

# Are You An Accidental Spammer?



How Australia's  
new anti-spam law  
affects your  
organisation's  
outgoing e-mail

A special report from  
**First Step Communications**

[www.firststep.com.au](http://www.firststep.com.au)

## **Copyright**

This report is copyright. Apart from any fair dealing for the purpose of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced by any process without written permission from the publisher.

## **Liability disclaimer**

The material contained in this report is general and is not intended as advice on any particular matter. First Step Communications and the author expressly disclaim all and any liability to any persons whatsoever in respect of anything done by any such person in reliance, whether in whole or in part, on this report. Please take appropriate legal advice before acting on any information in this report.

---

# Table of Contents

---

Copyright .....	1
Liability disclaimer .....	1
Table of Contents .....	2
Introduction .....	3
Is this report for you? .....	3
At a glance .....	3
Quick Summary .....	5
Scope of the Act .....	7
Who is affected? .....	7
What does it apply to? .....	7
Where does it apply? .....	8
When does it take effect? .....	8
Other Rules and Guidelines .....	9
"Netiquette" .....	9
The Privacy Act .....	11
Your Internet Service Provider .....	12
Other laws .....	12
Overview of the Requirements .....	13
Collecting e-mail addresses .....	14
Express consent .....	14
Inferred consent .....	15
Privacy implications .....	17
External Mailing Lists .....	18
Existing Mailing Lists .....	18
Sending e-mail .....	19
What <i>must</i> be included in a message? .....	19
Is it commercial e-mail? .....	19
Identifying the sender .....	20
Unsubscribe facility .....	21
Managing the e-mail addresses .....	24
Penalties .....	27
More Information .....	28
The Spam Act .....	28
Netiquette .....	28

---

# Introduction

---

This is a report about spam.

More precisely, it's a report about Australia's new anti-spam legislation, the *Spam Bill 2003* – also known as the Spam Act – which comes into effect on 10<sup>th</sup> April 2004. It may already be in force by the time you're reading this report.

By passing this law, the Australian Government has tightened the rules about sending e-mail. The purpose of this report is to explain how this will affect you when sending commercial e-mail from your organisation.

Throughout this report, the Spam Act will be referred to as just "the Act".

## Is this report for you?

The Act itself applies to almost every organisation in Australia. **If your organisation sends e-mail, you *will* be affected by it.**

This report doesn't attempt to cover the full scope of the Act. In particular:

- It applies to sending e-mail, not SMS messages or other electronic communication;
- It's mostly for businesses, though it does extend to most other organisations that send promotional e-mail. A few organisations are exempt from the main provisions of the Act – see "Who is affected?" below – and this report doesn't cover those organisations.

This report has been written for organisations who would like to use – and continue using – e-mail as part of their normal business operations. It's **not** for spammers looking for loopholes in the laws so that they can continue sending spam!

## At a glance ...

This report is organised as follows:

- The next section is a **Quick Summary** to give you a very brief overview of what you have to do under the Act.
- This is followed by the **Scope of the Act**, which describes who the Act affects and how; and then the **Other Rules and Guidelines**

section, which talks about other relevant laws and guidelines to consider when sending e-mail.

- The next section is the **Overview of the Requirements**, which breaks the legislation down into three broad areas. This is followed immediately by a detailed look at each of the three areas.
- Then comes the **Penalties** section, which describes the consequences of breaking this law.
- Finally, there is a list of references to **More Information**, which tell you where to find out more information about the Act and its consequences.

---

## Quick Summary

---

For those who like to cut to the chase, here's a summary of what you **must** do to ensure that you comply with the Act.

You can only send commercial e-mail to addresses that you've obtained using one of these three methods:

- The owner of the e-mail address has given you permission to send them e-mail; OR
- You have an existing business relationship with them; OR
- They have published their e-mail address publicly (but you cannot obtain e-mail addresses by using address-harvesting software).

