective in keeping large amounts of spam from reaching end users. Spam however continues to be a burden on Internet telecommunications networks.

ACMA has also reported that electronic messages delivered by mobile phones, including SMS and multimedia message services, are increasingly a focus of its enforcement activities.

ACMA also reports that consumers seem to find SMS even more intrusive than spam email. Approximately 10 per cent of spam-related complaints received by ACMA relate to the use of SMS. ACMA fined one Australian company for SMS spam in March 2005 and two others in June 2005. It has also worked closely with an international provider of mobile phone content to ensure its practices complied with the Spam Act.

Increasingly spam is being used as a vehicle for other e-security threats such as malicious code and ‘phishing’. Phishing is a technique used to gain personal information for the purposes of identity theft, using fraudulent email messages that appear to come from legitimate businesses, most commonly banks. These authentic-looking messages are designed to lure recipients into providing personal data such as account numbers and passwords and credit card numbers. In June 2005, the Australian Securities and Investment Commission reported that complaints regarding phishing have doubled over the past few months.⁴

Recent developments in the online environment have seen an increase in spam sent by “zombie” computers which have been infected or compromised by malicious code such as a virus or a Trojan. In these cases, the true originator of the spam may be located in another country. It is estimated that between 50 per cent and 80 per cent of all spam worldwide is now sent by compromised computers.⁵ ACMA has joined forces with five ISPs to pilot a system to identify infected computers, notify the owners and help them to take appropriate action. It is also using its international networks and drawing on its experience in enforcing the Spam Act to address this emerging issue.⁶

1.2 Introduction to the *Spam Act 2003*

In 2003 the Government examined the nature and extent of spam and the effectiveness of existing regulatory counter-measures.

The findings of this review were released in the April 2003 document titled *the Final Report of the NOIE Review of the Spam Problem and How it Can Be Countered* (the Final Report). The Final Report recommended a multi-layered strategy against spam consisting of legislation, education, international cooperation, industry cooperation and

⁴ ‘ASIC Issues Alert as Phishing Reports Double’, media release, June 2005 (available from www.asic.gov.au)

⁵ PC World, www.pcworld.com/news/article/0,aid,121381,00.asp

⁶ ‘Government Acts to Zap Zombies’, media release, 7 November 2005, www.minister.dcita.gov.au/media

technical countermeasures. Later in 2003, the Government accepted the recommendations made in the report, including the introduction of anti-spam legislation.

The anti-spam legislation was developed in consultation with key industry, marketing and consumer groups. The Spam Act received royal assent in December 2003. The penalty provisions of the Act came into effect in April 2004.

The legislation was accompanied by several consequential amendments to the *Telecommunications Act 1997* and the *Australian Communications Authority Act 1997*. These amendments extended the enforcement capabilities of ACMA to have application to the Spam Act and also provided a framework to enable the development of industry codes relating to the sending of commercial electronic messages.

1.3 Main Features of the Spam Act

The Spam Act prohibits the sending of spam, which is identified as a commercial electronic message sent without the consent of the addressee via email, short message service (SMS), multimedia message service (MMS) or instant messaging. The requirements under the Spam Act apply to all commercial electronic messages, including both bulk and individual messages.

Normal voice-to-voice communication by telephone is not covered by the Act. Messages sent by facsimile are, at present, excluded from coverage by regulation.

What is a commercial electronic message?

Commercial electronic messages are messages that offer to supply goods or services, or which advertise goods and services, land or business or investment opportunities, or which direct the recipient to a location where goods and services are sold or advertised, or which are to assist or enable a person to dishonestly obtain property, financial advantage or a gain from another person.

Australian link

The requirements created by the Spam Act only apply to electronic messages that have an ‘Australian link’. This means the legislation applies to:

- Messages that originate or are commissioned in Australia being sent to any destination;
- Messages that originate or are commissioned overseas being sent to an address accessed in Australia.

Three main requirements

There are three main requirements for sending commercial electronic messages.

Commercial electronic messages must be sent with consent

Commercial electronic messages must only be sent with the addressee's consent. Consent may be expressly given by the recipient, or under certain restricted circumstances it may be inferred from the conduct or business relationships of the recipient.

Information to identify the sender

The Spam Act requires all commercial electronic messaging with an Australian link to contain accurate information which identifies the sender of the message. This will be the person or organisation that authorised the sending of the message, regardless of whether they actually sent the message themselves or arranged for someone to do it on their behalf. The information must be reasonably likely to remain correct for a period of 30 days after the sending of the message.

Functional unsubscribe facility

A functional unsubscribe facility must be included in all commercial electronic messages sent. This facility allows people to opt out from receiving messages from that source in the future. This facility may be a statement that the message may be replied to with a request to opt out from future communications. The Act requires that a request to unsubscribe must be honoured within five working days. The unsubscribe facility must be reasonably likely to be able to receive and act on unsubscribe messages for a period of 30 days after the sending of the message.

Additional requirements

In addition to these three main requirements, the Spam Act also prohibits the sending of a commercial electronic message to a non-existent address that would have an Australian link if the address existed.

Further, it is prohibited to aid, abet or otherwise be party to a contravention of the legislation.

The Spam Act also prohibits the supply, acquisition or use of software that 'harvests' electronic addresses from the Internet for the purpose of sending spam. Similarly, the provision, acquisition or use of harvested address lists to send spam is prohibited.

Exclusions—‘Designated Commercial Electronic Messages’

Some limited exceptions from the Spam Act requirements apply to certain types of electronic messages, known as ‘designated commercial electronic messages’. These are messages that are sent by:

- government bodies;
- registered political parties;
- charities;
- religious organisations; or
- educational institutions in certain circumstances.

To be considered a designated commercial electronic message, it is necessary for the message to be in respect of goods or services that are being supplied by one of the organisations listed above. Purely factual messages, such as a product recall notice, are also classed as designated commercial electronic messages.

Designated commercial electronic messages are not required to have the addressee’s consent, but they must still carry accurate information to identify the organisation or individual that authorised the sending of the message.

Industry codes and standards

As the agency responsible for enforcing the Spam Act, ACMA has a legislated role in facilitating and supporting the development of industry codes that complement the Act. Industry codes provide relevant and achievable standards and procedures to assist compliance with the legislation, as well as procedures for the handling of complaints.

Enforcement of the Spam Act

ACMA commenced the enforcement of the Spam Act on April 10, 2004, when the penalty provisions of the Act came into effect. ACMA developed a means of reporting Spam Act breaches by direct contact, email and web form in early 2004.

In October 2005 ACMA launched its new spam reporting tool, “SpamMATTERS”. This software allows the public to report spam emails directly from their email software. The software uses a one-click process which sends spam mails direct and intact to ACMA via a plug-in for Microsoft Outlook which can be downloaded from the ACMA site (www.acma.gov.au). The forensic data gathered from complaints submitted in this way will assist ACMA to present evidence for cases in court. A component allowing for the submission of bulk spam complaints will be made available subsequently. Complaints and reports of spam may continue to be lodged directly via the ACMA website.

A range of powers have been provided to ACMA through amendments made to the Telecommunications Act, which allow it to enforce the Spam Act.

A breach of the Spam Act can lead to a formal warning, infringement notice (carrying lesser penalties), enforceable undertaking, injunction or prosecution.

Breaches carry civil, rather than criminal, penalties. The Government intended that the legislation would modify existing behaviours, and not punish spamming with imprisonment. Civil penalties are also considered to be more proportionate to the nature of the spam problem - financial fines help counter the financial motive associated with most spam.

International perspective

Anti-spam laws vary from country to country. The Spam Act includes provisions that provide for Australia's participation in multilateral arrangements with other countries concerned with the regulation of spam.

Chapter 2—The *Spam Act 2003*

2.1 Spam Act—Part 1 Introduction

The first part of the Spam Act deals with the key concepts used within the Act, such as what constitutes a ‘commercial electronic message’ and other terminology.

2.1.1 Definition of an ‘electronic message’

Spam Act, Section 5 (1–5)

‘Electronic Messages’

Basic definition

- (1) ...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.

- (2) For the purposes of subsection (1), it is immaterial whether the electronic address exists.
- (3) For the purposes of subsection (1), it is immaterial whether the message reaches its intended destination.
- (4) Subsection (1) has effect subject to subsection (5).

Excluded messages—voice calls

- (5) If a message is sent by way of a voice call made using a standard telephone service, the message is not an electronic message for the purposes of this Act.

The definition of an electronic message is made up of two parts. The first part of the definition relies on the message being sent using a particular type of carriage service, an Internet carriage service or any other listed carriage service.

Messages may come within this definition even if they use a carriage service in conjunction with another service. For example an email message may be sent using a standard telephone service and an Internet carriage service.

The second part of the definition requires the message to be sent to an electronic address in connection with a particular account. Email addresses and telephone numbers are examples of electronic addresses. To come within the meaning of an electronic message, the message must be sent to an electronic address which has a connecting account, for example an email account in the case of email or a phone account, in the case of SMS messages.

Voice calls via a standard telephone service

The Spam Act only applies to commercial electronic messaging. The definition of an electronic message contained in s.5 excludes voice calls made using a ‘standard telephone service’.

Unsolicited phone marketing, delivered via a standard telephone service, is currently excluded from coverage by the Act. The Spam Act only has application to ‘messaging’ communications, which differ fundamentally from a ‘conversation’—a type of communication typically associated with a standard telephone voice call.

