Australian Government

Department of Communications,
Information Technology and the Arts

Australian Communications Authority

Spam Act 2003:
A practical guide for government

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.

TABLE OF CONTENTS

SENDING ELECTRONIC MESSAGES – THE MAIN POINTS

INTRODUCTION

Every government body, whether operating at the local, state or federal level, needs to ensure that their communication practices comply with the provisions of the Spam Act and with the privacy requirements of their respective jurisdictions.

WHEN THE SPAM ACT APPLIES

The Spam Act aims to reduce unsolicited commercial electronic messages, but also sets new standards for legitimate electronic messages that have a commercial purpose.

If a message sent by email, SMS or other electronic media has a commercial purpose, then the Spam Act defines it as a "commercial electronic message" and states that it must satisfy the following three requirements:

1. **Consent** — it is sent with the express or inferred consent of the addressee;
2. **Identify** — the electronic message contains clear and accurate identification of the sender; and
3. **Unsubscribe** — the electronic message contains a functional unsubscribe facility to allow the addressee to opt out from future electronic messages.

*These requirements are discussed further on **page 4**.*

WHAT IS A COMMERCIAL ELECTRONIC MESSAGE?

The definition of a commercial electronic message under the Spam Act is very broad and includes an electronic message that offers or advertises the supply of goods or services, land, business or investment opportunities.

An electronic message is classified as commercial by examining the content of the message, the way in which the message is presented and the content that can be located using the links, telephone numbers or contacts in the message. For example, even if an electronic message itself does not have a commercial purpose, but provides a link to a web page that does have a commercial purpose, then it may be considered a commercial electronic message for the purposes of the Spam Act.

This definition could potentially include some government activities and services. For example, offers for grants, or services delivered on a fee-for-service basis. It should not be assumed that because a government body is non-commercial, all electronic messages it sends will also be considered non-commercial.

LIMITED EXEMPTION

To ensure that the Spam Act does not unintentionally restrict communication between government and the community, certain electronic messages authorised by government bodies are exempt from some requirements that would normally apply to commercial electronic messages. These messages, known as "designated commercial electronic messages" must include accurate sender information, but are not required to include an unsubscribe facility or to be sent with the consent of the addressee.

It is important to note the following:

- not all government electronic messages fall within this exemption. The message in question must satisfy particular requirements before it can be classified as a designated commercial electronic message;
- these provisions are safety net provisions and should not be relied on routinely;
- government bodies should always aim to meet or exceed the same high standards required of the private sector under the Spam Act; and
- government bodies that are commercialised or operating in an environment where they compete with the private sector (competitive environment) should not rely on the exemption provisions when sending commercial electronic messages.

*These provisions and requirements are discussed further on **page 12**.*

MESSAGES *NOT* COVERED BY THE SPAM ACT

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

- non-electronic messages (such as ordinary mail, paper fliers etc);
- voice-to-voice telemarketing;
- information posted on Internet pages;
- 'pop up' windows that appear on the Internet (they are usually an intrinsic part of a webpage that has been accessed, rather than an electronic message sent to an addressee); and
- electronic messages without any commercial purpose that do not contain links or directions to a website or location having a commercial purpose.

PRIVACY REQUIREMENTS

All government electronic messages, whether having a commercial purpose or not, must comply with the privacy requirements of their jurisdiction.

*These requirements are discussed further on **page 15**.*

THE SPAM ACT: 3 STEPS TO FOLLOW

When reviewing your business practices and the content of your commercial electronic messages to ensure you comply with the Spam Act, there are three key elements you should consider. Potential exemptions are discussed on page 12.

STEP 1 - CONSENT

Your commercial electronic 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 electronic 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 5**.*

STEP 2 - IDENTIFY

Your commercial electronic messages must always clearly and accurately identify who is responsible for authorising the sending of the message and how they can be contacted.

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

*The concept of identification is discussed further in the section starting on **page 8**.*

STEP 3 - UNSUBSCRIBE

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

After a person indicates that they wish to unsubscribe, you have 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) to honour their request.

Similar to the identification of the electronic 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 10**.*

THE SPAM ACT: CONSENT

STEP 1 - CONSENT

Your government body's commercial electronic messages should be sent with the addressee's consent - either express or inferred.

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 electronic message or messages of that nature; and
- **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 electronic 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 electronic messages or advertisements from you; or
- the addressee has specifically requested material from you over the telephone or through other media.