In all cases, you can only send them appropriate e-mail that they could reasonably expect to receive, based on your relationship with them or the place where they published their address.

Any commercial e-mail message must:

- Identify the organisation making the commercial offer (you, in most cases); AND
- Tell the recipient how to "unsubscribe" from receiving future messages.

When somebody asks to unsubscribe, you must:

- Remove them from your database.
- Do this within 5 working days.

That gives you a quick overview of the Act. However, it **is** only a very sketchy overview, and I recommend that you continue reading to find out the details.

By the way, if you'd like a more official summary of the Act, here's the simplified outline that appears at the front of the Act itself:

- This Act sets up a scheme for regulating commercial e-mail and other types of commercial electronic messages.
- Unsolicited commercial electronic messages must not be sent.
- Commercial electronic messages must include information about the individual or organisation who authorised the sending of the message.
- Commercial electronic messages must contain a functional unsubscribe facility.

- Address-harvesting software must not be supplied, acquired or used.
- An electronic address list produced using address-harvesting software must not be supplied, acquired or used.
- The main remedies for breaches of this Act are civil penalties and injunctions.

---

# Scope of the Act

---

## Who is affected?

The Act affects all Australian organisations that send commercial e-mail. To be more precise, it covers all organisations that send e-mail from Australia, so even foreign-owned bodies are included.

Obviously, this includes commercial organisations, so if you're operating a business in Australia, it affects you.

There **are** a few bodies that are exempt from some parts of the Act. Specifically, if your organisation is one of these:

- a government body
- a registered political party
- a religious organisation
- a charity or charitable institution

then this report is not for you. But the Act **does** apply to you in different ways, so seek advice from elsewhere.

Note that many not-for-profit organisations **do** fall under the full provisions of the Act. Organisations such as trade unions and professional associations must still comply, even if they have a not-for-profit purpose.

Educational institutions must also comply with the full provisions of the Act, except when promoting their goods or services to students or past students. So, for example, a university can send unsolicited e-mail advertising new courses to past students, but cannot send the same e-mail to the general public.

If you're not sure whether it applies to you, it's safer to assume that it does, until you know otherwise.

## What does it apply to?

The Act makes it illegal to send commercial e-mail to somebody without their consent.

(In fact, the Act covers other types of electronic communication, such as SMS messages. However, we're only covering e-mail in this report).

At first glance, that looks like a pretty strong definition. But, as we'll see later, the definition of "consent" is **very** different from what you would expect, and this greatly weakens the definition.

Please note that the Act applies to **all** e-mail that you send! It's not only for people who send to mailing lists and operate e-mail newsletters. It doesn't make a distinction between a single e-mail message and a bulk e-mail message. As far as it's concerned, a single e-mail message could also be considered illegal if it doesn't follow the rules. **So if your organisation sends e-mail, it falls under the provisions of the Act.**

### **Where does it apply?**

These are Australian laws, so they apply to organisations in Australia that send e-mail.

The wording in the Act talks about "an Australian link", which is defined as also covering e-mail sent **to** Australian residents, even from people outside Australia. But there aren't yet any international arrangements that allow the Australian Government to pursue overseas spammers, so this part of the Act has no practical use.

### **When does it take effect?**

The Act has already passed into law (on 12<sup>th</sup> December 2003). However, there is a 120-day grace period to allow organisations time to put processes into place to comply with the Act.

The Act takes effect in full from 10<sup>th</sup> April 2004.

If you're reading this after that date, then the Act is in force already. So make sure that you're complying!

---

## Other Rules and Guidelines

---

The Spam Act isn't the only thing that should guide you when sending e-mail. It doesn't live in isolation. Other relevant rules and guidelines come from other places, including:

- Netiquette – the established guidelines for “polite behaviour” on the Internet;
- The Privacy Act – and in particular, the National Privacy Principles which came into law in December 2001;
- Your own Internet Service Provider's rules about spam.

We'll describe these here so that you understand how they fit in with the Act.

