Australian Government
Office of the Privacy Commissioner

PRIVATE SECTOR INFORMATION SHEET 26 – *Interaction between the Privacy Act and the Spam Act*

Key Messages

Introduction

The Spam Act prohibits sending unsolicited commercial electronic messages ('spam'). The Act's coverage includes emails, instant messaging, SMS and MMS (text and image-based mobile phone messaging) of a commercial nature.

The Spam Act applies to any commercial electronic message with an Australian link, regardless of the size of the business that sent the message. This includes emails sent to anonymous email addresses, where the identity of the individual cannot be reasonably ascertained. The Spam Act partially exempts messages that contain purely factual material.

The Privacy Act may also regulate such activity where it involves the use of 'personal information' by private sector organisations that fall within its jurisdiction. Information is only 'personal information' if the organisation can identify or reasonably ascertain the identity of the individual to which it relates.

Depending on what other information is held, an anonymous email address may or may not be 'personal information' under the Privacy Act. If electronic direct marketing is sent without the use of personal information, then the Privacy Act would not apply.

Where both the Spam Act and the Privacy Act apply, both sets of obligations need to be met.

Key requirements of the Spam Act

The Spam Act requires that commercial electronic messages, except where designated as 'exempt', meet three conditions. They must:

- be sent with the consent of the recipient
- identify the sender
- include a functional unsubscribe mechanism.

Even where messages are 'exempt', they must still identity the sender.

Key requirements of the Privacy Act

All organisations covered by the Privacy Act must comply with the 'National Privacy Principles' when handling individuals' personal information. These principles cover how personal information is collected, stored, used, disclosed and destroyed, and give individuals the right to access that information.

How does the Privacy Act apply to messages exempt from the Spam Act?

If a commercial electronic message is exempt or partially exempt from the Spam Act, then that Act does not require the sender to obtain consent from the recipient or provide an unsubscribe mechanism.

However, if the sender is covered by the National Privacy Principles, any personal information must be handled in a way that complies with the Privacy Act. This will usually mean that these messages may only be sent where the use of the personal information for electronic direct marketing is:

- the primary or main reason why the information was originally collected or
- related to why it was originally collected (or directly related, if it is sensitive information), and that use falls within the recipient's reasonable expectations or
- is with the individual's express or implied consent.

Background

What is this information sheet about?

This information sheet explains:

- Areas of overlap between the *Privacy Act 1988* ('Privacy Act') and the *Spam Act 2003* ('Spam Act').

  However, it does not provide detailed guidance on all aspects of the Spam Act. If you wish to send commercial electronic messages, you should refer to guidance material prepared by the Australian Communications and Media Authority (ACMA) – see, www.spam.acma.gov.au.

- How the Privacy Act applies to the handling of personal information for the purpose of electronic direct marketing.

  This includes marketing by email and existing or emerging forms of mobile wireless technology, including short message service (SMS), multimedia message service (MMS), wireless access protocol (WAP) and third generation technology (3G).

This information sheet does not cover direct marketing through postal mail, faxes, internet pop-ups or voice telemarketing.

Who is this information sheet for?

Organisations that conduct electronic direct marketing by email, SMS, instant messaging or other wireless technologies, and contractors that perform such practices on behalf of other organisations, may find this information sheet helpful.

This information sheet is not intended for Commonwealth Government bodies (except to the extent that they have commercial operations), or State and Territory government agencies.[1]

[1] The use of personal information by Commonwealth and ACT agencies to send electronic communications will generally be covered by Information Privacy Principle 10 of the Privacy Act and may be covered by aspects of the Spam Act, particularly where they offer goods or services in competition with the private sector. More information on how government agencies are covered by the Spam Act may be obtained from ACMA at www.spam.acma.gov.au.

What is Spam?

Neither the Spam Act or the Privacy Act define the term 'spam.'