In response to consumer and industry demand, DCITA has undertaken public consultation in relation to the establishment of a ‘do not call’ register, encompassing the issue of unsolicited marketing contact via telephone. Further information is available from www.dcita.gov.au/donotcall

Recorded voice calls

A call which involves a recorded or synthetic voice or an equivalent call to a voice call for a person with a disability is also excluded. This provision is to ensure that the application of the National Relay Service is preserved. The National Relay Service is a telephone access service available to all Australians. It allows the deaf, or hearing or speech impaired, and those requiring the use of a teletypewriter to access anyone in the wider telephone network. Similarly, the National Relay Service can be used by anyone in the community to communicate with those who are deaf, or have a hearing or speech impairment using the standard telephone service. In this instance, the use of a teletypewriter by hearing impaired persons is considered to be a voice call for the purposes of the definition of a ‘voice call’.

ACMA has received complaints in relation to recorded voice calls. Following investigation in these instances, it was determined that these calls are not within the scope of the Spam Act.

Recorded voice marketing calls, and other telemarketing calls, are currently being considered by DCITA in the context of the ‘do not call’ register (see www.dcita.gov.au/donotcall for more information).

Voice over Internet Protocol (VOIP)

The Spam Act has been carefully designed to be as technology neutral as possible in its application. The Act allows for the making of regulations for certain provisions to enable the legislation to remain relevant for future technologies.

The question of the application of the Spam Act to emerging technologies, such as Voice over Internet Protocol (VOIP), has arisen as part of the Government's ongoing consideration of electronic communications.

VOIP is an emerging technology which allows for voice communication over Internet networks, in contrast to the approach used by traditional telephone networks.

There are a number of different ways in which VOIP services can be delivered. In general, VOIP services can make calls to other VOIP connections or to plain old standard telephone numbers.

While technical innovation in relation to VOIP is ongoing, the view of DCITA and ACMA is that VOIP services are generally 'carriage services' and 'standard telephone services' within the meaning of the current telecommunications regulatory regime.⁷

As the definition of an 'electronic message' in s.5(5) of the Spam Act excludes voice calls made using a standard telephone service, it is clear that unsolicited phone calls delivered via VOIP do not fall within the scope of the Spam Act.

According to the *Explanatory Memorandum to the Spam Act 2003*, the definition of a commercial electronic message is intended to 'exclude(s) Voice Over IP (VOIP) where telephone calls can be made using an Internet connection.'

Unlike the Spam Act, which is concerned with messaging, voice call marketing delivered over Internet networks is more like telemarketing (including automated voice-recorded calls). As noted above, DCITA has undertaken consultation on the issue of telemarketing and a 'do not call' register (www.dcita.gov.au/donotcall).

⁷ 'Examination of Policy and Regulation Relating to Voice over Internet Protocol (VOIP) Services', November 2005 (available from www.dcita.gov.au/tel).

2.1.2 Definition of a ‘commercial electronic message’

Spam Act, Section 6 (1)(a–p)

‘Commercial electronic messages - basic definition’

- (1) ...A commercial electronic message is an electronic message, where, having regard to:
- (a) the content of the message; and
 - (b) the way in which the message is presented; and
 - (c) the content that can be located using the links, telephone numbers or contact information (if any) set out in the message;
- it would be concluded that the purpose, or one of the purposes, of the message is:
- (d) to offer to supply goods or services; or
 - (e) to advertise or promote goods or services; or
 - (f) to advertise or promote a supplier, or prospective supplier, of goods or services; or
 - (g) to offer to supply land or an interest in land; or
 - (h) to advertise or promote land or an interest in land; or
 - (i) to advertise or promote a supplier, or prospective supplier, of land or an interest in land; or
 - (j) to offer to provide a business opportunity or investment opportunity; or
 - (k) to advertise or promote a business opportunity or investment opportunity; or
 - (l) to advertise or promote a provider, or prospective provider, of a business opportunity or investment opportunity; or
 - (m) to assist or enable a person, by a deception, to dishonestly obtain property belonging to another person; or
 - (n) to assist or enable a person, by a deception, to dishonestly obtain a financial advantage from another person; or
 - (o) to assist or enable a person to dishonestly obtain a gain from another person; or
 - (p) a purpose specified in the regulations.

The Spam Act only applies to commercial electronic messages: these are messages that have a commercial purpose, that offer to buy, sell or advertise something. The term is a key concept of the Act, whose primary purpose is to prohibit spam and provide reasonable, easy to follow rules for sending legitimate commercial electronic messages.

The majority of spam involves a commercial element, such as inviting payment for goods or services, or providing an opportunity for financial gain. Other unsolicited messages, for example, messages which are ‘spiritual’ or political in nature, account for a small proportion of all unsolicited messages. The focus of the legislation on commercial messaging means that the sending of unsolicited electronic messages in bulk is largely covered by the legislation as the primary motivation for such messages is financial gain. This commercial focus also ensures that the legislation does not impinge on the freedom of political, religious or ideological expression.

A range of commercial electronic messages are intended to be covered by the Spam Act. Examples include:

- Nigerian scam email;
- business marketing;
- get-rich-quick-schemes;
- pharmaceutical and health related product promotions; and
- promotions of pornographic websites or services.

Subsection 6 (7) allows specified kinds of electronic messages to be excluded from the meaning of 'commercial electronic message' by regulations. The regulations which accompanied the Spam Act exclude electronic messages that are facsimile messages from this definition. This means that the penalty provisions in Part 2 of the Act do not apply to facsimile messages. The issue of facsimile spam ('fax spam') is discussed in more detail at chapter 2.8.

QUESTIONS

The Spam Act covers commercial electronic messages.

-Q1 Do you think this provides suitable coverage?

-Q2 Does it include things that it should not?

-Q3 Does it fail to cover things that should be included?

2.1.3 Definition of an 'Australian link'

Spam Act, Section 7 (a–e)

'Australian link'

...A commercial electronic message has an Australian link if, and only if:

- (a) the message originates in Australia; or
- (b) the individual or organisation who sent the message, or authorised the sending of the message, is:
 - (i) an individual who is physically present in Australia when the message is sent; or
 - (ii) an organisation whose central management and control is in Australia when the message is sent; or
- (c) the computer, server or device that is used to access the message is located in Australia; or
- (d) the relevant electronic account-holder is:
 - (i) an individual who is physically present in Australia when the message is accessed; or

(ii) an organisation that carries on business or activities in Australia when the message is accessed; or
(e) if the message cannot be delivered because the relevant electronic address does not exist—assuming that the electronic address existed, it is reasonably likely that the message would have been accessed using a computer, server or device located in Australia.

The Spam Act applies to electronic messages that have an ‘Australian link’. This means that the Act applies to:

- messages that originate or are commissioned in Australia being sent to any destination; and
- messages that originate or are commissioned overseas being sent to an address accessed in Australia.

The Act also applies in the situation where it is reasonable to expect that that an electronic address has an Australian link, even if that address does not exist.

2.1.4 Sending of electronic messages—carriage service providers

Section 9 of the Spam Act specifies that a person will not be considered to be in breach of the legislation merely because they supply the carriage service that enables a contravening message to be sent. As long as the ISP or other carriage service provider is not responsible for, or knowingly concerned in, sending or authorising the sending of the message in question, they will not be considered to have committed the breach, or to have been a party to the contravention.

2.2 Spam Act Part 2—Rules about sending commercial electronic messages

Part 2 sets out the main requirements of the Spam Act to which civil penalty provisions apply. These are:

- unsolicited commercial electronic messages must not be sent (s.16);
- commercial electronic messages must include information about the individual or organisation who authorised the sending of the message (s.17); and
- commercial electronic messages must contain a functional unsubscribe facility (s.18).

2.2.1 Unsolicited commercial electronic messages must not be sent

Spam Act, Section 16 (1–11)

‘Commercial electronic messages must not be sent’

(1) A person must not send, or cause to be sent, a commercial electronic message that:

- (a) has an Australian link; and
- (b) is not a designated commercial electronic message.

Note 1: For Australian link, see section 7.

Note 2: For designated commercial electronic message, see Schedule 1.

(2) Subsection (1) does not apply if the relevant electronic account-holder consented to the sending of the message.

Note: For the meaning of consent, see Schedule 2.

(3) Subsection (1) does not apply if the person:

- (a) did not know; and
- (b) could not, with reasonable diligence, have ascertained; that the message had an Australian link.

(4) Subsection (1) does not apply if the person sent the message, or caused the message to be sent, by mistake.

(5) A person who wishes to rely on subsection (2), (3) or (4) bears an evidential burden in relation to that matter.

Message must not be sent to a non-existent electronic address

(6) A person must not send, or cause to be sent, a commercial electronic message to a non-existent electronic address if:

- (a) the person did not have reason to believe that the electronic address existed; and
- (b) the electronic message:
 - (i) has an Australian link; and
 - (ii) is not a designated commercial electronic message.

(7) Subsection (6) does not apply if the person:

- (a) did not know; and
- (b) could not, with reasonable diligence, have ascertained; that the message had an Australian link.

(8) A person who wishes to rely on subsection (7) bears an evidential burden in relation to that matter.

Ancillary contraventions

(9) A person must not:

- (a) aid, abet, counsel or procure a contravention of subsection (1) or (6); or
- (b) induce, whether by threats or promises or otherwise, a contravention of subsection (1) or (6); or
- (c) be in any way, directly or indirectly, knowingly concerned in, or party to, a contravention of subsection (1) or (6); or
- (d) conspire with others to effect a contravention of subsection (1) or (6).

(10) A person does not contravene subsection (9) merely because the person supplies a carriage service that enables an electronic message to be sent.

Civil penalty provisions

(11)

Subsections (1), (6) and (9) are civil penalty provisions.

Note: Part 4 provides for pecuniary penalties for breaches of civil penalty provisions.

Section 16 addresses the essence of the spam problem. It is the section which prohibits the sending of commercial electronic messages without consent. The issue of consent is addressed in more detail in the discussion on Schedule 2 of the Spam Act in Chapter 2.7.

It is also prohibited to aid, abet or be in any way, directly or indirectly, knowingly concerned in a breach of this provision.