### “Netiquette”

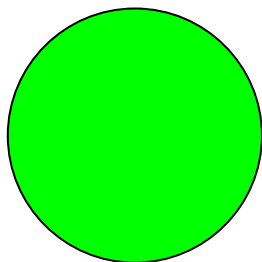
The Act defines what is allowed **within the law** when sending e-mail. But just because something is allowed by the law doesn't mean that you should do it. For example, the law doesn't stop people from speaking loudly into a mobile phone in a public restaurant, but you won't make many friends if you do so!

The same applies on the Internet.

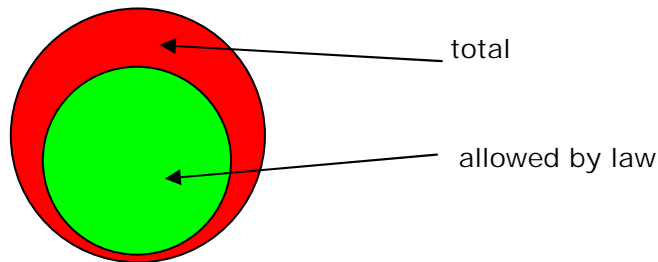
E-mail had been around for a long time before any government decided to pass laws about it. In that time, the Internet community has – by mutual consent – created its own set of guidelines for etiquette when using the Internet. These guidelines are known informally as “netiquette”.

By and large, netiquette is much stricter than the law.

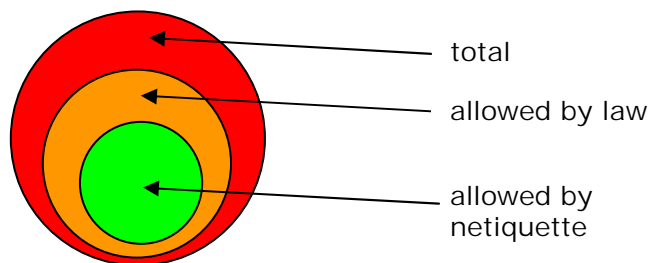
So, for example, if this circle represents all the e-mail users in the world:



then the Act lays down certain rules which restrict the people you're allowed to reach. So your allowed circle grows smaller – like this:



Netiquette takes this even further, so your circle is now even smaller:



### ***Why is this important to you?***

It's very, **very** important that you know – and follow – the rules of netiquette, not just the rules laid down by law.

Why? Because some people in the Internet community have taken it upon themselves to "police" these rules of netiquette, and take action against people who break them.

Here are some examples:

- They can publish your name and e-mail address in public Internet bulletin boards, giving your organisation bad publicity.
- They can add your address to e-mail "blacklists", which many Internet Service Providers use in order to block spammers.
- They can complain to your Internet Service Provider, who can cancel your account. Don't believe me? Check the fine print in your ISP's terms and conditions – most of them have a clause that allows them to do just that.
- They can "mail-bomb" you, by sending you thousands of junk e-mail messages over and over, blocking your in-box and making it impossible for you to get legitimate e-mail.

These self-appointed “Internet police” usually operate on the basis of “Shoot first, ask questions later”. In other words, if they classify you as a spammer, or somebody reports you to them, they will treat you as guilty first, and it’s up to you to prove your innocence.

Ironically, the smart spammers know clever ways to outwit the Internet police, so that they can continue sending spam. So it’s often the “small players” – ordinary businesses who send commercial e-mail but haven’t made spam an art form – who are hurt the most by their actions.

This might all seem far-fetched, but believe me, **it can happen to you** if you break the rules of netiquette. You see, most Internet users hate spam! So they are happy to trust anybody who can block some of their spam, and if a few dolphins get caught in the shark nets, hey, it’s better than a shark getting through, right?

That’s why it’s so important to ensure that you follow the rules of netiquette, not just the letter of the law.

The Australian Government’s own publications focus almost exclusively on what’s allowed and disallowed under the law, but don’t mention netiquette much, if at all. As far as I know, this is the only report that talks about them both.