ACMA explains that unsolicited commercial electronic messages are 'spam'. Section 6 of the Spam Act defines the term 'commercial electronic message' as an electronic message which, having regard to the message's content and presentation, offers, advertises or promotes goods, services, land, or business and investment opportunities.

Commercial electronic messages also include electronic messages that enable a person to dishonestly obtain property, financial advantage or gain from another person by deception.

The Spam Act applies to commercial electronic messages with an 'Australian link.' A commercial electronic message has an Australian link if it originates or was commissioned in Australia, or originated overseas but was sent to an address accessed in Australia.[2]

To avoid being viewed as 'spam', all commercial electronic messages must meet the following conditions:

- consent – the message must be sent with the recipient's consent. The recipient may give express consent, or under certain circumstances consent may be inferred from their conduct or an existing business or other relationship
- identify – the message must contain accurate information about the person or organisation that authorised the sending of the message and how to contact them
- unsubscribe – the message must contain a functional unsubscribe facility to allow the recipient to opt-out of receiving messages from that source in the future. The unsubscribe request must be honoured within five working days.[3]

If a message does not meet these three requirements, and is not designated as exempt under the Spam Act, then it can be considered spam and is unlawful. The penalty for sending spam is up to $1.1 million per day and the Federal Court may issue orders regarding the payment of compensation.

[2] The full definition is contained in section 7 of the Spam Act.

[3] See "How does it work" available from www.spam.acma.gov.au.

The Privacy Act and Spam Act have different purposes

The Spam Act generally prohibits the sending of 'spam', regardless of who the recipient is or whose information is used, so long as there is an 'Australian link'.

In contrast, the Privacy Act provides protection for the handling of an individual's personal information. It is not intended to protect the privacy of businesses or other types of organisations.

The handling of business to business information will not be covered by the Privacy Act, unless that information includes 'personal information'.

What is 'personal information'?

An organisation covered by the Privacy Act, will need to consider whether any data it handles, including to send commercial electronic messages, is 'personal information.'

'Personal information' is defined in section 6 of the Privacy Act as information or opinion, whether true or not, about an individual whose identity is apparent or can be reasonably ascertained from that information.

Some kinds of information, such as an email address or mobile phone number, will not always be 'personal information.'

Organisations should consider whether they can reasonably ascertain the identity of the individual concerned from the information that is available to them. Identity could be determined, for example, by linking an individual's email address or phone number with other identifying information held by the organisation.

Example: An email as personal information

Bob establishes an email account at hotmail.com and chooses a meaningless pseudonym as the username and first element of the email address. It is not possible to reasonably ascertain Bob's identity by the email address alone.

Bob gives his email address to a large electronics retailer so that he can receive regular email newsletters on new products. He does not provide any other information.

Bob also gives the email address to his phone company so he can receive electronic billing and other notices. The phone company also has other personal information about Bob, including his full name, address, phone numbers and date of birth.

Because the electronics store only has Bob's pseudonym, it cannot reasonably ascertain Bob's identity. How the store handles Bob's email address is not covered by the NPPs because the address, in this context, is not personal information. However, the retailer will still be bound by Spam Act obligations if it sends Bob a commercial electronic message.

In contrast, the phone company could reasonably link the email address to other information which it holds about Bob. In this case, Bob's email address would be personal information and the phone company would have to handle it in accordance with the NPPs.

The phone company would also have to comply with the Spam Act when sending Bob any commercial electronic messages.

Coverage and application of the Privacy Act and Spam Act

What does the Privacy Act cover?

The Privacy Act sets out 10 National Privacy Principles (or 'NPPs') that apply to how 'organisations' must handle 'personal information'.

'Organisations' are defined in section 6 of the Privacy Act to include:

- all businesses that are not small businesses: that is, businesses with an annual turnover greater than $3 million
- all private sector health service providers, regardless of turnover
- small businesses that trade in personal information without consent - for example, a small business will be covered by the Privacy Act if its primary business is compiling, buying or selling mailing lists of personal information for the purpose of direct marketing
- any other small business prescribed in regulations, such as residential tenancy databases.

