Spam Regulations 2004

Statutory Rules 2004 No. 56[1]

I, PHILIP MICHAEL JEFFERY, Governor-General of the Commonwealth of Australia, acting with the advice of the Federal Executive Council, make the following Regulations under the *Spam Act 2003*.

Dated 8 April 2004

P. M. JEFFERY
Governor-General

By His Excellency's Command

DARYL WILLIAMS
Minister for Communications, Information Technology and the Arts

Page

Contents

Part 1 Preliminary

1.1 Name of Regulations

These Regulations are the *Spam Regulations 2004*.

1.2 Commencement

These Regulations commence on the commencement of Parts 2 to 6 of the *Spam Act 2003*.

1.3 Definitions

In these Regulations:

Act means the *Spam Act 2003*.

carriage service has the same meaning as in the *Telecommunications Act 1997*.

carriage service provider has the same meaning as in the *Telecommunications Act 1997*.

carrier has the same meaning as in the *Telecommunications Act 1997*.

premium service means a premium service mentioned in:

(a) paragraph 3.12 (1) (a) of the *Telecommunications Regulations 2001*; or

(b) subparagraph 3.12 (1) (b) (i) of those Regulations; or

(c) paragraph 3.12 (1) (c) of those Regulations.

related person, in relation to the sender of a commercial electronic message, means a person who receives, or may receive, payment of a fee or charge, in relation to the use of an electronic address, on the basis of an agreement, arrangement or understanding with the sender, other than an agreement:

(a) made between the sender and a carrier or carriage service provider; and

(b) under which the fee or charge to be imposed by the carrier or carriage service provider in that capacity will be less than would otherwise be charged for the use of that kind of electronic address.

Part 2 Commercial electronic messages

2.1 Facsimile messages

For subsection 6 (7) of the Act, a facsimile message is a specified kind of electronic message.

Note The effect of subsection 6 (7) of the Act is that a kind of electronic message specified in regulations is not a ***commercial electronic message*** for the purposes of the Act.

Part 3 Rules about sending commercial electronic messages

3.1 Conditions

For paragraph 18 (1) (g) of the Act, this Part sets out conditions with which an electronic address must comply.

Note Paragraph 18 (1) (g) relates to an electronic address that is included in a commercial electronic message to send an unsubscribe message to the individual or organisation who authorised the sending of the commercial electronic message.

3.2 Unsubscribe facility — premium service

The use of the electronic address must not require the recipient of the commercial electronic message to use a premium service.

3.3 Unsubscribe facility — usual cost

The use of the electronic address must not cost more than the usual cost of using that kind of electronic address, using the same kind of technology as was used to receive the commercial electronic message.

3.4 Unsubscribe facility — fees and charges

(1) The use of the electronic address must not require the recipient of the commercial electronic message to pay a fee or other charge to:

(a) the sender of the message; or

(b) a related person.

(2) If the sender is also a carrier or a carriage service provider, subregulation (1) does not apply to a fee or charge ordinarily imposed by the sender:

(a) in the capacity of the carrier or carriage service provider; and

(b) on a monthly basis, or another periodic basis;

for the use of carriage services.

Note

1. Notified in the *Commonwealth of Australia Gazette* on 8 April 2004.

Australian Government

National Office for the Information Economy

Australian Communications Authority

Spam Act 2003:

A practical guide for business

adma
australian direct marketing association

CAUBE.AU

internet industry association

This guide provides practical information to businesses that send electronic messages. It explains the main requirements of the Spam Act 2003 (the Spam Act), and outlines business practices that comply with the legislation. The guide has been developed in consultation with key industry stakeholders to provide a clear explanation of the legislation's requirements.

The three key steps you should follow are:

1 Consent Only send commercial electronic messages with the addressee's consent - either express or inferred consent.

2 Identify Include clear and accurate information about the person or business that is responsible for sending the commercial electronic message.

3 Unsubscribe Ensure that a functional unsubscribe facility is included in all your commercial electronic messages. Deal with unsubscribe requests promptly.

Spam Act 2003: A practical guide for business, February 2004
ISBN (Print): 1 74082 046 0
ISBN (Online): 1 74082 047 9

Disclaimer

Please note:

This guide has been prepared by NOIE to provide information to business in relation to the sending of commercial electronic messages.