### ***Netiquette says ...***

Throughout this report, I’ll be referring to netiquette, especially when the requirements of the Act are different from the requirements of netiquette. To make it easy for you to spot these instances, I’ll use the text **NETIQUETTE SAYS** with a box and this warning symbol to highlight them for you:



So whenever you see this sign, read carefully!

## **The Privacy Act**

If your organisation falls under the provisions of the Privacy Act, and in particular the National Privacy Principles, you have further restrictions on the use of e-mail addresses.

The National Privacy Principles are mainly about protecting the **privacy** of personal information, so they are more to do with how you maintain your e-mail database than with how you use it for sending e-mail. However, they **do** have a component (NPP2) that’s related to e-mail marketing.

Where relevant, I'll mention the National Privacy Principles in this report. For a more detailed look at these requirements, you can read our special report *The National Privacy Principles and the Internet*, available from [www.firststep.com.au](http://www.firststep.com.au).

## Your Internet Service Provider

Regardless of the provisions of the Spam Act, your Internet Service Provider (ISP) might have different restrictions about sending e-mail.

Obviously, you have to obey the law, so if the Act is more restrictive than your ISP, then the Act takes precedence. However, it's usually the other way around. Most ISPs place strict restrictions on sending e-mail (usually bulk e-mail). Many ISPs have strict terms and conditions that allow them to immediately close down the account of any spammer or suspected spammer.

Why? Because if an Internet user starts sending spam, other ISPs around the world will start blocking **all** e-mail from the sender's ISP, which causes problems for all that ISP's clients. That's why most reputable ISPs take a very hard stance against spammers, because they can seriously damage the ISP's business.

## Other laws

There are other laws that apply when sending e-mail. For example:

- The *Crimes Act* makes it an offence to send harassing or offensive e-mail;
- The *Trade Practices Act* prohibits false or misleading information about products and services;
- The *Interactive Gambling Act* places restrictions on certain forms of on-line gaming.

These and other laws that relate to the **content** of your e-mail messages are beyond the scope of this report.

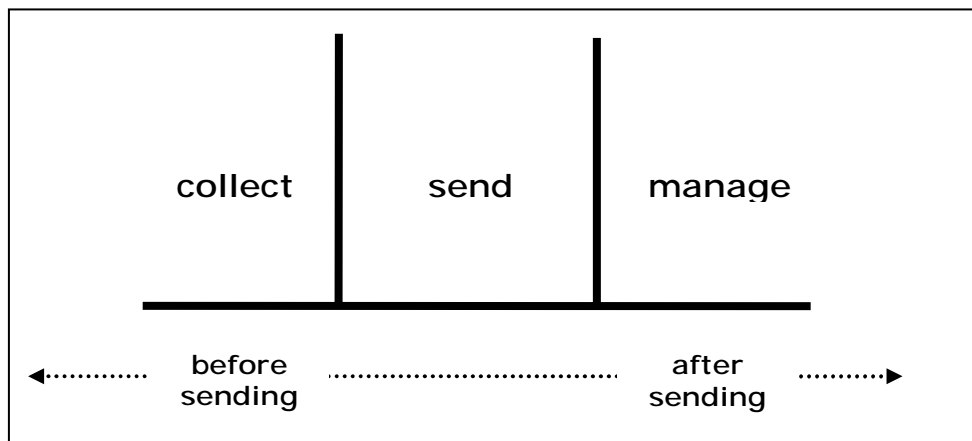
---

# Overview of the Requirements

---

OK, let's get down to the legislation itself.

For ease of understanding, consider it in three parts:



The Act itself isn't written in this order, but I think it's a good way to classify the most important parts. Here's what each part covers:

- **Collect:** There are certain rules that apply when you're **collecting** e-mail addresses to add to your database. Broadly, you require the owner's consent before you can use their e-mail address. But the definition of consent is very broad, as we'll see later.
- **Send:** There are certain rules that apply when you're **sending** a message to somebody. Broadly, you have to identify yourself clearly and offer a facility for people to request that you stop sending them further e-mail.
- **Manage:** There are certain rules that apply when you're **managing** your e-mail database. Broadly, you have to remove people from your database in a timely manner if they request it.