In addition, this section also prohibits the sending of a commercial electronic message to a non-existent address that would have an Australian link if the address existed. This prohibition is aimed at covering the common technique used by spammers known as a 'dictionary attack'. This technique consists of sending unsolicited commercial electronic messages to random addresses even if the addresses do not exist. This flood of automated messaging imposes a substantial burden on the information and communications infrastructure. An email that is sent to a non-existent address within a real domain will still be sent to that domain's mail server, and consume system resources.

According to this section, commercial electronic messages with an Australian link must not be sent.

The Spam Act applies to electronic messages that have an 'Australian link'. This means that the Act applies to:

- messages that originate or are commissioned in Australia being sent to any destination; and
- messages that originate or are commissioned overseas being sent to an address accessed in Australia.

The coverage of the Spam Act to overseas sourced spam and legitimate commercial messages discourages in-country spammers simply moving offshore. It also ensures that there is an appropriate enforcement regime in place to deal with overseas spammers via multilateral arrangements.

QUESTIONS

Q4 Does this provision cover messages that it should not?

Q5 Are there spam messages that are not currently covered by this provision that should be?

Q6 Does this provision suitably cover the spam problem?

2.2.2 The identification requirement

Spam Act, Section 17 (1–7)

‘Commercial electronic messages must include accurate sender information’

(1) A person must not send, or cause to be sent, a commercial electronic message that has an Australian link unless:

- (a) the message clearly and accurately identifies the individual or organisation who authorised the sending of the message; and
- (b) the message includes accurate information about how the recipient can readily contact that individual or organisation; and
- (c) that information complies with the condition or conditions (if any) specified in the regulations; and
- (d) that information is reasonably likely to be valid for at least 30 days after the message is sent.

Note: For Australian link, see section 7.

(2) Subsection (1) does not apply if the person:

- (a) did not know; and
- (b) could not, with reasonable diligence, have ascertained; that the message had an Australian link.

(3) Subsection (1) does not apply if the person sent the message, or caused the message to be sent, by mistake.

(4) A person who wishes to rely on subsection (2) or (3) bears an evidential burden in relation to that matter.

Ancillary contraventions

- (5) A person must not:
- (a) aid, abet, counsel or procure a contravention of subsection (1); or
 - (b) induce, whether by threats or promises or otherwise, a contravention of subsection (1); or
 - (c) be in any way, directly or indirectly, knowingly concerned in, or party to, a contravention of subsection (1); or
 - (d) conspire with others to effect a contravention of subsection (1).
- (6) A person does not contravene subsection (5) merely because the person supplies a carriage service that enables an electronic message to be sent.

Civil penalty provisions

- (7) Subsections (1) and (5) are civil penalty provisions.

Note: Part 4 provides for pecuniary penalties for breaches of civil penalty provisions.

Section 17 requires that commercial electronic messages must clearly and accurately identify the individual or organisation that authorised the sending of the message. The message must also include accurate information about how the recipient can readily contact that individual or organisation.

The identification requirement (s.17), is designed to limit unsolicited commercial electronic messages sent by people who purposefully disguise the source of the message by using false identification information. This provision applies to all commercial electronic messages with an Australian link.

This provision ensures that the recipient of a legitimate commercial electronic message knows who is responsible for sending it.

Legitimate commercial messaging must comply with the identification requirement. This enables legitimate organisations to demonstrate that they are clearly accountable for the messages they send. It also allows the recipient to contact the sender in the case of an error, complaint, or a request to unsubscribe from future messages.

QUESTIONS

Q7 Is this a suitable requirement for commercial electronic messages?

2.2.3 *The unsubscribe requirement*

Spam Act, section 18 (1–9)

‘Commercial electronic messages must contain a functional unsubscribe facility’

- (1) A person must not send, or cause to be sent, a commercial electronic message that:
- (a) has an Australian link; and
 - (b) is not a designated commercial electronic message;
- unless:
- (c) the message includes:
 - (i) a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the individual or organisation who authorised the sending of the first-mentioned message;
 - or
 - (ii) a statement to similar effect; and
 - (d) the statement is presented in a clear and conspicuous manner; and
 - (e) the electronic address is reasonably likely to be capable of receiving:
 - (i) the recipient's unsubscribe message (if any); and
 - (ii) a reasonable number of similar unsubscribe messages sent by other recipients (if any) of the same message;at all times during a period of at least 30 days after the message is sent; and
 - (f) the electronic address is legitimately obtained; and
 - (g) the electronic address complies with the condition or conditions (if any) specified in the regulations.

Note 1: For unsubscribe message, see subsection (8).

Note 2: For Australian link, see section 7.

Note 3: For designated commercial electronic message, see Schedule 1.

- (2) Subsection (1) does not apply if the person:
- (a) did not know; and
 - (b) could not, with reasonable diligence, have ascertained; that the message had an Australian link.
- (3) Subsection (1) does not apply to the extent (if any) to which it is inconsistent with the terms of a contract or other agreement between:
- (a) the individual or organisation who authorised the sending of the first-mentioned message; and
 - (b) the relevant electronic account-holder.
- (4) Subsection (1) does not apply if the person sent the message, or caused the message to be sent, by mistake.
- (5) A person who wishes to rely on subsection (2), (3) or (4) bears an evidential burden in relation to that matter.

Ancillary contraventions

(6) A person must not:

- (a) aid, abet, counsel or procure a contravention of subsection (1); or
- (b) induce, whether by threats or promises or otherwise, a contravention of subsection (1); or
- (c) be in any way, directly or indirectly, knowingly concerned in, or party to, a contravention of subsection (1); or
- (d) conspire with others to effect a contravention of subsection (1).

(7) A person does not contravene subsection (6) merely because the person supplies a carriage service that enables an electronic message to be sent.

Civil penalty provisions

(8) Subsections (1) and (6) are civil penalty provisions.

Note: Part 4 provides for pecuniary penalties for breaches of civil penalty provisions.

Unsubscribe message

(9) For the purposes of the application of this section to a commercial electronic message, where the sending of the message is authorised by an individual or organisation, an unsubscribe message is:

- (a) an electronic message to the effect that the relevant electronic account-holder does not want to receive any further commercial electronic messages from or authorised by that individual or organisation; or
- (b) an electronic message to similar effect.

Section 18 requires that all commercial electronic messages contain an unsubscribe facility. This requirement is included to ensure that recipients can opt out of future communications. The requirement does not apply to ‘designated commercial electronic messages’ (see Chapter 2.6).

To comply with this provision, the unsubscribe facility may take various forms, including:

- *Email*: 'Unsubscribe: if you no longer want to receive messages from us, simply reply to this email with the word "unsubscribe" in the subject line.'
- *Email*: 'If you no longer want to receive these messages, please click the "unsubscribe" button below.'
- *SMS*: 'Unsub: reply NO' or 'Unsub: (1800-number)'

Section 18 (1)(g) also requires that an electronic address associated with an unsubscribe facility must comply with the conditions specified in the regulations. Regulations are a set of rules approved by Parliament that provide guidance on the interpretation or application of a particular piece of legislation. The regulations that accompany the Spam Act specify three conditions with which an electronic address used as an unsubscribe facility must comply. The conditions are that the use of an electronic address must not:

- require the recipient of the message to use a 'premium service' to send an unsubscribe message (regulation 3.2);
- cost more than the usual cost of using that kind of electronic address, using the same kind of technology that was used to receive the commercial electronic message (regulation 3.3); and
- require the recipient of the commercial electronic message to pay a fee or charge to the sender of the message or to a 'related person' (sub-regulation 3.4(1)).

The conditions have been designed to ensure that when someone is sent a commercial electronic message they are not required to pay any abnormal fees or charges or use high cost premium services in order to unsubscribe.

SMS is a limited text medium which makes it difficult to include the required identification information and unsubscribe facility in addition to the content of the message. To an extent, this problem can be combated through the combination of identification information and the unsubscribe details within the body of the message. The Frequently Asked Questions section of the ACMA website provides some guidance on acceptable unsubscribe options for commercial SMS messages (www.acma.gov.au).

QUESTIONS

Q8 Is this a suitable requirement for legitimate commercial electronic messages?

2.3 Spam Act—Part 3 Rules about address-harvesting software and harvested address lists

Spam Act, Section 22

‘Address-harvesting software and harvested-address lists must not be used’

(1) A person must not use:

- (a) address-harvesting software; or
- (b) a harvested-address list;

if the person is:

- (c) an individual who is physically present in Australia at the time of the use; or
- (d) a body corporate or partnership that carries on business or activities in Australia at the time of the use.

Note: For treatment of partnerships, see section 585 of the Telecommunications Act 1997.

(2) Subsection (1) does not apply in relation to the use of address-harvesting software or a harvested-address list, if the use was not in connection with sending commercial electronic messages in contravention of section 16.

Ancillary contraventions

(3) A person must not:

- (a) aid, abet, counsel or procure a contravention of subsection (1); or
- (b) induce, whether by threats or promises or otherwise, a contravention of subsection (1); or
- (c) be in any way, directly or indirectly, knowingly concerned in, or party to, a contravention of subsection (1); or
- (d) conspire with others to effect a contravention of subsection (1).

Civil penalty provisions

(4) Subsections (1) and (3) are civil penalty provisions.

Note: Part 4 provides for pecuniary penalties for breaches of civil penalty provisions.

Part 3 of the Spam Act states that address-harvesting software and electronically harvested address lists must not be supplied, acquired or used, in conjunction with a breach of s.16 (which requires that unsolicited commercial electronic messages must not be sent).

‘Address-harvesting software’ is defined as software that is specifically designed or marketed for use for searching the Internet for electronic addresses (for example email addresses).

Often unsolicited commercial electronic messages are sent to recipients using electronic addresses which have been collected without the owner's consent. For example, many spammers use address lists electronically harvested from public sources, such as web pages or newsgroups.