While every effort has been made to ensure that the document is accurate, no warranty, guarantee or undertaking is given regarding the accuracy, completeness or currency of the document. This guide should not be relied upon as legal advice. Users are encouraged to seek independent advice relevant to their own particular circumstances.

Links to other websites are inserted for convenience only and do not constitute endorsement of material at those sites, or any associated organisation, product or service.

TABLE OF CONTENTS

ABOUT THIS DOCUMENT

INTRODUCTION

The National Office for the Information Economy (NOIE) has prepared this guide in consultation with the business community to provide practical information about the Spam Act and guidance on steps that may be taken to assist in complying with it.

Italicised terms appear in the glossary on ***page 19***.

WHAT IS SPAM?

The Spam Act refers to spam as "unsolicited commercial electronic messaging".

"Electronic messaging" covers emails, instant messaging, SMS and other mobile phone messaging, but does not cover normal voice-to-voice communication by telephone.

To be covered by the Spam Act, the message must be commercial in nature – for instance offering a commercial transaction, or directing the recipient to a location where a commercial transaction can take place.

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

A single message may be spam. The message does not need to be sent in bulk, or received in bulk. The Spam Act makes no reference to bulk messaging - a single unsolicited commercial electronic message could be spam.

PURPOSE OF THE SPAM ACT 2003

The Spam Act was developed in response to the problems caused by the growing volume of *unsolicited commercial electronic messages*, or spam. Spam threatens the viability and efficiency of electronic messaging. It damages consumer confidence, obstructs legitimate business activities and imposes many costs on users. The legislation prohibits *unsolicited commercial electronic messages*.

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

120 DAY GRACE PERIOD

The Spam Act became law on 12 December 2003 with a proviso that its penalty provisions would come into effect 120 days later. This grace period was included to ensure that people could learn about the requirements of the Spam Act, and ensure that their business practices satisfy those requirements.

All provisions of the Spam Act are in effect from 10 April 2004.

THE PRIVACY ACT, AND THE NATIONAL PRIVACY PRINCIPLES

Businesses need to comply with the provisions of the Spam Act when sending commercial electronic messages.

Equally importantly, businesses should make sure that their practices are in accordance with the National Privacy Principles, available from **www.privacy.gov.au**, in all activities where they deal with personal information. Personal information includes customers' contact details.

NOIE

The National Office for the Information Economy is responsible for providing information and education material about the Spam Act during its implementation.

Additional material about the Spam Act is available from NOIE at: **www.noie.gov.au**.

THE ACA

The Australian Communications Authority is responsible for enforcing the provisions of the Spam Act.

Additional information about the Spam Act, and the ACA's role is available from: **www.aca.gov.au**.

*The ACA's enforcement role is discussed further in the section starting on **page 15**.*

THE SPAM ACT - WHAT DOES IT SAY?

SPAM PROHIBITED

The Spam Act says that *unsolicited commercial electronic messages* must not be sent.

Messages should only be sent to an address when it is known that the person responsible for that address has consented to receive it.

There is discussion of consent and what it means on **page 7**.

ADDRESS HARVESTING SOFTWARE, HARVESTED ADDRESS LISTS

Businesses must not use electronic *address harvesting software*, or lists which have been generated using such software, for the purpose of sending *unsolicited commercial electronic messages*.

There is a description of *address harvesting software* and harvested lists on **page 10**. The same section provides some guidance when using contact lists supplied by a third party.

RULES FOR SENDING COMMERCIAL ELECTRONIC MESSAGES

Commercial electronic messages must contain:

- Accurate information about the sender of the message;
- A functional way for the message's recipients to indicate that they do not wish to receive such messages in the future – that they wish to *unsubscribe*.

MESSAGES COVERED BY THE ACT

The Spam Act covers *commercial electronic messages* that are sent using applications such as:

- email;
- short message service (SMS);
- multimedia message service (MMS); and
- instant messaging (iM).