I've said this before, but it's worth repeating that everything in the Act applies to **all** e-mail addresses that you collect and use, not just those that you're using for a mailing list.

In the next three sections of the report, we'll look at each of these three areas in more detail.

## Collecting e-mail addresses

---

The Act says that you must have a person's consent before sending them any commercial e-mail.

That sounds like a fairly strict rule, but in fact it's not.

Here's why: Most ordinary people would say that "consent" means getting their permission. But the Act has a much broader definition of "consent". It says that consent can be given in two ways:

- **Express consent** happens when somebody explicitly gives you permission to send them e-mail – for example, by subscribing themselves to your mailing list, or giving you their business card and asking you to contact them.
- **Inferred consent** happens when somebody hasn't given you explicit permission to send them e-mail, but they could reasonably expect to receive e-mail from you.

### Express consent

If somebody gives you permission to send them e-mail, then obviously it makes sense that you can do so. That's just plain common sense, and you won't get many complaints about that (provided you only send them the sort of e-mail they agreed to receive, of course).

For example, these are all examples of express consent:

- You have a newsletter subscription form on your Web site, and somebody signs up to receive your newsletter;
- Somebody at a networking function gives you their business card and asks you to send them information about your products;
- You conduct an in-store competition that requires people giving you their e-mail address, and you make it clear that by doing so they are giving consent to receive marketing e-mail from you;
- Somebody visits your Web site, and e-mails you to ask for further information.

On the other hand, here are some things that would **not** be considered express consent (though some of them might be inferred consent, which we discuss later):

- You publish a printed newsletter and you decide to switch to an e-mail newsletter, so you take all your existing subscribers and add their e-mail addresses to a mailing list;

- Somebody at a networking function gives you their business card, and you add them to a mailing list;
- You conduct an in-store competition to collect e-mail addresses for a mailing list, but you don't make it clear on the competition form that you're planning to use their e-mail addresses in this way;
- Somebody visits your Web site and e-mails you for further information, and you add them to your e-mail newsletter list;
- Somebody sees a newsletter subscription form on your Web site, and subscribes **somebody else** (for example, a friend or colleague) to your newsletter.

### ***Double opt-in***

Consider that last example above, where a well-meaning person signs up their friend for your newsletter. This it can cause trouble for **you**, because the friend might accuse you of spamming.

If you **do** experience this problem regularly, the best solution is a "double opt-in" subscription. This means that when somebody subscribes via the Web site, instead of adding their e-mail address to your list immediately, you send them a separate e-mail message, which they have to confirm before you add them to the list. This ensures that it **was** that person who made the original subscription, not somebody else who, mischievously or in good faith, subscribed them on their behalf.

The Act does **not** require you to use a double opt-in system, but if you're getting complaints from subscribers who claim that they didn't join your list, a double opt-in system can solve this problem.

### **Inferred consent**

Now let's talk about inferred consent, which is not as clear-cut.

If you have somebody's e-mail address, but they haven't **explicitly** given you permission to send them e-mail, then can you do so? And should you?

The Act says yes, you can, provided that it's "reasonable" to do so. So let's look at what could be considered reasonable.

There are two things that could contribute to whether something is considered reasonable in this context:

1. Whether you have an existing business relationship with that person;
2. Whether that person has made their address public in a way that invites e-mail communication.

### ***Existing business relationship***

If you have an existing business relationship with somebody, then you have much more freedom to send them e-mail in the future.

For example, if that person is a customer, and they gave you their e-mail address, then they might reasonably expect that you keep in touch with them by e-mail, even to send them marketing material. Similarly, if you exchange business cards with a businessperson at a networking function, it's reasonable to send them an e-mail message to follow up that initial contact, as long as that e-mail is related to their work.