WHAT IS "INFERRED CONSENT"?

Consent may be inferred when the person you wish to contact has not directly instructed you to send them an electronic message, but it is still clear that there is a reasonable expectation that electronic 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 as part of that relationship has previously provided their electronic address then it would be reasonable to infer that consent has been provided.

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.

Both the Information Privacy Principles and the National Privacy Principles, which can be found at **www.privacy.gov.au**, provide guidance on inferred consent and relationship status that is relevant both for the private and the public sector.

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

- superannuation subscriber;
- employers and employees/contractors;
- utility or rate payers;
- magazine and newspaper subscribers;
- registered users or subscribers to a service;
- subscribers to information/advisory services; and
- professional association members.

WHAT IS NOT AN "EXISTING RELATIONSHIP"

Consent will not always be inferred where there is a pre-existing relationship. Transactions such as the purchase of a publication or service, attendance at a function, conference, or performance alone are unlikely to be a sound basis for inferring consent or assuming that there is a pre-existing relationship.

WHAT ABOUT MY OLD CONTACT LISTS?

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

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 amend forms, letters or invoices to seek consent from a person to send them commercial electronic messages.

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 government body receives a message saying that an electronic address (email, SMS or similar) should be added to your contact list for commercial electronic messages;
2. your government body sends an electronic message to that address, requesting confirmation that electronic messages should be sent there in future. The electronic message also contains a notification that they will only be added to your contact list if they send a confirmation within a set period, say 14 days; and

3. after 14 days, there are two possible outcomes:
    - confirmation received – the electronic address is added to the contact list; or
    - there has been a negative response or no response – the electronic address is not added to the contact list for future electronic 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 when 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 third party to send commercial electronic messages to an addressee. In this case the addressee has not directly submitted the request and as a result the consent requirements of the Spam 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.

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. They are also often used to create distribution lists for sending spam.

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

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).

THE SPAM ACT: IDENTIFY

STEP 2 – IDENTIFY

Addressees who receive your commercial electronic 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.

Sender details and contact information must relate to the individual or government body that authorises the sending of the electronic message rather than the individual or organisation that actually sends the information on behalf of a government body. If an individual authorises the sending of an electronic message on behalf of a government body, the government body is taken to have authorised the electronic message.

Clear and accurate information must be included about the person or government body that is responsible for authorising the sending of 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 government body is provided in all commercial electronic messages authorised by that government body. This information should include details that clearly identify your government body (for example the government body 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 electronic messages that are sent to existing and potential customers.

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

Sometimes a government body might use another organisation to send commercial electronic messages on its behalf. This third party must include accurate information about the government body that authorised the sending of the message. For example, its name, address and contact details.

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

The Spam Act does not require the third party's information to be included in the electronic 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 can 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 government body name and contact number). You might also include an additional link to more information about your government body (for example, 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 electronic message. This requirement ensures that addressees have a reasonable chance of being able to contact you.

THE SPAM ACT: UNSUBSCRIBE

STEP 3 – UNSUBSCRIBE

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

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 enables an addressee to opt out from future commercial electronic messages. It must be a clear, conspicuous statement supported by a functional electronic address that an addressee may use to send an unsubscribe message to the individual or government body who authorised the commercial electronic message. The electronic address must be reasonably likely to be capable of receiving unsubscribe messages for a period of at least 30 days from the date that an unsolicited commercial electronic message is sent. This feature need not be an automated process and 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 feature might provide a number that addressees can SMS their request to unsubscribe or, alternatively, to provide an email address for the addressee to contact with their opt out request.

An unsubscribe facility is not the only means by which an addressee can withdraw their consent. Alternatives might include telephone calls to your existing business number, requests by facsimile or through your government body's email address.

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 five working days from the date on which the request was sent (for electronic unsubscribe requests), or delivered (for 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 Spam Act.

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 less than 5-day turn around; or
- changing your process for sending out electronic messages so that the electronic addresses of addressees that have unsubscribed are always removed from your contact list, just before any subsequent electronic messages are sent.

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

THE SPAM ACT: A LIMITED EXEMPTION

INTRODUCTION

To prevent any unintended restriction on communication between government and the community the Spam Act includes a limited exemption for some commercial electronic messages authorised by government bodies.

WHAT IS A DESIGNATED COMMERCIAL ELECTRONIC MESSAGE?