MESSAGES *NOT* COVERED BY THE ACT

The following examples are **not** covered by the Spam Act:

- Non-electronic messages (such as ordinary mail, paper flyers etc);
- Voice to voice telemarketing;
- The majority of "pop up" windows that appear on the internet (they are usually an intrinsic part of a webpage that has been accessed, rather than a message sent to the recipient address); and
- Messages without any commercial content that do not contain links or directions to a commercial website or location.

MESSAGES WITH AN AUSTRALIAN LINK

The provisions of the Spam Act cover *commercial electronic messages*:

- **originating in Australia** that are sent to any destination; and
- **originating overseas** that are sent to an address accessed in Australia.

FINANCIAL PENALTIES ASSOCIATED WITH A BREACH OF THE SPAM ACT

The maximum penalties under the Spam Act are substantial:

- A business that is found to be in breach of the Spam Act may be subject to a Court imposed penalty of up to $220,000 for a single day's contraventions. If, after that finding, the business contravenes the same provision, they may be subject to a penalty of up to $1.1 million.
- The Spam Act specifies a number of options that are available to enforce the legislation, depending on which is the most appropriate response to the contravention that has occurred. The range of possible activities includes formal warnings, infringement notices (similar to a speeding ticket), and court actions.

INDUSTRY CODES AND STANDARDS

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

3 STEPS TO FOLLOW

When reviewing your business practices, and the content of your commercial messages to ensure you comply with the Spam Act, you should consider the following three steps:

STEP 1 - CONSENT

Your commercial messages should only be sent when you have **consent**.

This may be **express consent** from the person you wish to contact – a direct indication that it is okay to send the message, or messages of that nature.

It is also possible to **infer consent** based on a business or other relationship with the person, and their conduct.

*The concept of consent is discussed further in the section starting on **page 7**.*

STEP 2 - IDENTIFY

Your commercial messages should always contain clear and accurate **identification** of who is responsible for sending the message, and how they can be contacted.

It is important for people to know who is contacting them, and how they can get in touch in return. This will generally be the organisation that authorises the sending of the message, rather than the name of the person who actually hits the "send" button.

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

*The concept of identification is discussed further in the section starting on **page 11**.*

STEP 3 - UNSUBSCRIBE

Your commercial messages should contain an **unsubscribe facility**, allowing people to indicate that such messages should not be sent to them in future.

All *commercial electronic messages* must contain a functional unsubscribe facility, allowing people to opt-out from receiving future messages. Such a request must be honoured.

The Spam Act specifies that the person's consent has been withdrawn within five working days from the date that the *unsubscribe* request was sent (in the case of electronic unsubscribe messages) or delivered (in the case of unsubscribe messages sent by post or other means).

Similar to the identification of the message's sender (step 2, above) the unsubscribe facility must be reasonably likely to remain accurate and functional for a 30 day period.

*The concept of the unsubscribe facility is discussed further in the section starting on **page 13**.*

1 – CONSENT

STEP 1 - CONSENT

Your commercial messages should only be sent when you have **consent**.

Only send *commercial electronic messages* with the addressee's consent - either express or inferred consent.

TYPES OF CONSENT

There are two forms of consent:

Express consent from the person you wish to contact – a direct indication that it is okay to send the message, or messages of that nature.

Inferred consent based on a business or other relationship with the person, and their conduct.

WHAT IS "EXPRESS CONSENT"?

You have received **express consent** from an addressee if that person has specifically requested messages from you. Examples of this include when:

- the addressee has subscribed to your electronic advertising mailing list;
- the addressee has deliberately ticked a box consenting to receive messages or advertisements from you; or
- the addressee has specifically requested such material from you over the telephone.

WHAT IS "INFERRED CONSENT"?

Consent may be inferred when the person you wish to contact has not directly instructed you to send them a message, but it is still clear that there is a reasonable expectation that messages will be sent.

You may be able to reasonably infer consent after considering both the conduct of the addressee and their relationship with you. For example, if the addressee has an existing relationship with you and has previously provided their address then it would be reasonable to infer that consent has been provided.