#### **NETIQUETTE SAYS ...**



Some people will still get upset if you send them marketing e-mail, even if they already have a business relationship with you. So be very careful about how you apply this rule.

Although the Act doesn't make a distinction between single e-mail messages and bulk e-mail, netiquette does. Generally, netiquette **does** allow you to send single e-mail messages to people. On the other hand, sending bulk e-mail is considered **poor** netiquette unless you have the person's explicit permission. So, in the example above, if you exchange business cards with somebody, netiquette says that it's OK to send them a follow-up e-mail the next day, but **not** to add them to your newsletter mailing list.

I recommend that you only send your customers bulk e-mail if it's **directly** related to products or services that they purchased from you. You can give them the **option** to sign up for, say, a general-purpose newsletter with other news and marketing material, but make it **their** choice, not yours.

Having done business with somebody doesn't **automatically** give you the right to send them commercial e-mail. It still has to be a "reasonable" expectation that there has been consent and a "business relationship". For example, according to the National Office for the Information Economy (a government department that provides guidance to the public), simple one-off transactions, such as buying movie tickets or groceries, are **not** enough to infer consent.

### ***Published addresses***

The Act says that even if you don't have an existing business relationship with somebody, you **are** allowed to send them unsolicited commercial e-mail if they have "conspicuously published" their e-mail address. So, for example, if you find their address on their Web site,

their business card, their brochures, or any other public place, then that's considered to be "inferred consent".

When you think about it, that's a reasonable rule. After all, if somebody has published their e-mail address on, say, their Web site, they **are** expecting to receive e-mail at that address (Otherwise, why publish it at all?)

There are a few restrictions, though, and they are to do with what's reasonable:

- You can only send them e-mail that's related to their work.
- If the published address is accompanied by a statement that explicitly tells you **not** to use that address (for example, the words "no spam"), then you have to respect that choice, and you cannot send them e-mail.
- You cannot use "address harvesting" software to search Web sites automatically in order to extract e-mail addresses. In other words, you can only collect e-mail addresses manually, not automatically.

For example, if a purchasing officer's e-mail address is published on a company's Web site, it's reasonable to assume that potential suppliers can contact that person using that address. But it's **not** reasonable to contact that person with information about, say, home mortgages.

#### NETIQUETTE SAYS ...



Again, netiquette has its say here, because it makes a distinction between single e-mail messages and bulk e-mail. In short, **don't send bulk e-mail without explicit permission.**

In the example above, if you're a potential supplier to the purchasing officer's company, the Act **does** allow you to add the purchasing officer's e-mail address to a bulk e-mail mailing list. **But don't do this** – it's poor netiquette! In fact, you're skating on thin ice if you send them anything more than a very specific e-mail message that could only have been written for that person. Even a generic message that's obviously been mass-produced can get you in trouble with the "Internet police".

## Privacy implications

If your business falls under the requirements of the National Privacy Principles which came into force in December 2001, another rule applies (in addition to the rules above for express or inferred consent):

You can only use an e-mail address for the primary purpose for which it was collected, or a related secondary purpose.

This means that, even if somebody has given you express consent to send somebody e-mail, you can't just send them **any** e-mail. It has to be related to the primary purpose for which they provided their e-mail address, or a related secondary purpose.

This is discussed in more detail in our report *The National Privacy Principles and the Internet*, available from [www.firststep.com.au](http://www.firststep.com.au).

(As an aside, one of the reasons a separate Spam Act was required was because the National Privacy Principles themselves aren't enough to stop spam. For example, a spammer could claim that the primary purpose of collecting e-mail addresses was to send spam!)

## External Mailing Lists

Be especially careful if you buy mailing lists from a third party.

- Did that third party get consent (express or inferred) from the people on the mailing list?
- Even if they did get consent, was it consent to receive the sort of messages you're going to send them?
- And did those people know that their e-mail addresses would be disclosed to you?