The Spam Act uses the term *designated commercial electronic messages* to indicate those electronic messages that have a limited exemption from the main provisions of the legislation. An electronic message authorised to be sent by a government body is a designated commercial electronic message if:

- that message relates to goods or services and the government body is the supplier or prospective supplier of those goods or services; or
- it is a factual message, as described below.

It should be noted that:

- the electronic message does not have to be sent by the government body. For example it may be sent by a third party under the authorisation of a government body; and
- not all commercial electronic messages sent by government bodies will fall within the exemption.

If an electronic message is a *designated commercial electronic message*, then it may be sent without the addressee's consent and without an unsubscribe facility. However, the electronic message must contain accurate sender information and, as always, must comply with the privacy requirements of the jurisdiction.

FACTUAL MESSAGE

Under the Spam Act, electronic messages that contain no more than factual information and certain specified additional information are designated commercial electronic messages.

Many government bodies use newsletters or updates as a means of distributing information among sections of the general or business community. Examples of this include:

- an electronic version of a neighbourhood watch newsletter that is sponsored by a local business establishment;
- a recall notice on a product for safety reasons;
- an update on current arrangements for a government program; and,
- advice on entitlements for citizens or community groups.

Even though these electronic messages may have a commercial element, it is recognised that their primary purpose is to provide news, summaries or updates rather than to offer, advertise or promote goods, services, land, business or investment opportunities. Electronic messages of this nature are *designated commercial electronic messages*.

WHAT IS A GOVERNMENT BODY?

The Spam Act includes in its definition of a "government body" any department, agency, authority or instrumentality of the Commonwealth, the states, territories or local government.

WHAT COULD BE GOODS, SERVICES FROM GOVERNMENT?

The terms 'goods' and 'services' are defined in the Spam Act.

In the government context, examples of goods and services provided by government are very broad and could potentially include such diverse items as:

- trees, shrubs and plants from a government nursery;
- maps, videos and publications from a government bookshop;
- training materials and plans from a government educational body; and
- noxious weed eradication activities on fee-for-service basis.

Activities such as government grant programs may also fall within the scope of "services". It is recommended that government bodies use caution and assume that the exemptions do not apply to messages relating to such activities.

In many of the circumstances described above a government body may be commercialised or operating in a competitive environment. In these circumstances it is important that government is not perceived as having undue advantage. It is strongly recommended that you do not rely on the exemptions that apply to government bodies when sending commercial electronic messages. You should aim for best practice by ensuring you fully meet, or exceed, the requirements of the Spam Act. You must also comply with the relevant privacy legislation and requirements.

WHEN MAY THE EXEMPTION BE USED?

The evaluation of whether the exemption applies to an electronic message needs to be undertaken on a case by case basis taking into account both legal requirements and policy considerations. The legal requirements that apply are whether:

- the message is being sent through an electronic medium and has a commercial purpose (otherwise the Spam Act does not apply); and
- the electronic message is either factual, as described on page 12, or relates to goods or services that are, or will be supplied by the government body authorising the message.

The policy considerations that apply are whether:

- the message is essential to the work of government and
- there is no practical alternate way of complying with the consent requirements of the Spam Act.

If your government body is commercialised or operates in a competitive environment – it is strongly recommended that you do not rely on the exemptions that apply to government bodies when sending commercial electronic messages. You should aim for best practice by ensuring you fully meet, or exceed, the requirements of the Spam Act. You must also comply with the relevant privacy legislation and requirements.

If you are not commercialised or operating in a competitive environment, and you need to send some commercial electronic messages – you should still exercise your judgment and only rely on the exemptions that apply to government bodies if it is impractical to comply with the consent requirements of the Spam Act. You should aim for best practice by endeavouring to fully meet, or exceed, the requirements of the Spam Act. You must also comply with the relevant privacy legislation and requirements.

PRIVACY LEGISLATION

PRIVACY LEGISLATION

Although the Spam Act makes no specific reference to privacy legislation, it is intended to closely complement existing state and Commonwealth privacy policy. All Commonwealth, state and local government bodies need to ensure that their electronic communication practices comply with both the Spam Act, and the relevant privacy acts, codes of practice, or privacy principles applicable within their respective state or territory.

THE COMMONWEALTH AND THE A.C.T.