For these 'organisations', the handling of personal information is regulated by the NPPs.

Data that is used for electronic direct marketing need not always be 'personal information'. If it is not, then the Privacy Act will not apply to the

handling of that data. This is explained further above, under '*What is 'personal information'?*

Particular practices of political parties and media organisations are also exempt from the NPPs. However, the latter are only exempt in regard to practices conducted "in the course of journalism". For example, a newspaper publisher using personal information to solicit subscriptions would be covered by the NPPs.

Further information on the coverage of the NPPs is available from the Office's *Information Sheet 12 – Coverage of and Exemptions from the Private Sector Provisions*.

What does the Spam Act cover?

With some exceptions, the Spam Act prohibits the sending of unsolicited commercial electronic messages with an Australian link.

Certain types of 'designated' electronic messages are partially exempt from the Spam Act. Exempt messages can be from:

- government bodies
- registered political parties
- religious organisations
- registered charities
- educational institutions (sent to current and past students and their households).

Further information on exemptions under the Spam Act is available from ACMA.[4]

The Spam Act should also be read in conjunction with the relevant codes such as the Australian E-Marketing Code of Practice, which sets out detail such as hours when individuals may be contacted and industry complaint handling schemes.

Example: A small business

Sarah owns and operates a conference-organising business with an annual turnover of $1.8 million. She collects names and contact details from attendees at each conference, primarily so that she can process their registrations and confirm arrangements. Sarah also uses these details to email people to promote upcoming commercial events.

Using personal information for this purpose is unlikely to be covered by the NPPs, because Sarah's business has an annual turnover of less than $3 million and does not fall into any of the categories described in section 6D(4) of the Privacy Act (such as by providing a health service).

However, Sarah's promotional emails would be covered by the Spam Act. The emails would be 'commercial electronic messages' because they advertise or promote services provided by Sarah's organisation.

Sarah would need to ensure that the emails compy with the Spam Act, particularly the elements of:

- consent
- identification
- functional unsubscribe mechanism.

Address harvesting software and the use of harvested-address lists

The Spam Act also prohibits the supply or acquiring of 'address harvesting' software or lists compiled using such software.

Address harvesting software is defined in the Spam Act as software that is specifically designed or marketed for use for:

- searching the internet for electronic addresses
- collecting, compiling, capturing or otherwise harvesting those electronic addresses.

Civil penalties apply for the breach of these provisions.

Other forms of Direct Marketing

The Spam Act does not cover faxes, internet pop-ups or voice telemarketing.[5] However, the 'Do not Call Register' (established under the *Do Not Call Register Act 2006*) prohibits telemarketers from making calls to numbers listed on the register. For more information about the Do Not Call scheme go to the www.donotcall.gov.au.

The Privacy Act will apply to how organisations may use personal information for these other forms of direct marketing. For general advice on these obligations, see the Office's *Guidelines on the National Privacy Principles* available from our website at www.privacy.gov.au.

[4] See "Exemptions" available from www.spam.acma.gov.au.

[5] See the Spam Act, section 5 (definition of 'Electronic Messages') and Section 6 (definition of 'Commercial Electronic Messages').

Is consent needed to send commercial electronic messages?

Consent must always be obtained, unless the message is exempt under the Spam Act.

Under the Spam Act, an individual's consent must always be obtained for commercial electronic messages unless the message is exempt. This consent may be 'express' or 'inferred'.

In the Privacy Act, section 6 states that consent may be 'express' or 'implied'. Express consent is given explicitly, either orally or in writing. Implied consent is agreement that can be inferred from an individual's conduct. In either case, the individual must actively indicate their consent to the act or practice in question.

To be valid, consent must be fully informed and freely given.

How does 'inferred consent' align with the Privacy Act?

While 'express consent' is a common concept to both Acts, 'inferred consent' is not a form of consent used in the Privacy Act. Schedule 2 of the Spam Act sets out what is meant by 'inferred consent'.