Investigate this carefully before using these addresses, and if you're not sure of the answers, it's best not to buy the list.

## Existing Mailing Lists

What about e-mail addresses that you collected **before** the new Act? Are they exempt from the rules for consent?

The answer is: No.

Remember that, as far as consent is concerned, the Act applies to **sending** e-mail, not collecting the addresses. So it applies to any e-mail that you send in the future, even if you're sending it to an e-mail address that you obtained in the past.

The Act is not retrospective with respect to the **messages** that you sent in the past, but it **is** still applicable to **e-mail addresses** you obtained in the past.

So be sure that your old mailing lists are "clean", and that you do have consent from everybody on the lists.

## Sending e-mail

---

Now let's move on to the second area that's covered by the Act: What to do when sending e-mail.

### What *must* be included in a message?

The Act says that any commercial e-mail message **must** have these two things clearly identified:

- A way of accurately identifying the sender;
- A clear method for the recipient to "unsubscribe" from receiving future messages.

We're going to look at each of these in more detail soon. But first let's look at the issue of what's meant by a "commercial" message.

### Is it commercial e-mail?

The Act goes to great lengths to define a commercial message. Essentially, it says that any e-mail message with any promotional content, including a link to a Web site that has promotional content, is a commercial message.

In practical terms, here are some examples:

- An announcement of new products in store (an obvious example);
- A regular newsletter that is mostly informative, but also has a special offer for subscribers;
- A message with an e-mail "signature" (the few lines at the bottom of your outgoing e-mail) that directs people to your Web site;
- In fact, **any** message that has a link to your Web site (or any other Web site that has some commercial content).

You can see that this is a very broad definition. Some of the examples are obvious, but others aren't. For example, many businesses include their Web site address automatically in every outgoing message. This means that they **are** commercial messages, even though the body of the message might be non-commercial.

### ***Non-commercial messages***

The Act says that e-mail messages that are "purely factual" are not commercial messages, and so they are exempt from this part of the Act. For example, if you send a customer an e-mail invoice, or tell them

about your new opening hours, that's not a commercial message, so you don't have to identify yourself or provide an unsubscribe facility.

However, in practice, there's not much point making such a distinction, because you'll probably be using the same method for sending **all** e-mail, even for non-commercial messages.

So don't waste time trying to figure out if a message is commercial or not. Just treat everything as if it is a commercial message, and you'll be safe.

#### NETIQUETTE SAYS ...

The Act says that non-commercial messages don't even require the user's consent, so you're allowed to send such messages to **anybody**.



However, netiquette says something different. Netiquette is about **consent**, not **content**. Netiquette says that sending **any** e-mail to somebody, even if it's non-commercial, requires their consent.

## Identifying the sender

The first requirement for sending e-mail is that you must identify yourself clearly in the message.

The Act doesn't say exactly **how** you have to identify yourself (unlike the American CAN-SPAM law, which requires the identification to be in the From address of the e-mail). Typically, it means you will provide your business name and contact details. It's not compulsory to include your Australian Business Number (ABN) or Australian Company Number (ACN), though the government's guidelines do suggest this as a way of complying with the law.

The exact wording of the Act is that:

"the message clearly and accurately identifies the individual or organisation who authorised the sending of the message; and the message includes accurate information about how the recipient can readily contact that individual or organisation".

If you're sending commercial e-mail already as part of your business, you're probably identifying yourself already, so that's probably sufficient. But check this anyway to ensure that you're doing so.

Again, remember that this applies to **all** your outgoing e-mail, not just your mailing lists. So make sure that you identify yourself appropriately even in single e-mail messages. Most e-mail programs allow you to

create a "signature file" which is appended automatically to every outgoing message. You can add the appropriate identification in your signature file.

### ***30-day minimum***

The identification information you provide must be valid for 30 days. This is to prevent spammers from bypassing the law by registering an e-mail address, sending spam, then shutting down that address and moving on to another address.