Part 3 of the Spam Act sets out rules about address-harvesting software and harvested-address lists which are designed to prohibit uses of such software and lists to send spam.

Because there are some legitimate uses of addressing harvesting software and address harvesting lists, a blanket prohibition has not been included. The prohibition only applies in respect of an intent to breach the spamming provisions of the Act.

QUESTIONS

Q9 Do the address harvesting provisions suitably cover spam-related activities?

Q10 Do these provisions cover circumstances that they should not?

2.4 Spam Act—Enforcement: Spam Act—Parts 4, 5, 6, 7 and Schedule 3: Civil penalties, injunctions, enforceable undertakings, formal warnings and infringement notices

Parts 4,5,6,7 and Schedule 3 of the Spam Act contain provisions which deal with the consequences of breaching the Spam Act. A breach of the Spam Act can lead to a formal warning, infringement notice, enforceable undertaking, injunction, or prosecution.

A range of powers have been provided to ACMA to allow it to enforce the Spam Act. These powers have been derived from amendments made to the Telecommunications Act.

A breach of the Spam Act carries civil penalties, rather than criminal penalties. The Government intended that the legislation would modify existing behaviours, and not punish spamming breaches with imprisonment. Civil penalties are also more proportionate to the spam problem, which consists mainly of nuisance commercial messages.

ACMA has actively enforced the Spam Act since the penalty provisions came into effect in April 2004.

Summary of ACMA’s enforcement activities (April 2004–October 2005)

Activity	Number of actions taken
Businesses warned to comply with the Act	more than 350
Formal warnings under section 41	8
Fines and infringement notices	5
Enforceable undertakings	3
Search warrants	5
ACMA notices demanding information or attendance at a formal interview	5
Prosecution	1 (This case was still before the court at November 2005.)

2.4.1 Enforcement actions under the Spam Act

Warnings and advice

ACMA has the general power to issue a letter, or other communication, warning a business that it should adjust its practices to comply with the Spam Act. ACMA has reported that this is the swiftest and most effective means of dealing with most cases.

Prior to the commencement of the Spam Act, ACMA issued warnings and offered advice to businesses alleged to have been sending unsolicited commercial electronic messages of the imminent commencement of the Act and the need to ensure their practices were compliant after 10 April 2004.

Since April 2004, ACMA has required more than 350 businesses to adjust their practices to comply with the Spam Act.

Formal warnings

Spam Act—Section 41

‘Formal Warnings—breach of civil penalty provision’

The ACMA may issue a formal warning if a person contravenes a civil penalty provision.

According to s. 41 of the Spam Act, ACMA may choose to issue a Formal Warning, rather than issue an infringement notice or initiate court proceedings for a breach of the Act. A formal warning might be issued where ACMA is satisfied that the breach was inadvertent and would not be repeated, or in other cases where a warning would suffice to change the behaviour. This generally takes the form of a letter outlining the relevant provisions of the Act.

Since the penalty provisions of the Spam Act came into effect in April 2004, ACMA has issued formal warnings to eight companies or individuals.

Infringement Notices

According to Schedule 3 of the Spam Act, ACMA may choose to issue infringement notices for breaches of the legislation, instead of initiating court proceedings.

These are similar to on-the-spot fines for parking or speeding infringements.

A person who receives an infringement notice may refuse to pay, but could then be subject to a court action. If a contravention is proven in court, the offender could be penalised at a rate higher than that of the infringement notice.

Since April 2004, ACMA has issued infringement notices and fines to five companies or individuals.

Infringement Notices

Penalties

The infringement notice penalties for sending unsolicited commercial electronic messages are:

- \$440 per contravention for an individual, with a maximum penalty of \$22 000 set for all contraventions that occur on a single day.
- \$2200 per contravention for a body corporate, with a maximum penalty of \$110 000 set for all contraventions that occur on a single day.

The infringement notice penalties for sending commercial messages without an unsubscribe facility, or without accurate sender information, or for a contravention of the harvesting provisions, are half of these amounts.

Court Action

ACMA may initiate a court action in respect of a breach of the legislation. If a contravention is found to have occurred, ACMA 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 activity.

Any person who has suffered loss or damages from someone else contravening the Spam Act, or ACMA on their behalf, may apply to the court to make an order for compensation.

In 2005 ACMA initiated proceedings against one alleged spammer in the Federal Court. The case was still before the court at November 2005.

QUESTIONS

Q11 Are these enforcement measures suitable and appropriate?

Q12 Are there any spamming activities so serious as to warrant criminal sanctions?

Court imposed penalties for spamming

The main penalty provisions of the Spam Act are:

- Sending unsolicited commercial electronic messaging;
- Sending commercial electronic messages to a non-existent address; and
- Aiding, abetting or otherwise being a party to such a contravention.

The maximum penalties that a court may impose for sending spam are:

- \$2200 per contravention for an individual, with a maximum penalty of \$44 000 set for all contraventions that occur on a single day.
- \$11 000 per contravention for a body corporate, with a maximum penalty of \$220 000 set for all contraventions that occur on a single day.

Where a court has found an individual or business to be in contravention of the particular provision in the past, and they have contravened subsequent to the court finding, then these amounts are five times higher. For example: \$55 000 per contravention for a body corporate, with a maximum penalty of \$1.1 million set for all contraventions that occur on a single day.

Penalty amounts for other offences

Additional penalty provisions in the Spam Act are:

- failure to include accurate sender information;
- failure to include a functional unsubscribe capability;
- address harvesting software and harvested lists—supply, acquisition, use; and
- aiding, abetting or otherwise being a party to such a contravention.

Where a court has found an individual or business to be in contravention of the particular provision in the past, and they have contravened subsequent to the court finding, then these amounts are five times higher. For example: \$27 500 per contravention for a body corporate, with a maximum penalty of \$550 000 set for all contraventions that occur on a single day.

The Court may also require a spammer to compensate the victim (s.28) or surrender any financial gain associated with the activity (s.29).

Enforceable undertakings

Part 6 of the Spam Act permits ACMA to accept enforceable undertakings in appropriate circumstances. These are effectively a formal administrative promise to not breach particular provisions of the Spam Act. It may also consist of a promise to perform a particular action in respect of the legislation. The acceptance of such an undertaking would not preclude ACMA from instituting proceedings against a person who was suspected of contravening a civil penalty provision.

Since April 2004, ACMA has accepted three enforceable undertakings from companies and individuals.

Injunctions

Part 5 of the Spam Act allows the Federal Court to grant injunctions in relation to contraventions of civil penalty provisions. These injunctions can be either ‘restraining’, ‘performance’, or ‘interim’ injunctions and are designed to require a person to refrain from engaging in a particular conduct or to undertake a particular action.

2.4.2 Telecommunications Act

The Spam Act was accompanied by several consequential amendments to the Telecommunications Act. These amendments extended the investigation capabilities of ACMA to have application to the Spam Act and also provided a framework to enable the development of industry codes relating to the sending of commercial electronic messages.

These amendments empower ACMA to carry out investigations in relation to breaches of the Spam Act (Part 26—investigations, Part 27—information-gathering powers and part 28—enforcement).

The amendments made to Part 26 of the Telecommunications Act enable ACMA to investigate a contravention of the Spam Act, or a code registered under Part 6 of the Telecommunications Act.

Warrant—search and seizure

Amendments were made to Part 28 of the Telecommunications Act which deals with the enforcement powers of inspectors. The amendments allow for searches relating to breaches of the Spam Act to be conducted under the authority of a search warrant or with the consent of the owner or occupier. Searches to monitor compliance are also able to be conducted. An inspector is able to require the giving of certain information, or production of certain documents, relevant to compliance with the Spam Act.

Under this provision, ACMA may apply to a magistrate to be granted a warrant to search premises involved in a breach of the Spam Act. If a thing is found that has been, or is being, used to breach the Act, or provides evidence of the breach, the inspector may seize that item.

A search of a premises may only take place if an inspector has a warrant obtained from a magistrate, or has been given the consent of the owner or occupier of the premises.

The search and seizure provisions relating to breaches of the Spam Act are consistent with existing provisions contained in the Telecommunications Act, and in other Commonwealth legislation.

ACMA has reported that during 2004–05, the premises of five companies or persons were subject to search warrants.

Monitoring warrants

Section 547 (d–f) of the Telecommunications Act allows ACMA to apply for a monitoring warrant, which would be used to ascertain compliance with the Spam Act where a person had been previously found by a court to have breached the legislation. The inspector may search the premises, inspect any document or thing and remove or take copies of documents.

Warrant – access to computer data

**Telecommunications Act,
Section 547J**

‘Access to computer data that is relevant to the *Spam Act 2003*’

Scope

(1) This section applies if:

(a) both:

(i) a warrant is in force under Division 3 authorising an inspector to enter particular premises; and

(ii) the warrant relates to the Spam Act 2003; or

(b) a warrant is in force under Division 5A authorising an inspector to enter particular premises.

Application to magistrate for access order

(2) The inspector may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow the inspector to do one or more of the following:

(a) access data held in, or accessible from, a computer that is on those premises;

(b) copy the data to a data storage device;

(c) convert the data into documentary form.

Grant of access order

(3) The magistrate may grant the order if the magistrate is satisfied that:

(a) there are reasonable grounds for suspecting that a thing connected with a breach of the Spam Act 2003 is held in, or is accessible from, the computer; and

(b) the specified person is:

(i) reasonably suspected of having been involved in the breach; or

(ii) the owner or lessee of the computer; or

(iii) an employee of the owner or lessee of the computer; and

(c) the specified person has relevant knowledge of:

(i) the computer or a computer network of which the computer forms a part; or

(ii) measures applied to protect data held in, or accessible from, the computer.