Inferred consent occurs:[6]

- through an existing business or other relationship, where there is a reasonable expectation of receiving those commercial electronic messages
- through conspicuous publication of a work-related electronic address.

When compared to how 'implied consent' is applied under the Privacy Act, 'inferred consent' could have a broader meaning. In particular, it permits practices that fall within an individual's reasonable expectations. NPP 2 deals separately with consent and an individual's reasonable expectations.

However, where an organisation validly relies on 'inferred consent' under the Spam Act to send commercial electronic messages, then it is likely that this can be taken as being a practice that is authorised by law. In turn, this would satisfy NPP 2.1(g) under the Privacy Act, which permits the use or disclosure of personal information for secondary purposes where 'required or authorised by law'.

In handling a complaint alleging that consent to use personal information to send a message could not be inferred, the Privacy Commissioner would consider whether reliance on inferred consent was justified. Among other things, the Privacy Commissioner would take into account the provisions and policy intent of the legislation, and ACMA's views.

For further discussion on complaints, see below under '*How will complaints be handled?'* (page 10).

What if consent is impracticable?

The Spam Act requires that consent be obtained before sending commercial electronic messages that are not designated as exempt. It is unlawful to send commercial electronic messages that do not meet this consent requirement.

A matter that has caused uncertainty for some stakeholders is the relationship between the requirement to obtain consent under the Spam Act and NPP 2.1(c) in the Privacy Act.

NPP 2.1(c) provides that personal information may be used or disclosed for the secondary purpose of direct marketing (of any kind) if:

- it is not 'sensitive information' (such as health information)'
- consent is 'impracticable' to obtain
- certain other requirements are met, such as affording individuals the right to opt-out of receiving such messages.

Because the Spam Act requires consent, if consent is impracticable to obtain, then the commercial electronic message should not be sent.

The application of NPP 2.1(c) to exempt messages is discussed further at page 9.

[6] See the "Express & Inferred consent" at www.spam.acma.gov.au.

How do organisations identify themselves when sending commercial electronic messages?

The Spam Act requires that all commercial electronic messages must identify the sender and provide information on how they may be contacted. Unlike the consent and unsubscribe requirements of the Spam Act, there are no exemptions to this requirement.

Every commercial electronic message sent must:

- clearly and accurately identify the individual or organisation who authorised sending the message. For example, if a third party sends out messages on behalf of your organisation, the message must include the correct legal name of the organisation or individual on whose behalf the message is being sent and an Australian Business Number, where applicable.
- include accurate information about how the recipient can contact your organisation, or you as an individual sender, for example, a website address and a telephone number.

These obligations set out similar matters to the notice obligations under NPP 1. NPP 1 specifies what individuals must be told when their personal information is initially collected by organisations covered by the Privacy Act.

Further information on these notice obligations is provided below, under '*What other obligations apply under the Privacy Act?'*

Must organisations provide a functional 'unsubscribe' mechanism?

Yes.

The Spam Act expressly requires organisations to include a functional unsubscribe mechanism in each message. This requirement does not apply where the message is designated as exempt.

The Privacy Act imposes similar obligations for all direct marketing under NPP 2.1(c). However, as explained below (see page 9), regardless of whether a commercial email message is exempt from the Spam Act, it is unlikely that an organisation would be able to rely on this exemption to use personal information for electronic direct marketing.

Accordingly, organisations should ensure that they meet the requirement of the Spam Act to provide unsubscribe options. An unsubscribe mechanism must satisfy the following conditions:

- it must remain functional for at least 30 days after the original message was sent
- it must allow the unsubscribe message to be sent to whoever authorised the sending of the message, not necessarily any third party that sent it on their behalf
- unsubscribe instructions must be presented in a clear and conspicuous way
- a request to unsubscribe must be honoured within five working days
- unsubscribing must be at low cost, or no cost, to the user (for example, in the case of SMS unsubscribe facilities, a 1800-telephone number would be acceptable).[7]

Further information on the unsubscribe requirements under the Spam Act is available from ACMA at www.spam.acma.gov.au.