The Office for the Federal Privacy Commissioner provides a comprehensive range of information on the requirements of the *Privacy Act 1988* (Cth), and on the Information Privacy Principles that apply to Commonwealth and Australian Capital Territory government bodies.

www.privacy.gov.au

NEW SOUTH WALES

Privacy NSW is the Office of the New South Wales Privacy Commissioner. Their role includes provision of information and assistance to New South Wales government bodies to help them comply with their obligations under the *Privacy and Personal Information Protection Act 1998* (NSW).

www.lawlink.nsw.gov.au/pc.nsf/pages/index

NORTHERN TERRITORY

In the Northern Territory, an Information Act that covers the protection of personal information, record keeping and archive management of information held in the public sector was passed in October 2002. The *Information Act 2002* (NT), incorporates freedom of information, privacy principles and record and archive management.

www.nt.gov.au/dcm/parliamentary_counsel/current_legislation.shtml

Health Information Privacy provides information and links to health privacy related matters in the Territory including a Code of Conduct.

www.nt.gov.au/health/org_supp/legal/privacy/health_privacy.shtml

QUEENSLAND

A privacy scheme applies to Queensland State government bodies and most statutory government-owned corporations. The regime is based on the Federal Privacy Commissioner's Information Privacy Principles and includes an Information Standard and Privacy Guidelines. Further information can be obtained from the Queensland Department of Innovation and Information Economy website.

www.iie.qld.gov.au/informationstandards/current.asp

SOUTH AUSTRALIA

South Australia has issued an administrative instruction requiring its government bodies to generally comply with a set of Information Privacy Principles (SA).

South Australia also has a Code of Fair Information Practice, based on the National Privacy Principles. This Code applies to all personal information including health information handled by the South Australian Department of Human Services and its agencies that deal with health, housing and community areas.

www.dhs.sa.gov.au/finalcodeDec01.pdf

TASMANIA

In 1997 Tasmania issued Information Privacy Principles based on Federal legislation and recommended the principles to Tasmanian Government bodies. Privacy legislation for the public sector is in development.

www.go.tas.gov.au/standards/privacy/privacy.htm

VICTORIA

The Victorian *Information Privacy Act 2000* covers all personal information except health information in the public sector in Victoria. The Office of the Victorian Privacy Commissioner has more information.

www.privacy.vic.gov.au/dir100/priweb.nsf

WESTERN AUSTRALIA

The state public sector in Western Australia does not currently have a legislative privacy regime. Various confidentiality provisions cover government bodies and some of the privacy principles are covered in the Freedom of Information legislation.

http://www.foi.wa.gov.au/

THE AUSTRALIAN COMMUNICATIONS AUTHORITY (ACA) AND SPAM

THE ACA

The ACA is responsible for enforcing the provisions of the Spam Act. In this role the ACA is working closely with a range of other enforcement agencies both nationally and internationally, as well as relevant industry bodies and providers.

Under section 109 of the *Telecommunications Act 1997*, persons including government bodies can refer spam complaints to the ACA for investigation.

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 itself may be illegal under other laws - for example, it may be fraudulent, offensive or carry a computer virus. 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 Spam Act, 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 Spam Act. 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 damage from someone else contravening the Spam Act, or the ACA on their behalf, may apply to the court to make an order for compensation.

MORE INFORMATION

DCITA

The Department of Communications, Information Technology and the Arts (DCITA) is responsible for raising awareness and providing information about the Spam Act during its implementation.

Additional material about the Spam Act is available from DCITA at:
www.dcita.gov.au/spam