Offence

(4) A person is guilty of an offence if:

(a) the person is subject to an order under this section; and

(b) the person omits to do an act; and

(c) the omission breaches the order.

Penalty: Imprisonment for 6 months.

Definitions

(5) In this section:

data includes:

- (a) information in any form; and
- (b) any program (or part of a program).

data held in a computer includes:

- (a) data held in any removable data storage device for the time being held in a computer; and
- (b) data held in a data storage device on a computer network of which the computer forms a part.

data storage device means a thing containing, or designed to contain, data for use by a computer.

(6) This section does not, by implication, affect the meaning of the expression data when used in any other provision of this Act or the Telecommunications (Consumer Protection and Service Standards) Act 1999.

According to section 547J of the Telecommunications Act, an additional warrant may also be issued by a magistrate that would require a person to assist the inspector in assessing, copying or printing computer data and records. This provision is intended to facilitate access to password-protected or otherwise encrypted electronic documents. ACMA has gathered information under such orders on two occasions.

The warrant provisions allow for sufficient admissible evidence to be gathered for a court to make an informed and considered judgement.

Telecommunications Act—Part 6

Amendments were also made to Part 6 of the Telecommunications Act to enable additional industry codes and standards to be made relating to unsolicited commercial electronic messages. This enables industry sections to develop codes and register them with ACMA. The role of industry in relation to the Spam Act is discussed further in Chapter 4.

QUESTIONS

- Q13 Are the investigatory powers granted in these sections sufficient and appropriate for effective enforcement of the Spam Act?
- Q14 Do they go too far?
- Q15 Do they not go far enough?

2.5 Spam Act—Part 7 Miscellaneous

2.5.1 Additional ACMA functions

**Spam Act—Section 42
'Additional ACMA functions'**

The ACMA has the following functions:

(a) to conduct and/or co-ordinate community education programs about either or both of the following:

- (i) unsolicited commercial electronic messages;
- (ii) address-harvesting software;

in consultation with relevant industry and consumer groups and government agencies;

(b) to conduct and/or commission research into issues relating to either or both of the following:

- (i) unsolicited commercial electronic messages;
- (ii) address-harvesting software;

(c) to liaise with regulatory and other relevant bodies overseas about co-operative arrangements for the prohibition or regulation of either or both of the following:

- (i) unsolicited commercial electronic messages;
- (ii) address-harvesting software.

In Section 42, additional functions to be carried out by ACMA are described. These empower ACMA to initiate education and awareness programs, to conduct research relating to spam and to enter into cooperative arrangements with overseas bodies regarding spam.

This part also refers to giving effect to international conventions on spam (s.45). Although such formal regulatory-based agreements do not yet exist, ACMA and DCITA have entered into a number of bilateral and multilateral agreements with other countries, in accordance with s.42(c) (as above). Chapter 5 of this paper contains a discussion on international cooperative arrangements, and Chapter 6 considers ACMA’s education and awareness activities, in the context of the Government’s multi-layered strategy against spam.

2.5.2 Implied freedom of communications

**Spam Act, section 44
‘Implied freedom of political communication’**

This Act does not apply to the extent (if any) that it would infringe any constitutional doctrine of implied freedom of political communication.

Section 44 of the Spam Act provides that the legislation does not infringe any constitutional doctrine of implied freedom of political communication.

The ‘Designated Commercial Electronic Messages’ provision (see Chapter 2.6 below) also serves to protect the freedom of political and religious speech.

2.6 Spam Act—Schedule 1 Designated commercial electronic messages

Schedule 1 deals with the special rules that apply under the Spam Act for certain commercial electronic messages sent by certain groups. Special rules applying to commercial messages which consist of factual information are also outlined in this part.

These messages, known as ‘designated commercial electronic messages’, are permitted to be sent under the Act without prior consent, and are not required to include an unsubscribe option.

The categories of designated commercial electronic messages identified in Schedule 1 are:

- messages which contain only factual information (but which may also carry certain permitted other information (schedule 1, s.2);
- certain messages sent by or on behalf of government bodies, political parties, religious organisations or charities (schedule 1, s.3); and
- certain messages sent by or on behalf of educational institutions (schedule 1, s.4).

Spam Act, Schedule 1(2–4)

‘Designated commercial electronic messages’

2 Factual information

(1) For the purposes of this Act, an electronic message is a designated commercial electronic message if:

(a) the message consists of no more than factual information (with or without directly-related comment) and any or all of the following additional information:

- (i) the name, logo and contact details of the individual or organisation who authorised the sending of the message;
- (ii) the name and contact details of the author;
- (iii) if the author is an employee—the name, logo and contact details of the author's employer;
- (iv) if the author is a partner in a partnership—the name, logo and contact details of the partnership;
- (v) if the author is a director or officer of an organisation—the name, logo and contact details of the organisation;
- (vi) if the message is sponsored—the name, logo and contact details of the sponsor;
- (vii) information required to be included by section 17;
- (viii) information that would have been required to be included by section 18 if that section had applied to the message; and

(b) assuming that none of that additional information had been included in the message, the message would not have been a commercial electronic message; and

(c) the message complies with such other condition or conditions (if any) as are specified in the regulations.

3 Government bodies, political parties, religious organisations and charities

For the purposes of this Act, an electronic message is a designated commercial electronic message if:

(a) the sending of the message is authorised by any of the following bodies:

- (i) a government body;
- (ii) a registered political party;
- (iii) a religious organisation;
- (iv) a charity or charitable institution; and

(b) the message relates to goods or services; and

(c) the body is the supplier, or prospective supplier, of the goods or services concerned.

4 Educational institutions

For the purposes of this Act, an electronic message is a designated commercial electronic message if:

(a) the sending of the message is authorised by an educational institution; and

(b) either or both of the following subparagraphs applies:

(i) the relevant electronic account-holder is, or has been, enrolled as a student in that institution;

(ii) a member or former member of the household of the relevant electronic account-holder is, or has been, enrolled as a student in that institution; and

(c) the message relates to goods or services; and

(d) the institution is the supplier, or prospective supplier, of the goods or services concerned.

Designated commercial electronic messages must comply with the requirements of s.17 of the Spam Act which requires messages to contain information that clearly identifies the individual or organisation that authorised the sending of the message, and provide details of how they can be contacted.

The provision is mainly a precautionary measure, as the majority of messages sent from these groups would be non-commercial in nature and therefore outside of the scope of the Spam Act.

Under this provision, several restrictions apply. The message must also be commercial in nature to fall under the coverage of the Spam Act.

For the organisations listed in Schedule 1, (3–4) it is necessary for the messages to be in respect of goods or services that are being supplied by the originating organisation.

The purely factual messages provision allows messages to be sent which might be considered to have some commercial element, but are generally considered acceptable, such as in the case of a product recall notice.

The designated messages provision has been designed to ensure there is no unintended restriction on government to business or government to citizen communication, and to protect the freedom of religious and political speech.

QUESTIONS

Q16 Are the provisions relating to designated commercial electronic messages necessary?

Q17 Are these provisions appropriate as to:

(a) exemption from the prohibition on unsolicited commercial electronic messages?

(b) exemption from the requirement for a functional unsubscribe facility?

(c) other issues?

2.7 Spam Act - Schedule 2- Consent

2.7.1 Express and inferred consent

Spam Act, Schedule 2, Clause 2 'Consent—Basic definition'

For the purposes of this 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.

The Spam Act hinges on the concept of 'consent'. A key goal of the legislation is to provide people with the right to choose which messages they receive. The consent requirement addresses the invasive nature of commercial messaging. The second clause in Schedule 2 of the Spam Act requires the sender of any commercial electronic message to have the consent of the addressee prior to that message being sent. Consent may be 'express' consent or 'inferred' consent.

Express consent is where there has been a direct request to receive commercial electronic messages, such as when a person has subscribed to an electronic mailing list.

According to Schedule 2, certain conduct or relationships can also give rise to an inferred consent. Inferred consent is when a person has not directly requested information but has demonstrated a clear expectation that they wish to receive messages, based on their conduct and their relationship with the sender.

Consent can be inferred from an existing business relationship. For example if the person has an existing business relationship with the sender and as part of that relationship has knowingly and directly provided an electronic address to the sender, then it would be reasonable to infer that the person has consented to receiving certain commercial electronic messages from the sender.

Such messages must only be in relation to the purpose for which the electronic address was provided. For example, a client providing email contact details for a specific product or service might reasonably expect messages about that product or service, but may not reasonably expect to receive messages about other unrelated products or services.

2.7.2 Conspicuous publication

Consent cannot be inferred from the mere fact that a relevant electronic address has been published. Another scenario in which consent can sometimes be inferred is when an electronic address is conspicuously published. Conspicuous publication arises where the electronic address of a person or organisation has been made publicly available (such as in an advertisement for a person’s business activities). In this situation, it is reasonable to infer that consent has been granted to send commercial electronic messages to that address.

Under the conspicuous publication rule, the message must also directly relate to the published employment function or role of that individual or organisation. For example, if a plumber advertises his email address in the Yellow Pages® or on his public website, then he could reasonably expect to receive emails advertising plumbing supplies or offers of work, but not messages unrelated to his work, such as emails advertising discounted pharmaceuticals.

Consent cannot be inferred under this rule if the publicly advertised address is accompanied by a statement that the account-holder does not wish to receive unsolicited commercial electronic messages.

QUESTIONS

A key principle of the Spam Act is that people should be able to decide what messages are sent to them, and have that decision respected.

-Q18 Do the consent provisions effectively support people’s ability to choose what messages are sent to them?

-Q 19 Do the consent provisions provide a clear distinction between legitimate commercial electronic messages and spam?

2.8 Other

Facsimile spam

Facsimile communications are currently excluded from coverage by the Act through regulation.