Example: How the Spam Act might apply to a nightclub sending SMS messages

Ben goes to a nightclub and is asked to provide his mobile phone number, email address and name. He is told that this will put him on a 'VIP' list whereby he will be contacted by the nightclub with information about special nights, DJs and other promotions done by the nightclub.

Do the Privacy Act or Spam Act apply?

Ben doesn't really want the nightclub to have his name, and his email address is for work, so he only provides his mobile number. Other people did provide their names and identifiable email addresses, so the contact list will include personal information, though not Ben's.

Because the nightclub will probably not be able to identify Ben from his mobile number alone, especially if it is only used for sending SMS messages, this information is unlikely to be personal information under the Privacy Act.

However, the nightclub intends to send

[7] See "Unsubscribe ability is mandatory" at www.acma.gov.au.

commercial electronic messages to Ben that promote its commercial services, so these messages would be covered by the Spam Act. These messages must meet the three conditions of consent, identification, and a functional unsubscribe mechanism.

Has the Spam Act been satisfied?

Ben was told what his mobile number would be used for, and chose to provide it, so the nightclub can infer that Ben has consented. The messages it sends should be related to what Ben has consented to. For example, the nightclub should not assume that Ben has consented to receiving messages about other goods or services offered by other businesses.

In any messages it sends, the nightclub must clearly identify itself and how it can be contacted. It must also provides the option for individuals to unsubscribe from receiving future messages.

Disclosing the information

In time, the nightclub owner is asked by the owner of a local concert venue if it can buy the nightclub's contact list for its own direct marketing purposes. The concert venue attracts a similar clientele to that which goes to the nightclub, so it is likely to be of value to the venue.

Before using the list, the concert venue owner needs to consider a number of issues.

The Spam Act does not prohibit the sale of the contact list, but the concert venue does need to meet the three conditions of the Spam Act when it sends any commercial electronic messages. The message sender - in this case, the concert venue owner – must ensure that consent exists. The Spam Act prohibits the sending of messages that aim to 'test the water', or gauge the recipient's interest in receiving future commercial messages.

The concert venue would need to gain consent through other means.

The nightclub owner would need to ensure that the disclosure of the list to the venue complies with NPP 2. Unless individuals consented to this disclosure when they provided their personal information, or were told that this may happen, it would probably not be permitted by the Privacy Act.

What other obligations apply under the Privacy Act?

The Privacy Act contains obligations concerning other aspects of personal information handling that the Spam Act does not address. This includes obligations that apply when personal information is initially collected for electronic and other forms of direct marketing, as well as how it must be stored and handled.

Collection and providing notice

NPP 1.1 provides that an organisation must only collect personal information by lawful and fair means and not in an unreasonably intrusive way. Practices such as the use of address harvesting software, which is prohibited by the Spam Act, would also likely be in breach of NPP 1.1.

Under NPP 1.3, organisations that collect personal information directly from individuals must take reasonable steps to provide individuals with notice of certain matters, including:

- the identity of the organisation and how to contact it
- the fact that he or she is able to gain access to the information
- the purposes for which the information is collected
- the organisations (or the types of organisations) to which the organisation usually discloses information of that kindany law that requires the particular information to be collected
- the main consequences (if any) for the individual if all or part of the information is not provided.

This information should generally be provided to the individual before the collection or, if this is not practicable, as soon as possible afterwards.

Under NPP 1.5, organisations that collect personal information from someone other than the individual, must take reasonable steps to ensure that the individual is or has been made aware of the matters listed under NPP 1.3.

Accordingly, direct-marketing organisations that collect personal information from other organisations may also have 'notice' obligations.

This could include:

- obtaining confirmation from the disclosing organisation that notice has been given
- taking reasonable steps itself to contact individuals and provide them with notice.