Other examples of where consent may be inferred are:

- when purchasing goods or services an addressee has provided their *electronic address* in the general expectation that there will be follow-up communications;
- when an addressee has provided their address with the understanding that it would be used in day-to-day transactions (such as online banking or business), and may be used for additional communications (for example notification of related services or products);
- online registration of a product or a warranty;

- when an addressee has *conspicuously published* their *electronic address*. In such a case the Spam Act permits commercial *electronic messages* to be sent to the addressee, if the message relates to the addressee's published employment function or role. If a plumber advertises their email address, it is okay to send them offers of work or of plumbing supplies, but not to send an offer unrelated to their work, such as cheap pharmaceuticals. If the published address is accompanied by a statement saying that it should not be used for such messages, such as the words "no spam", then it cannot be used to infer consent to a message being sent;
- similarly, when an addressee has provided a business card containing their *electronic address*, it would be a reasonable expectation on both sides that relevant messages would be sent to that *electronic address*. For example, if the business card was provided for work purposes then it would not be reasonable to infer that the addressee consented to receiving messages from you which are unrelated to their work.

WHAT IS AN "EXISTING RELATIONSHIP"?

It will be possible for you to infer consent based on the status of your relationship with the addressee, as long as it is consistent with the reasonable expectations of the addressee, and their conduct. The National Privacy Principles (available from **www.privacy.gov.au**), and particularly Privacy Principle 2, provides guidance on such communications. An existing business or other relationship may, for example, be a relationship that was initiated by a commercial activity (including provision, for a fee or free of charge, of information, goods, or of services) or other communication between you and potential addressee.

The following are examples that might suggest that a business, or other, relationship exists from which you may reasonably infer consent:

- persons who have purchased goods or services which involves ongoing warranty and service provisions;
- shareholders;
- magazine and newspaper subscribers;
- subscribers to a service;
- registered users of online services;
- utility or rate payers (i.e. in a business relationship with utility company/government body);
- subscribers to information/advisory services;
- financial members of a club;
- professional association members;
- members of frequent flyer or buyer clubs;
- bank account holders;
- superannuation subscriber;
- employers and employees; or
- contractors.

CIRCUMSTANCES WHEN AN "EXISTING RELATIONSHIP" CANNOT BE ASSUMED

Consent will not always be inferred where there is a pre-existing relationship between you and a person. For example, it would not be reasonable to infer that a person consented to receiving *commercial electronic messages* from you simply because of a transaction along the lines of any one-off purchase. Transactions such as the purchase of a t-shirt or groceries from a shop, attendance at a concert, performance or movie, would not be a good basis for inferring consent, or assuming that there is a pre-existing relationship.

THE PRIVACY ACT AND THE NATIONAL PRIVACY PRINCIPLES

The National Privacy Principles, available from **www.privacy.gov.au**, should always be followed by businesses when handling personal information, including customers' contact details. You should be aware of your obligations under the privacy legislation.

WHAT ABOUT MY OLD CONTACT LISTS?

Commercial electronic messages must only be sent with consent. It does not matter when the contact list was gathered, or how it has been used. You should be able to look at the addresses on your contact list and be certain that you have either express or inferred consent to contact each addressee.

When you are satisfied that your existing list of addressees have consented to receiving *commercial electronic messages*, you should ensure that the collection of future addresses is also based on consent. To do so, you may wish to consider amending any forms, letters or even invoices to seek consent from a person to send them *commercial electronic messages*.

WHAT IF I'M NOT SURE WHETHER CONSENT HAS BEEN GIVEN?

To remove any uncertainty about whether you have the consent of the potential addressee, you should seek confirmation from that addressee that you can send *commercial electronic messages* to them.

DOUBLE OPT-IN PROCESS

A 'double opt-in' process (sometimes also referred to as a 'closed-loop confirmation') can be used to validate that an addressee has consented to receiving *commercial electronic messages* and provides the evidence that you have the consent of the addressee.

The steps typically involved are:

1. Your business receives a message saying that an *electronic address* (email, SMS or similar) should be added to your contact list for commercial messages or company newsletters;
2. Your business sends a message to that address, requesting confirmation that messages should be sent there in future. The message also contains a notification that they will only be added to your contact list if they send a positive confirmation within 14 days.

3. After 14 days, there are 3 choices:
    - There has been a positive confirmation – the address is added to the contact list; or
    - There has been a negative response – the address is **not** added to the contact list for future messages
    - There has been no response – the address is **not** added to the contact list for future messages.