THE ACA

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

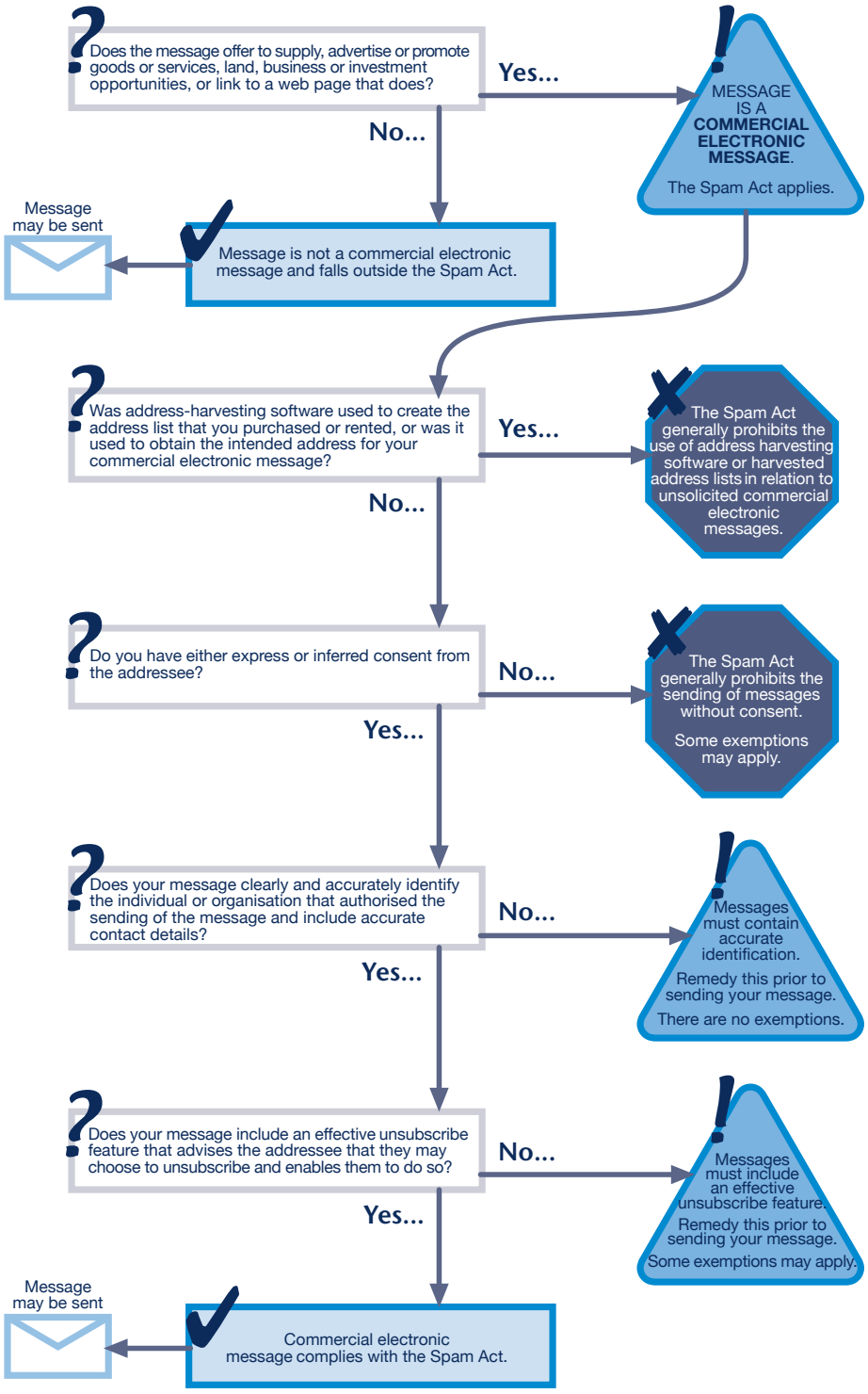
Additional information about the Spam Act, and the ACA's role is available from:
www.aca.gov.au

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**.

WHAT DO I NEED TO CONSIDER BEFORE SENDING A COMMERCIAL ELECTRONIC MESSAGE?




consent


email from@address.com
identify


unsubscribe
unsubscribe

This guide provides practical information to government bodies on how their communications practices may be affected by the requirements of the *Spam Act 2003* (Cth) (the Spam Act). The Spam Act became fully effective on 10 April 2004. For the purposes of the Spam Act a "government body" is any department, agency, authority or instrumentality of the Commonwealth the States, Territories and local government.

The Spam Act applies to commercial electronic messages, including those authorised by government bodies to be sent. Government bodies will need to be aware of when their electronic messages are commercial electronic messages. Examples include electronic messages that offer or advertise the supply of goods or services, land, business or investment opportunities. This guide provides information on how to identify whether an electronic message is commercial and what attributes the electronic message should possess in order to comply with the Spam Act.

The Spam Act states that certain types of electronic messages from government bodies do not have to meet all of the requirements imposed on commercial electronic messages. This guide outlines the nature of these messages and provides guidance on when this limited exemption may apply.

The Spam Act enables addressees that receive unsolicited commercial electronic messages to refer complaints to the Australian Communications Authority (ACA) for investigation.

Spam Act 2003: A practical guide for government, April 2004
ISBN (Print): 0 642 75175 7
ISBN (Online): 0 642 75181 1

Disclaimer

Please note:

This guide has been prepared by the Department of Communications, Information Technology and the Arts (DCITA) to provide information to Australian government bodies 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.


SPAM