Other uses and disclosures

As noted above, NPP 2 obligations are not restricted to direct marketing. They apply to uses and disclosures of personal information regardless of the context in which they occur. Organisations using or disclosing personal information for secondary purposes other than direct marketing, should consider whether the activity complies with the obligations described in NPP 2.1.

An organisation may only use or disclose personal information for the primary purpose for which it is collected, and in other limited circumstances. The primary purpose should be narrowly and specifically defined.

Organisations should carefully consider their privacy obligations before giving other organisations access to personal information from their customer databases.

Unless one of the provisions in NPP 2 applies, disclosures such as selling direct mailing lists may breach the Privacy Act.

Security

NPP 4 requires that organisations take reasonable steps to ensure that the personal information they hold is protected from:

- misuse and loss
- unauthorised access, modification or disclosure.

NPP 4 also requires that organisations take reasonable steps to destroy or permanently de-identify personal information when it is no longer needed. An organisation that collected personal information for a specific promotional campaign should destroy or permanently de-identify that information at the campaign's conclusion.

Access and Correction

NPP 6 gives individuals the right to access their personal information. This provision would apply to organisations that originally collected the information and to contractors who receive it to conduct direct marketing on that organisation's behalf.

An organisation must not charge an individual for lodging a request for access but may apply a reasonable charge to recover costs of providing access (NPP 6.4).

The steps an organisation must take to comply with the access principle will vary, depending on circumstances such as the type of organisation.

NPP 6 also requires organisations to take reasonable steps to ensure that personal information that they hold is corrected, where the individual concerned shows that it is not accurate, complete or up-to-date.

Transferring personal information overseas

Organisations considering transferring personal information overseas should consider what privacy protection will apply to the information in the receiving country.

NPP 9 requires that these transfers should generally only occur where the organisation reasonably believes that the privacy protection regime available is substantially similar to that provided under the NPPs. These protections may take the form of legislation, a binding scheme or a contract.

Transfer of personal information may also be permitted in other specific circumstances, such as where the individual has consented to the transfer. [8]

What if an organisation is covered by the NPPs, but its messages are exempt from the Spam Act?

Some commercial electronic messages can be exempt or partially exempt from the Spam Act, but using personal information to send such messages could still be covered by the Privacy Act. Such messages could include those from registered political parties, charities, religious groups and education institutions.

Although these exempt messages do not need to meet the requirements regarding consent and a functional unsubscribe mechanism, they must identify the sender and provide contact details.

The following types of organisations will generally be covered by the NPPs if they have a turnover of more than $3 million, even if their messages are exempt from the Spam Act:

[8] There are other mechanisms under NPP 9 – see Schedule 4 of the Privacy Act

- private educational institutions (including pre-schools, schools, colleges and universities)
- religious organisations
- registered charitable organisations.

If such organisations are 'using' personal information to send commercial electronic messages, they must comply with NPP 2. The implications of this are discussed below, under '*Is consent required for commercial electronic messages that are designated as exempt?'*

Because it is generally practicable to obtain consent for electronic direct marketing, organisations will not usually be able to rely on NPP 2.1(c). As NPP 2.1(c) can generally not be relied upon, the other matters set out in this principle will also not apply, including the requirement to provide an unsubscribe mechanism.

While exempt messages are not required to include an unsubscribe mechanism by either the Spam Act or the Privacy Act, the provision of such a mechanism is strongly encouraged as good privacy practice.

In addition, organisations that send commercial electronic messages that are exempt from the Spam Act, must still comply with each of the other nine NPPs when handling personal information.

Is consent required for commercial electronic messages that are exempt from the Spam Act?

No, it is not required, though if the organisation is covered by the Privacy Act, it will still need to comply with NPP 2. Obtaining consent, whether express or implied, is a valid method of achieving such compliance.

The Spam Act does not require consent for commercial electronic messages that are designated as exempt.

However, even where a commercial electronic message is exempt from this requirement under the Spam Act, a sender must still comply with any obligations it has under the NPPs.