Original consultations on whether facsimile spam (or ‘fax spam’) should be covered by the legislation failed to yield conclusive results. The Government decided to exclude fax spam from the Act by regulation, allowing the potential for it to be brought into coverage at a later stage. Since the Act came into effect, the Minister for Communications, Information Technology and the Arts, ACMA and DCITA have received a number of queries from the general public concerning the application of the Act to fax spam.

In the case where a single phone line is used to service a fax and phone system in one establishment, consumers and small business operators have reported the inconvenience of nuisance faxes tying up the phone line, often the business phone number. In the case of small business operators working from home, the home and business phone are both affected. There is also concern over the consumption of costly fax paper and toner. Incidents of failure to comply with opt-out requests have also been reported.

DCITA has issued a discussion paper that considers the possible establishment of a do not call register. While that discussion paper asks whether direct marketing by fax should be covered under a do not call register, it notes that the Spam Act currently has the capacity to deal with commercial messages sent via fax and that the issue of unsolicited fax communications will be considered by the Spam Act Review. Further information is available at www.dcita.gov.au/donotcall

QUESTIONS

- Q 20 Should commercial electronic messages sent by facsimile be covered by the Act?*
- Q21 Why?*
- Q22 Why not?*

Chapter 3—Interaction of the Spam Act with other legislation

Spam is often used as a delivery mechanism for fraudulent and other malicious or misleading materials, which is of concern to several regulatory and policy agencies. In the implementation of the Spam Act, ACMA is required to work closely with a number of enforcement agencies.

When ACMA receives a spam complaint, it is analysed to determine whether the Spam Act has been breached and acted on accordingly. If the complaint reveals that another law is likely to have been breached, it may be passed on to the relevant enforcement agency for further investigation. ACMA's online complaint form for reporting spam allows the complainant to indicate if they wish to have their details passed on to another agency.

In the case of spam which is malicious or fraudulent in nature, ACMA may pass the complaint on to the Australian High Tech Crime Centre (AHTCC), a national centre hosted by the Australian Federal Police. An ACMA investigator is stationed in the AHTCC to allow sharing of intelligence and joint investigations where appropriate. This network is assisting a more targeted response to criminal activity associated with spam, such as fraud and cybercrime.

3.1 Criminal laws

Spam is increasingly being used as a vehicle for malicious content, including 'phishing' fraud and viruses. Such spam is a breach of existing criminal laws including fraud offences and cybercrime offences. ACMA works closely with the AHTCC and regularly refers criminal spam to that centre. An ACMA staff member is stationed in the AHTCC to allow close working relationships.

ACMA also works through international channels to shut down offshore infected computers and fraudulent Internet domains identified by ACMA investigators as being used by spammers and phishers to target Australians.

3.2 Privacy Act

The National Privacy Principles contained in the *Privacy Amendment (Private Sector) Act 2000* also contain provisions similar to the Spam Act which apply more generally to direct-marketing. These principles deal with the issues of seeking consent to send a commercial message, identifying the sender to the recipient and providing opportunities for the recipient to opt-out of receiving future messages. These provisions have recently been subjected to a legislative and a Senate Committee review. The reviews resulted in recommendations which seek to enhance the rights of consumers to control the degree of direct-marketing material they receive. Further information is available from www.privacy.gov.au

3.3 Broadcasting Services Act

Spam messages containing links to websites with offensive or illegal content are subject to a co-regulatory scheme for Internet content. The scheme was established by the *Broadcasting Services Amendment (Online Services) Bill 1999*, which amended the *Broadcasting Services Act 1992*. The Act empowers ACMA to receive and investigate complaints about Internet content. If ACMA finds that the content is prohibited, it can take steps to have the content removed from the Internet or to filter access to the site. If the content is sufficiently serious, ACMA may also refer the material to the appropriate law enforcement agency.

3.4 Trade Practices Act 1974 and State and Territory fair trading laws

Spam messages may carry scams or be otherwise misleading and deceptive. ACMA liaises closely with the Australian Competition and Consumer Commission, which enforces the *Trade Practice Act 1974*, and with state and territory fair trading agencies on new scams being promoted into Australia via spam.

General Questions on Part A

- *Are the provisions operating effectively?*
- *Are there any provisions which could be improved? If so, how?*
- *Have any of the provisions had a negative impact?*
- *Are there any other provisions which require further clarification or education materials?*

PART B :THE MULTI-LAYERED STRATEGY

Part B deals with the operation of the legislation in the context of the Australian multi-layered spam strategy.

Chapter 4—The role of industry

This chapter addresses the operation of the provisions of the legislation that deal with industry codes and standards. It also discusses the extent to which Internet industry and e-marketing bodies, and their members, have developed guidelines and standards to ensure compliance with the Act, and have made available spam-related information and product resources to consumers.

4.1 Industry codes and standards

The Telecommunications Act was amended to provide for the development of industry codes in recognition of the essential role that industry has in managing the levels of spam in Australia. This was put in place on the basis that industry is best placed to address spam.

Part 6 of the Telecommunications Act deals with industry codes and standards. It provides for industry bodies and associations to develop codes of practice and have them approved and registered by ACMA. Once industry participants sign up to the code, they bind themselves to comply with its requirements.

Industry codes further support the operation of the Spam Act and help to define good business practices. Codes of practice also provide industry with guidelines that encourage compliance with the Spam Act, in a format that is relevant to their specific business needs and practices. These also foster an environment where electronic technologies remain as legitimate business marketing tools.

Although compliance with the codes is voluntary, ACMA does have the power to direct industry participants to comply with the codes. ACMA can seek to impose pecuniary penalties under Part 31 of the Telecommunications Act for a failure to comply with such a direction. ACMA also has the ability to create standards if a sector fails to register a code.

The *Spam (Consequential Amendments) Act 2003* (the Consequential Amendments Act) amended the Telecommunications Act to insert more examples of the matters which can be dealt with by industry codes and standards relevant to the ISP and electronic messaging service provider industries (s113(3)(q)-(v)). These examples include:

- procedures to be followed by ISPs and electronic messaging service providers when dealing with ‘unsolicited commercial electronic messages’, otherwise known as spam;
- providing information to consumers about the availability, use and appropriate application of software for filtering spam;
- the action to be taken to assist in the development and evaluation of software for filtering spam;

- action to be taken in order to minimise or prevent the sending or delivery of spam, including the configuration of servers so as to minimise or prevent the sending or delivery of spam, and the shutdown of open relay servers;
- action to be taken to ensure responsible practices in relation to the use of commercial electronic messages to market, advertise or promote goods or services to individuals who are under 18 years of age; and
- procedures to be followed in relation to the giving of consent by relevant electronic account-holders to the sending of commercial electronic messages.

4.1.1 eMarketing code

The e-marketing industry is potentially a major source of commercial electronic messages and has a vested interest in ensuring responsible behaviour from its members. In 2004, an eMarketing Code of Practice was developed by an industry committee for relevant peak bodies. This process was led by the Australian Direct Marketing Association (ADMA). The code provides practical guidance for the industry to use e-marketing responsibly, to handle any complaints about spamming practices and to monitor industry compliance. The code represents best practice compliance with the provisions of the Spam Act.

The eMarketing Code was registered by ACMA in March 2005.

Under the eMarketing Code of Practice, an organisation that is a member of the industry may also sign up to the code, indicating its willingness and commitment to comply with the code rules. A signatory to the code may also nominate a Recognised Industry Body (such as an industry association), of which they are a member, to handle complaints about their compliance with the code. As of October 2005, there were 48 signatories to the code. The code can be viewed on the ADMA website www.adma.com.au

Registration of the code means that, if necessary, ACMA can enforce compliance with the code rules on all members of the e-marketing industry, as defined by the Telecommunications Act, and can direct individual e-marketing firms to comply with it. ACMA provided support and advice for the code committee towards the finalisation and registration of the code, but did not otherwise influence its content.

ACMA is monitoring the performance of e-marketers against the code rules and has the power to require a company whose compliance appears to be inadequate to address any process problems or difficulties.

The code allows for an industry-based complaints handling process, with safety-net provisions so that complaints can be referred to ACMA as a last resort. Signatories to the code are required to nominate an ACMA-accredited Recognised Industry Body to handle escalated complaints on their behalf. By June 2005, ACMA had accredited three industry organisations to deal with complaints against e-marketers -ADMA, the Advertising Federation of Australia and the Public Relations Institute of Australia.

In the first instance, a complaint about a breach of the code will be handled by the e-marketing company to which the complaint relates—generally the organisation that sent the commercial electronic message, or authorised that it to be sent. In cases where the complaint is not successfully resolved by the responsible e-marketer, it will be referred to

the Recognised Industry Body nominated by the e-marketing company. However, if the complaint relates to an e-marketing company that is not a signatory to the code, or if they are a signatory to the code but have not nominated a Recognised Industry Body, ACMA will handle the complaint. At any time during the complaint-handling process, a complainant may request that his/her complaint be referred to ACMA for consideration. More information about the complaint process can be found on the ACMA website www.acma.gov.au

Industry organisations have been actively promoting the code to their members. They have also been actively engaged in self-regulatory compliance. Recognised industry bodies have received complaints about e-marketers from members of the public and have resolved them directly through industry compliance processes. The eMarketing Code successfully complements the Australian anti spam regime. It sets a standard of behaviour that while serving a real marketing purpose is beyond the minimums required under the Spam Act.

ACMA itself has referred public complaints about e-marketers who are signatories to the eMarketing Code to the relevant Recognised Industry Body.

QUESTIONS

Q23 Does the eMarketing Code of Practice sufficiently cover the practices of e-marketing activities?

Q24 Is the application of the e-marketing code too wide?

Q25 Is the application of the e-marketing code too narrow?

4.1.2 Internet industry code

An industry code of practice is also in development for ISPs and email service providers. The code is sponsored by the Internet Industry Association (IIA), in conjunction with the Western Australian Internet Association and the South Australia Internet Association.