While not a legislated requirement, you are encouraged to consider implementing a double opt-in process, whether it is an automated system or a manual procedure, for instances where it is difficult to validate whether the potential addressee has actually consented. These instances can occur when dealing with online subscriptions, requests from third parties and other occasions where consent has not been given at the time of a personal communication or transaction.

CAN SOMEONE SUBSCRIBE ON ANOTHER PERSON'S BEHALF?

Sometimes you may receive a request from a person to send *commercial electronic messages* to another person. In this case the addressee themselves did not submit the request and as a result the consent requirements of the Act may not be met.

If you receive a request like this you should contact the addressee and seek confirmation of the request that was made and ensure that they consent to you sending *commercial electronic messages* to them.

When doing this it may be useful to provide information on whom requested the initial subscription on their behalf, or how the subscription request was submitted.

WHAT ABOUT ADDRESS-HARVESTING SOFTWARE?

Address-harvesting software and *harvested-address lists* are often used for legitimate purposes such as collecting data for research, marketing or maintaining websites; but they are also often used to create distribution lists for sending spam.

The legislation bans the use of *address-harvesting software* and *harvested-address lists*, for the purpose of sending spam. You should ensure that the use of such software and lists are for purposes other than for sending *unsolicited commercial electronic messages*.

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

CAN I USE PURCHASED CONTACT LISTS?

You may use a purchased or rented list of contacts, but you should be careful to ensure that the requirements of the Spam Act have been met (i.e. consent has been obtained).

2 – IDENTIFY

STEP 2 - IDENTIFY

People who receive your commercial messages should be able to read them and know who you are, and how to get in contact with you. This means including accurate sender details and contact information.

Include clear and accurate information about the person or business that is responsible for sending the *commercial electronic message*.

WHAT IDENTIFICATION DO I NEED TO PROVIDE?

To comply with the Spam Act you should ensure that accurate information identifying your business is provided in all *commercial electronic messages* you have authorised to be sent. This information should include details that clearly identify your business (for example the business name) and details about how the addressee may contact you.

This may be as simple as amending templates that are used for electronic letters, quotes, invoices and other messages that are sent to existing and potential customers.

HOW ABOUT WHEN I'M USING A THIRD PARTY TO SEND THE MESSAGE?

Sometimes you might use another organisation, a third party, to send *commercial electronic messages* on your behalf. This third party must include accurate information about your business, for example; name, address and contact details.

When instructing the third party to send messages on your behalf you should ensure that you provide your sender information and authorise its inclusion in messages to be sent.

The Spam Act does not require the third party's information to be included in the message – you may decide whether it would be appropriate or not.

WHAT IF THERE ARE LIMITATIONS ON THE AMOUNT OF INFORMATION I AM ABLE TO SEND?

The content of electronic messages may depend on the size and capacity of different technologies.

For example, more information is able to be sent by email than by SMS. In most cases it is unlikely that detailed sender information and detailed unsubscribe information will be able to be provided in an SMS message.

In these circumstances, your sender information might be brief (for example, your business name and contact number). You might also include an additional link to more information about your business (a free information number or an internet address).

FOR HOW LONG MUST THIS INFORMATION REMAIN ACCURATE?

Sender information must be reasonably likely to be accurate for a period of 30 days after the day on which you send your message. This requirement ensures that addressees have a reasonable chance of being able to contact you.

If you are planning on changing premises within that period, you could include postal information and phone contacts for both addresses, and the date when the transfer will occur, or, alternatively, you could make arrangements for communications that go to the old premises to be re-directed to your new premises for a period of time.

3 – UNSUBSCRIBE

STEP 3 - UNSUBSCRIBE

You need to provide people the choice to opt out, or *unsubscribe*, from your future *commercial electronic messages*. It needs to be a clearly presented and easy to use.

Ensure that a functional unsubscribe facility is included in all your *commercial electronic messages*. Deal with *unsubscribe* requests promptly.

WHAT FORM SHOULD THE UNSUBSCRIBE FACILITY TAKE?

An unsubscribe facility is basically an *electronic address* that messages can be sent to, and a clear, conspicuous statement that the address can be used to opt out from future messages. The form it takes can vary, as long as these basic requirements are met.