This scenario may occur, for example, where commercial electronic messages are being sent by religious organisations, charities or educational institutions with an annual turnover greater than $3 million. While messages from these organisations are exempt from the Spam Act, their handling of personal information will still be covered by the Privacy Act.

An organisation covered by the Privacy Act must determine whether it is proposing to use 'personal information' (see *What is 'personal information'?* above at page 3) before sending 'designated' commercial electronic messages. If it is, it must ensure that the use complies with NPP 2.

NPP 2 provides that personal information may only be used for the purpose for which it was initially collected, unless a specified exception applies.

For example, obtaining the individual's express or implied consent to the secondary use or disclosure (NPP 2.1(b)). This consent may be verbal or in writing.

Another exception that might be relevant is where:

- the secondary purpose is related to the primary purpose of collection (or directly related if the information is 'sensitive') and
- is within the individual's reasonable expectations (NPP 2.1(a)).

The individual's reasonable expectations might be informed by what they are told when their information is initially collected (see, *Collection and providing notice* at page 7).

NPP 2.1(c) will not generally apply to electronic direct marketing

While NPP 2.1(c) provides an exception for instances where consent for direct marketing is impracticable to obtain, in general, NPP 2.1(c) is unlikely to apply to commercial electronic messages.

A key benefit of sending commercial electronic messages for direct marketing is that they provide a highly cost and time effective form of communication.

Given the ease and relatively negligible cost required to contact individuals using such technologies, it is unlikely that it would be 'impracticable' to obtain an individual's consent. An organisation will usually have to consider whether another exception under NPP 2 would permit the use of personal information for this purpose.

Therefore, while the Privacy Act does not *require* consent to send commercial electronic messages that are exempt from the Spam Act, obtaining consent is one option that is available under NPP 2.

Example: Exempt commercial electronic message sent by an organisation covered by the NPPs

A large registered charity sells merchandise to raise funds, in addition to receiving donations. The charity has an annual turnover of more than $3 million, and so is covered by the NPPs.

Is it personal information?

The charity sends commercial electronic emails to individuals who have previously made donations. These emails promote the sale of the charity's merchandise. The donors provide their names and email addresses when making donations through the charity's website. Together, these pieces of information allow the charity to identity the donor, and are 'personal information' under the Privacy Act.

How does the Spam Act apply?

It is a registered charity and the emails relate to goods supplied by it, so any commercial electronic message will be partially exempt from the Spam Act. While they must identify the charity and provide current contact details, these emails are exempt from the requirement to obtain consent (whether express or inferred) or to provide a functional unsubscribe mechanism.

Notice obligations under NPP 1

When initially collecting the donors' personal information, the charity ensured that it met its obligations under NPP 1.3 to provide donors with notice of its identity, how it can be contacted, and the purposes for which the information was collected.

In describing the purposes of collection, the charity's collection notice included reference to using the personal information for future direct marketing. This step created a 'reasonable expectation' on the part of donors that their personal information may be used for the purpose of electronic direct marketing. As this potential secondary use of personal information is related to the primary purpose, and falls within the individual's reasonable exceptions, the charity may use the email address for this purpose.

Good privacy practice: Seek consent

While in this case it was not required by law, the charity also promoted good privacy practice by giving individuals the opportunity to unsubscribe from receiving future direct marketing emails, and continues to do so with any subsequent message. This allows the charity to rely on the implied consent of donors for the use of their personal information, and avoids the charity having to make judgements about whether the donors' reasonable expectations are sufficiently clear.

Not within reasonable expectations

If the charity had not provided adequate notice of this potential secondary use of personal information, then NPP 2 would generally require the donors' consent be obtained, whether express or implied.

While NPP 2.1(c) does allow direct marketing where consent is impracticable, as the charity has donors' email addresses, it could easily and cheaply contact them to seek consent. Accordingly, it is unlikely that it could be said that seeking consent is impracticable.