The draft code is intended to set out the steps that ISPs should take, as carriers of email traffic, to reduce the amount of spam entering or being sent over Australian networks. This draft code is designed to complement the spam code for e-Marketers. ACMA, consumer groups and the public have provided comment during the development phase of the code.

This code is expected to be submitted to ACMA soon for registration. Registration would allow ACMA to direct individual ISPs to comply with it.

QUESTIONS

Q26 Are industry codes useful and successful?

Q27 What could be done to aid their success?

4.1.3 Industry standards

Industry standards may also be another useful mechanism through which compliance with anti-spam laws can be maximised. Standards can reinforce industry codes and may also be developed where industry has not put in place codes of practice, or where compliance with such codes is problematic.

ACMA has reserve powers to make an industry standard in the event that a code has not been developed, or where it considers that the industry code is deficient. Compliance with industry standards made by ACMA is mandatory and can be enforced under Part 31 of the Telecommunications Act and civil penalties may apply.

4.2 Non-regulatory activities

Industry cooperation is an essential element of the Government's multi-layered approach to spam. Industry responses to spam may encompass a number of options in addition to best practice guidelines and industry codes, such as consumer awareness-raising and technical counter-measures.

4.2.1 Awareness-raising and consumer resources

The Internet and e-marketing industry has worked to minimise user risk of spam through awareness raising and education activities.

The IIA's 'National Spam Initiative' coincided with the introduction of the Spam Act and aimed to empower Internet users, from home users to corporate organisations, to better control their exposure to spam. The initiative included information designed to educate consumers about spam and how it can be managed. The IIA's members also supplied anti-spam products that were made available for a free one-month trial.

ADMA also promotes its eMarketing Code through an Internet site dedicated to educating the industry about the code and responsible e-marketing. ADMA provides training for new signatories to the code about strategies to ensure compliance with the code and the Spam Act.

4.2.2 Industry technical measures

In addition to educating consumers about prevention strategies to protect themselves against spam, the industry has also responded by making technical filtering options available for consumers.

The Internet security industry has evolved to keep pace with spam and other emerging online threats. Spam is increasingly becoming associated with more malicious online threats. e-Security specialists have responded to the blending of threats with a range of new products. Computer security software is being integrated to provide firewalls and combined with anti-virus, anti-spyware, and anti-spam software. Security tools are also being packaged with new software platforms and hardware components prior to reaching the consumer.

E-security and spam are increasingly being regarded internationally as interwoven parts of a single problem: the misuse and malicious use of the online environment. The Australian Internet and e-security industry is working with ACMA to address emerging global trends such as hijacked or “zombie” computers that spammers use to distribute spam around the world.

4.2.3 Protecting industry development

One of the principal goals of an anti-spam regulatory framework is ensuring that the negative impact of such a regime on legitimate business is kept to a minimum.

Compliance with anti-spam measures can result in positive outcomes for individuals and businesses. Compliance with the requirements of the legislation provides a legitimate means for marketing and advertising material to be received by the intended audience.

QUESTIONS

Q28 From an industry perspective, what has been the impact of the Spam Act?

Chapter 5—International Cooperation

This chapter addresses how the legislation has enabled the Australian Government and industry bodies to enter into agreements with other countries to reduce the total volume of spam, participate in global anti-spam initiatives and move towards the development of international guidelines and the application of the legislation in other jurisdictions.

5.1 The legislation

Section 42 of the Spam Act outlines additional functions for ACMA, including those relating to international cooperation. Subsection (c) gives ACMA the additional function ‘to liaise with regulatory and other relevant bodies overseas about co-operative arrangements for the prohibition or regulation of either or both of the following: (i) unsolicited commercial electronic messages; (ii) address-harvesting software’.

The Spam Act also provides for the implementation of future international conventions dealing with spam. Section 45 of the Spam Act provides for regulations made under the legislation to give effect to international conventions dealing with commercial electronic messages and address-harvesting software.

Spam is a global problem that requires a global solution. International cooperation is a vital part of the Australian multi-layered approach to spam. Preventing spam nationally is important, but it has been recognised that long-term gains will only be made through cooperation with other countries and overseas regulators.

The vast majority of spam on Australian networks originates from overseas. Australia is actively seeking to form relationships with other countries and organisations which are addressing the spam problem. This is a long-term strategy and it is likely to take some time before the full benefits from these arrangements, in Australia or internationally, are realised.⁸ By removing Australia as a source of spam, the Government is able to promote, facilitate and participate credibly in international efforts on spam.

5.2 The Australian Government’s international anti-spam agreements

Since the introduction of the Spam Act, the Australian Government has established a number of international anti-spam information sharing and enforcement arrangements with other governments and agencies.⁹

In October 2003, DCITA and ACMA signed an agreement with the Korea Information Security Agency (KISA) concerning cooperation in the regulation of spam. This initial Memorandum of Understanding (MoU) was later used as a foundation for a wide-ranging Asia Pacific agreement on spam.

⁸ *Spam Bill Explanatory Memorandum*, 2003, B:2

⁹ The agreements discussed in this section are available for download at www.dcita.gov.au/spam

5.2.1 UK, US and Australia—tripartite MoU on spam—July 2004

In July 2004, ACMA and the Australian Competition and Consumer Commission (ACCC), signed a MoU with agencies from the United States and the United Kingdom. These agencies were the United States Federal Trade Commission, the Secretary of State for Trade and Industry in the United Kingdom, the Office of Fair Trading in the United Kingdom and the United Kingdom's Information Commissioner. This MoU is designed to facilitate the sharing of enforcement information across borders.

5.2.2 Australia and Thailand—joint statement on telecommunications and information technology—July 2004

DCITA signed a joint statement with the Ministry of Information and Communication Technology of the Kingdom of Thailand on telecommunications and information technology in July 2004. The statement includes an undertaking to exchange information about anti-spam policies and strategies.

5.2.3 London Action Plan on spam—October 2004

In October 2004, ACMA and the ACCC agreed to participate in the London Action Plan (LAP), a network of public and private sector bodies established by the US Federal Trade Commission and the UK Office of Fair Trading to curb the activities of international spammers. The plan draws together government and private sector organisations in over 20 countries to fight spam. Through its participation in the LAP, Australia also supported the US Federal Trade Commission's *Operation Zombie Drone* - an international campaign to educate ISPs and other Internet connectivity providers about hijacked, or 'zombie' computers that spammers use to distribute spam around the world.

5.2.4 Seoul-Melbourne Multilateral MoU—Asia Pacific region—April 2005

In October 2003, DCITA and ACMA signed an agreement with the Korea Information Security Agency concerning cooperation in the regulation of spam. This initial Memorandum of Understanding (MoU) was used as the foundation for a wide-ranging Asia Pacific agreement in April 2005.

The Seoul-Melbourne Multilateral MoU on Cooperation on Countering Spam includes twelve agencies in ten major Asian economies and has a strong focus on technological, educational and policy responses to spam and the underlying Internet security flaws that spammers exploit. The MoU provides for additional agencies and countries to join the agreement in the future.

5.2.5 Asia Pacific assistance

The Australian Government is also responding to requests for information and assistance from nations wishing to establish their own strategic responses to spam. Australia is assisting Pacific Island countries in the development of e-commerce legislation. A pilot project is currently being designed to assist Pacific countries to maximise the potential

opportunities for economic and social development offered by e-commerce by promoting take-up and strengthening e-security.

The first objective is to contribute to the legislative framework in the Pacific by providing a legislative anti-spam model for ready adoption by Pacific Island Countries.

5.3 Involvement with international organisations

Australia is also working with international organisations such as the International Telecommunication Union (ITU), the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC TEL), the Asia-Pacific Telecommunity (APT), the Pacific Islands Telecommunications Association (PITA) and the Organisation for Economic Co-operation and Development (OECD) to develop a multilateral approach to reducing spam.

The aims of this range of interactions has been to reach the greatest audience possible with the message that strong legislation is needed but a wider range of interactions and cooperation between regulators, industry associations, ISPs and others is crucial to solving the global spam problem.

5.3.1 Organisation of Economic Co-operation and Development (OECD)

Australia has been influential in the establishment of the OECD's anti-spam taskforce which it also chairs. The task force is working on an 'anti-spam toolkit' which will provide countries that are intending to create anti-spam policies with information to support a multi-layered strategy against spam. Australia has taken a lead role in the development of the anti-spam regulation element of the toolkit, to assist countries looking to establish anti-spam legislation. This evolving resource will be made available to economies both within and outside of the OECD.

Australia is also encouraging greater collaboration between international organisations on spam activities and will participate in an APEC workshop on spam at the APEC TEL 33 meeting. More information is available on the OECD website at www.oecd.org.au

5.3.2 International Telecommunications Union (ITU)

The ITU has been significant in bringing together a wide range of countries and regulators on the issue of spam, especially through the Global Symposium of Regulators.

The ITU secretariat is preparing a suggested framework for global cooperation on spam for the World Summit on the Information Society meeting in November 2005. Australia is a participant in this process. More information is available on the ITU website at www.itu.org

5.3.3 APEC Telecommunications and Information Working Group (APEC TEL)

Australia has assisted in the development of the APEC Principles and Implementation Guidelines for Action Against Spam. These principles and implementation guidelines were adopted at the APEC Ministerial Meeting in June 2005. More information is available on the APEC website at www.apec.org

APEC is also inviting the OECD, the ITU, and the Asia Pacific Telecommunity to participate in a workshop on spam in Canada in 2006.