In relation to email messages, this could be in the form of a link that creates an automatically addressed email to be sent in reply. Alternatively, a link could take the addressee to your website where they can fill in their details and send them to you. An accompanying note along the lines of "Click here to unsubscribe" would satisfy the requirement. Alternatively, a message saying "If you wish to opt out from future messages, send a reply email with the subject UNSUBSCRIBE" is commonly used.

In relation to SMS, the facility might provide a number that addressees can SMS their request to unsubscribe, or alternatively, provide an email address for the person to contact with their opt out request.

You might also consider providing additional ways for addressees to *unsubscribe*. Alternatives might include acceptance of requests through telephone calls to your existing business number. Otherwise, you could use a dedicated line such as a 1800 number, accepting requests by facsimile or through your business email address.

FOR HOW LONG MUST THE UNSUBSCRIBE FACILITY REMAIN WORKING?

In terms of the Act, the unsubscribe facility must be reasonably likely to be functional for a period of 30 days after the day on which your message was sent. You should, however, endeavour to have a permanent facility available to addressees.

HOW QUICKLY MUST I ACTION REQUESTS TO UNSUBSCRIBE?

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

Any *commercial electronic message* sent after this five day period contrary to an unsubscribe request may be considered to be in breach of the legislation.

You are strongly encouraged to ensure that your unsubscribe facilities and business processes are set up to support this requirement. Options for doing this could be:

- Setting up a same-day *unsubscribe* regime, so that opt-out requests have a 24 hour turn around; or
- Change your process for sending out electronic messages so that the addresses that have unsubscribed are always removed from your contact list, just before any messages are sent.

You also should consider keeping unsubscribe requests for a specified period in order to check addresses against future message mailouts.

THE AUSTRALIAN COMMUNICATIONS AUTHORITY - THE SPAM ACT'S "WATCHDOG"

THE ACA

The ACA is responsible for regulating telecommunications and radiocommunications, including licensing, spectrum management, compliance with codes and standards, performance monitoring and consumer safeguards.

The Australian Communications Authority is responsible for enforcing the provisions of the Spam Act.

INDUSTRY CODES AND STANDARDS

Industry codes of practice are likely to be developed by industry organisations such as the ADMA and the IIA. The codes will aim to provide relevant and achievable standards and procedures developed by groups representing industry sectors for their member organisations, to assist compliance with the Act. These codes are likely to be presented to the ACA for registration.

ENFORCEMENT OF THE SPAM ACT

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

In addition to working on industry codes and standards, the Spam Act gives the ACA the ability to pursue a number of options in enforcing the legislation.

FORMAL WARNINGS

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

INFRINGEMENT NOTICES

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

COURT ACTIONS

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

INTERNATIONAL LAWS

COVERAGE OF AUSTRALIA'S SPAM ACT

The legislation is intended to prohibit:

- spam **originating in Australia** being sent to any destination;
- spam **originating overseas** being sent to an address accessed in Australia.

Enforcement of the penalties relating to overseas sourced spam will be problematic until international arrangements are in place. Australia is actively seeking partnerships with other countries and organisations in the fight against spam.

The legislation ensures that there is an appropriate enforcement regime in place to deal with overseas spammers as soon as international arrangements are in place. The Spam Act includes provisions that anticipate Australia's entry into such arrangements with other countries concerned about spam. This will enable regulations to be made giving effect to these agreements once in place.

OTHER COUNTRIES' LAWS

Australia's legislation is currently one of the world's best examples of an anti-spam legislative regime. The number of countries that have passed, or are considering passing, national legislation against spam is growing. Often the requirements of these laws vary subtly from country to country, and if you are planning to send *commercial electronic messages* to addressees outside of Australia, you should find out about the specific requirements of their anti-spam laws.

MORE INFORMATION

CHECK YOUR ISP'S POLICIES

It should be noted that many businesses may have existing agreements with their Internet Service Providers (ISPs) on "Acceptable Use Policies" (AUPs) which specify a higher level of consent than is provided for in the spam legislation. For example, they may require express consent or require the use of double opt-in methodologies for confirming consent. They do this to protect their business reputation and to avoid problems with spam blocking groups on the Internet. The spam legislation does not overrule cases where a higher standard is required in an AUP. Businesses should pay close attention to their AUPs to avoid difficulties with their ISP.