Other NPPs met

The charity also ensures that it meets its other obligations under the NPPs, including by taking reasonable steps to keep the direct mailing list secure and not using it for other unrelated purposes.

How will complaints be handled?

An individual may complain to ACMA about receiving spam. Information on making a complaint to ACMA can be obtained from www.spam.acma.gov.au.

Complaints to the Privacy Commissioner

An individual may complain to the Privacy Commissioner about an act or practice that may interfere with their privacy.

Complaints to the Privacy Commissioner must be in writing. The complaint should generally be made first to the organisation concerned, which should be given 30 days to respond.

However, the Privacy Act provides that the Privacy Commissioner may decide not to investigate a matter in certain circumstances.[9] For example, where another Commonwealth, state or territory law provides more appropriate remedy for the matter that is subject of the complaint.

The Spam Act deals specifically with electronic direct marketing, and provides for civil penalties as well as Federal Court orders for

[9] See section 41 of the Privacy Act.

compensation. The Privacy Commissioner will usually advise a complainant that the matter is best dealt with by ACMA under the Spam Act.

If a matter appears to constitute an interference of privacy under the Privacy Act, but would not constitute an infringement under the Spam Act, the Privacy Commissioner may conduct preliminary enquiries or investigate the complaint. This could include circumstances where:

- the alleged interference with privacy concerns personal information in an email address or phone number, though the act or practice in question was not related to the sending of commercial electronic messages.

  This could include where personal information was not afforded reasonable security (NPP 4), or where the information was disclosed in a manner that did not comply with NPP 2.

- a commercial electronic message is sent, or caused to be sent, by an organisation covered by the NPPs, though that message was exempt from the Spam Act. In such circumstances, the Spam Act may not offer an adequate remedy for the individual.

Complaints to the industry bodies

If a complaint concerns a matter set out in the Australian eMarketing Code of Practice, then the complaint should first be made to the e-marketing company to which the complaint relates.

ACMA explains that if the complaint is not handled to the satisfaction of the complainant, it will be referred to the Recognised Industry Body nominated by the e-marketing company.

ACMA will deal with the complaint if it 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. A complainant may request that his or her complaint be referred to ACMA for consideration at any stage of the complaint handling process.[10]

More information

More information is available from the Office of the Privacy Commissioner and the Australian Communication and Media Authority.

The Office has produced the following resources:

- National Privacy Principles
- Guidelines to the National Privacy Principles
- Information Sheets
- Frequently Asked Questions

For consumers

Information for consumers on direct marketing can also be found in the Office of the Privacy Commissioner's (the Office) Frequently Asked Questions and in ACMA's Spam and E-Security pages.

More information about complaint handling is also available:

- More information about the Office's complaints process
- More information about ACMA's complaints process

[10] See "Australian E–marketing code of practice" available at www.spam.acma.gov.au.

Private Sector Information Sheets

Information sheets are advisory only and are not legally binding. The National Privacy Principles in Schedule 3 of the Privacy Act do legally bind organisations.

Information sheets are based on the Office of the Privacy Commissioner's understanding of how the Privacy Act works. They provide explanations of some of the terms used in the NPPs and good practice or compliance tips. They are intended to help organisations apply the NPPs in ordinary circumstances. Organisations may need to seek separate legal advice on the application of the Privacy Act to their particular situation. Nothing in an information sheet limits the Privacy Commissioner's ability to investigate complaints under the Privacy Act or to apply the NPPs in the way that seems most appropriate to the facts of the case being dealt with. Organisations may also wish to consult the Commissioner's guidelines and other information sheets.

Office of the Privacy Commissioner

Privacy Enquiries Line **1300 363 992** - local call (calls from mobile and pay phones may incur higher charges)
TTY 1800 620 241 – no voice calls; Fax + 61 2 9284 9666; GPO Box 5218, Sydney NSW 2001.

Private Sector Information Sheet 26
Web HTML, Word and PDF published August 2008
ISBN 978-1-877079-61-0

www.privacy.gov.au