5.3.4 International Consumer Protection and Enforcement Network (ICPEN)

In February 2005, the Australian Government participated in an international project to investigate and collect information about spammers and spamming activities. Coordinated by the ACCC, the International Consumer Protection and Enforcement Network Internet Sweep project on spam involved 76 agencies from 25 countries including participants from the London Action Plan against spam. More information is available at www.icpen.org

5.3.5 Asia-Pacific Telecommunity (APT) and Pacific Islands Telecommunications Association (PITA)

In August 2005, DCITA and ACMA participated in the APT Symposium on Network Security and Spam. In October 2005, DCITA sponsored and ACMA participated in the joint APT/ PITA conference on spam and security.

5.4 Other international Activities

In January 2004, Australia participated in the US Federal Trade Commission's (FTC) *Operation Secure Your Server*.¹⁰ This activity aimed to reduce the flow of unsolicited commercial email by urging organisations to close open relays. Spammers often exploit open relay ports on email servers which can be used to send spam anonymously. The operation involved notifying operators of open relays and requesting they shut their open ports to reduce opportunities for spammers. Australia's participation was managed through ACMA and the ACCC.

QUESTIONS

Q29 There are privacy constraints and other legislative constraints on spam investigations which require the sharing of information about spam and spammers across borders. Should these constraints be addressed? How?

¹⁰ More information is available at www.ftc.gov/bcp/online/edcams/spam/secureyourserver/

Chapter 6—Information and Awareness Activities

This Chapter addresses the information and awareness activities carried out by Government and other bodies to educate end-users and industry about the Spam Act and the mechanisms established to allow spam to be reported.

6.1 The legislation

Section 42 of the Spam Act provides ACMA with the ability to carry out additional functions, including community education programs about unsolicited commercial electronic messages and address-harvesting software, in consultation with the relevant industry and consumer groups and government agencies.

The effectiveness of the Spam Act largely hinges on consumers having a good awareness of the legislation, the recourse available and the avenues for lodging complaints.

It is particularly important that industry is made aware of the requirements of the Act so as to ensure that their marketing practices adhere to best practice compliance when sending legitimate commercial electronic messages.

6.2 Government education and awareness

The Government has used a variety of channels to communicate the requirements of the Spam Act. Numerous ongoing activities have been undertaken throughout the course of 2004 and 2005. These activities include public seminars, media interviews and magazine articles and the distribution of official government guides for business, government and consumers. Comprehensive online resources have also been developed.

The active enforcement of the Spam Act has also led to a greater awareness amongst businesses about how to comply with the legislation. These enforcement activities have been picked up in mainstream media, communicating the key message that significant issues of non-compliance will be actively investigated and enforced by ACMA. These activities continue to reduce the incidence of spam originating in Australia.

The Government continues to educate business and the community about the application of the Spam Act.

6.2.1 Early awareness raising activities

The Government commenced education and awareness activities in advance of the enforcement date of 10 April 2004 to alert end-users of their rights under the Spam Act, and to ensure that industry was made aware of the requirements of the Act.

In response to particular emergent types of spam, or particular industries involved in sending spam, ACMA also initiated targeted education and awareness activities outlining the compliance requirements and giving specific details relevant to the particular industry

or practice in question. For example, the emergence of mobile phone spam relating to nightclub promotion, and mobile phone spam promoting car sales companies, were tackled in this manner.

6.3 Spam Act and Internet security seminars for business

In 2004 and 2005 DCITA and ACMA ran a series of information seminars about the Spam Act's requirements for the business sector, with an emphasis on small business operators. More than 50 small business seminars were delivered throughout regional Australia.

The seminars were focused on providing the small business sector with useful tools to ensure compliance with the Spam Act, reduce the amount of spam they receive and safeguard their computer systems so they cannot be exploited by spammers. Positive feedback was received on this program with the majority of attendees reporting that the seminars were relevant and that the information would be useful to them.

The seminar program also provided a valuable channel for distributing DCITA and ACMA information guides specifically developed for business users. The promotion of the seminar series led to repeat interviews on ABC Regional Radio and a number of editorial pieces in regional and local press.

6.4 Publications

A variety of information materials have been developed by DCITA and ACMA to explain the Act's requirements in practical and easy-to-understand terms.

These materials target business, government organisations and consumers. Specific guides for business were developed in consultation with the business community to provide practical information about the Spam Act and its main requirements. DCITA, in conjunction with ADMA, has also developed fact sheets providing specific information for business and e-marketers.

Education materials targeting government bodies have also been distributed. An overview of the legislation and a practical guide to compliance have been circulated throughout Commonwealth, state, territory and local government.

The following resources are available for download at www.dcita.gov.au/spam or in hard copy by contacting DCITA at spam.comments@dcita.gov.au

- Spam Act 2003: An overview for business
- Spam Act 2003: A practical guide for business
- Spam Act 2003: An overview for government
- Spam Act 2003: A practical guide for government
- Spam Act 2003: What is a commercial electronic message?

- Fighting spam in Australia: A consumer guide
- Final Report on NOIE review of the spam problem
- ACMA Frequently Asked Questions

Consumers have benefited from an easy-to-understand guide to spam produced by ACMA, and a set of comprehensive frequently asked questions, available online at www.acma.gov.au. ACMA has also produced a consumer education slideshow about the Spam Act, including tips on how to reduce spam, which is also available through its website.

ACMA has produced a number of consumer ‘tool kits’ as part of its general telecommunications consumer education program. The ACMA brochure, ‘Fighting spam in Australia: a consumer guide’, was incorporated into ACMA’s Internet Tool Kit. This Tool Kit has been distributed in electronic, print and CD form.

6.5 Avenues for complaint

There appears to be a reasonable awareness amongst Australian consumers about the Spam Act and how to lodge a complaint. Enquiries to ACMA are dealt with by email or through a telephone enquiry hotline. From 1 July 2004 to 30 June 2005, the spam section of the ACMA website averaged 40 000 hits per month and more than 1500 enquiries were answered by email, letter or phone.

In October 2005 ACMA launched a new spam reporting tool. The SpamMATTERS software allows the public to report spam emails directly from their email software. The software uses a one-click process which sends spam mails direct and intact to ACMA via a plug-in for Microsoft Outlook which can be downloaded from the ACMA site (www.acma.gov.au). The forensic data gathered from complaints submitted in this way will assist ACMA to present evidence for cases in court. A component allowing for the submission of bulk spam complaints is being prepared for release at a later date.

6.6 Other groups

ACMA has convened a forum of industry and consumer groups on an *ad hoc* basis to advise on how best to educate consumers about protecting themselves from spam and e-security threats.

ACMA also works with other government agencies on consumer awareness of fraudulent messages.

QUESTIONS

Q30 Are there other types of awareness activities that should be undertaken in relation to the Spam Act?

Q31 Is there scope for further government/industry collaboration in relation to education and awareness activities?

Appendix A

Summary of questions for comment

PART A

2.1 Spam Act—Part 1—Introduction

2.1.2 Definition of a ‘commercial electronic message’

The Spam Act covers commercial electronic messages.

Q1 Do you think this provides suitable coverage?

Q2 Does it include things that it should not?

Q3 Does it fail to cover things that should be included?

2.2 Spam Act Part 2—Rules about sending commercial electronic messages

2.2.1 Unsolicited commercial electronic messages must not be sent

Q4 Does this provision cover messages that it should not?

Q5 Are there spam messages that are not currently covered by this provision that should be?

Q6 Does this provision suitably cover the spam problem?

2.2.2 The identification requirement

Q7 Is this a suitable requirement for commercial electronic messages?

2.2.3 The unsubscribe requirement

Q8 Is this a suitable requirement for legitimate commercial electronic messages?

2.3 Spam Act—Part 3—Rules about address-harvesting software and harvested address lists

Q9 Do the address harvesting provisions suitably cover spam-related activities?

Q10 Do these provisions cover circumstances that they should not?

2.4 Spam Act—Enforcement

Q11 Are these enforcement measures suitable and appropriate?

Q12 Are there any spamming activities so serious as to warrant criminal sanctions?

Q13 Are the investigatory powers granted in these sections sufficient and appropriate for effective enforcement of the Spam Act?

Q14 Do they go too far?

Q15 Do they not go far enough?

2.6 Designated commercial electronic messages

Q16 Are the provisions relating to designated commercial electronic messages necessary?

- Q17 Are these provisions appropriate as to:*
- (a) exemption from the prohibition on unsolicited commercial electronic messages?*
 - (b) exemption from the requirement for a functional unsubscribe facility?*
 - (c) other issues?*

2.7 Spam Act—Schedule 2—Consent

A key principle of the Spam Act is that people should be able to decide what messages are sent to them, and have that decision respected.

- Q18 Do the consent provisions effectively support people’s ability to choose what messages are sent to them?*
- Q19 Do the consent provisions provide a clear distinction between legitimate commercial electronic messages and spam?*

2.8 Other—Facsimile spam

- Q20 Should commercial electronic messages sent by facsimile be covered by the Act?*
- Q21 Why?*
- Q22 Why not?*

General Questions on Part A

- *Are the provisions operating effectively?*
- *Are there any provisions which could be improved? If so, how?*
- *Have any of the provisions had a negative impact?*
- *Are there any other provisions which require further clarification or education materials?*

PART B

4 The role of industry

- Q23 Does the eMarketing Code of Practice sufficiently cover the practice of e-marketing?*
- Q24 Is the application of the eMarketing Code too wide?*
- Q25 Is the application of the eMarketing Code too narrow?*
- Q26 Are industry codes useful and successful?*
- Q27 What could be done to aid their success?*
- Q28 From an industry perspective, what has been the impact of the Spam Act?*

5 International cooperation

- Q29 There are privacy and other legislative constraints on spam investigations which require the sharing of information about spam and spammers across borders. Should these constraints be addressed? How?*

6 Information and awareness

Q30 Are there other types of awareness activities that should be undertaken in relation to the Spam Act?

Q31 Is there scope for further government/industry collaboration in relation to education and awareness activities?