THE PRIVACY ACT 1998, AND THE NATIONAL PRIVACY PRINCIPLES (NPP)

The Office of the Federal Privacy Commissioner, **www.privacy.gov.au**, provides a comprehensive range of information on the requirements of the Privacy Act, and on the National Privacy Principles.

In addition to the requirements of the Spam Act, you should always be in compliance with the provisions of the National Privacy Principles.

OTHER SOURCES OF INFORMATION

Additional information in relation to the Spam Act and preventative measures is available from the ACA and NOIE websites located at the following addresses: **www.aca.gov.au** and **www.noie.gov.au**.

LINKS

Many industry organisations also offer advice about the Spam Act and about spam in general. This information can be found from the following website addresses:

- Australian Direct Marketing Association (ADMA) **www.adma.com.au/asp/index.asp**;
- Coalition against Unsolicited Bulk Email (CAUBE) **www.caube.org.au**;
- Internet Industry Association (IIA) **www.iia.net.au**;
- Internet Society of Australia (ISOC) **www.isoc-au.org.au**;
- Public Relations Institute of Australia (PRIA) **www.pria.com.au/home.php**;
- Small Enterprise Telecommunications Centre (SETEL) **www.setel.com.au**; and
- Presidian Legal Publications **www.presidian.com.au**.

GLOSSARY OF TERMS

Additional definitions can be found in the *Spam Act 2003* and its accompanying *Explanatory Memorandum*. Both are available from **http://scaleplus.law.gov.au/**.

120 -DAY GRACE PERIOD

Time between Royal Assent (enactment) and penalty provisions of the Act coming into force.

This provision was designed to allow time for the review of business practices to ensure conformity with the Act.

ACA

Australian Communications Authority

ACCOUNT-HOLDER

The person responsible for the *electronic address*. When an organisation provides email addresses for its employees, both the organisation and the employee may consent to messages being sent to that address.

ADDRESS-HARVESTING SOFTWARE

Address-harvesting software is a computer program that is designed to automatically collect *electronic addresses* from the Internet. The software searches public areas such as from web pages, newsgroups, chat rooms and other online directories to compile or 'harvest' lists of addresses.

ADMA

Australian Direct Marketing Association

COMMERCIAL ELECTRONIC MESSAGE

An electronic message, for example an email or a text message, for example, that offers or advertises the supply of goods or services, land, business or investment opportunity.

For more information please see the fact sheet on commercial electronic messages.

CONSPICUOUS PUBLICATION

Prominent display of an address to which electronic messages can be sent

ELECTRONIC ADDRESS

The means for contacting a particular person through a communications medium. So, an email address for emails, telephone number for mobile phone messaging, and user identity number for instant messaging.

ENFORCEABLE UNDERTAKING

Where an organisation submits a formal commitment that certain behaviour or activities will be done or will not be done.

HARVESTED-ADDRESS LISTS

A *harvested-address list* is a collection of electronic addresses that has been compiled through the use of *address-harvesting software* often without the consent or knowledge of the addressee. The use of these types of software or address lists is only prohibited if the purpose of their use is to send *unsolicited commercial electronic messages*.

IIA

Internet Industry Association

INJUNCTION

A court based order requiring a person to do or stop doing something.

PENALTY AMOUNTS

The amount of monies fined.

UNSOLICITED COMMERCIAL ELECTRONIC MESSAGE

An electronic message, for example, an email or a mobile phone text message, that is commercial in nature and has not been consented to.

UNSUBSCRIBE

To cause an address to be removed from a mailing or distribution list.


SPAM

OVERVIEW - THE 3 STEPS TO FOLLOW

When reviewing your business practices, and the contents of your commercial electronic messages for compliance with the Spam Act, there are three key elements you should consider:

1 – CONSENT

Only send commercial electronic messages with the addressee's consent – either express or inferred consent.

2 – IDENTIFY

Include clear and accurate information about the person or business that is responsible for sending the commercial electronic message.

3 – UNSUBSCRIBE

Ensure that a functional unsubscribe facility is included in all your commercial electronic messages.

Deal with unsubscribe requests promptly.