This requirement probably won't affect you, unless you plan to move premises soon after sending a message. In that case, make sure that you do provide valid contact details – either by forwarding contacts from the old address or by including both addresses in your messages.

### ***Third-party mailings***

If you use another organisation to send commercial e-mail on your behalf, the Act says that the e-mail message must identify **you**, not the organisation sending the message (It **can** identify them as well if you choose, but it **must** identify you).

## **Unsubscribe facility**

The Act says that every outgoing commercial e-mail message must tell the reader how they can unsubscribe from future e-mail.

It doesn't specify **how** the unsubscribe facility should be done, so the details are up to you. The wording of the Act is that you must have:

"a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the individual or organisation who authorised the sending of the first-mentioned message."

Note that the Act refers to an "electronic address" which must be provided as a means of unsubscribing. This doesn't mean that the unsubscribe request has to be handled automatically at your end, but it does mean that you can't deliberately make it difficult to unsubscribe by forcing the person to, say, send you their request by postal mail.

The other provision of the Act is that the unsubscribe instructions are "presented in a clear and conspicuous manner." This should go without saying for a legitimate business anyway, and the Act now makes this explicit.

Here are some examples you could use:

- "To stop receiving future messages, reply to this message with the word REMOVE in the subject line";
- "To unsubscribe, forward this message in its entirety to remove@example.com";
- "To stop receiving future messages, [click here](#)" (and this leads to a Web page where they can unsubscribe);
- "Click here to manage your subscription or to unsubscribe"

If you operate a regular e-mail mailing list, you probably have an unsubscribe facility in place already.

But again I remind you that the Act applies to **all** your outgoing e-mail. So make sure that every e-mail message you send has an unsubscribe facility, even if it seems silly to offer it for some messages. It's not just a good idea; it's the law.

#### NETIQUETTE SAYS ...

Unfortunately, many experienced Internet users ignore unsubscribe options, unless they are sure that the e-mail is from somebody they trust.



Why? Because smart spammers **do** include unsubscribe instructions in their messages, even though they have no intention of honouring these requests.

In fact, people who do click an unsubscribe link from a spammer might end up with even **more** spam, because the spammer now knows that (a) the person has a valid e-mail address, (b) the spam message hasn't been blocked, (c) the person hasn't recognised it as spam and deleted it, and (d) the person is naïve (or gullible!) enough to trust that the spammer will honour their request.

That's why many people are suspicious of unsubscribe instructions, and why it's so important that you **do** identify yourself clearly, so that people know who they are dealing with.

#### **30-day minimum**

The unsubscribe facility must be working for at least 30 days. Again, as with your identification information, this is to prevent spammers from shutting down their unsubscribe facility soon after sending their spam.

As a legitimate business, this probably won't affect you because your unsubscribe facility will probably be permanent.

This only becomes an issue if, say, you send out a newsletter using one provider and you're transferring your entire mailing list to a new provider. In that case, make sure the old provider's unsubscribe facility is still working for at least 30 days after you send your last message using that provider.

***Exceptions***

There is an important exception: You do not have to provide an unsubscribe facility if you have an existing agreement with the recipient that overrides this requirement.

For example, if somebody agreed to receive a certain amount of promotional e-mail from you (say, once a week) in return for free or discounted services, then the on-going commercial e-mail is part of an existing agreement, so the Act doesn't force you to provide an unsubscribe facility. If there's a dispute, it's up to you to prove that this agreement exists, so make sure you've got it in writing!

---

## Managing the e-mail addresses

---

The third main component of the Act ensures that you manage your database of e-mail addresses properly.

In simple terms, the Act requires that you remove people from your database when they request it.

This sounds simple and straightforward, and in most cases it is. There are just a few specific things to remember, and we'll cover them here.

### ***Removing people on request***

The Act does require that you take action for every unsubscribe request. Even if you offer a method for people to remove themselves from your mailing list, if they ignore that method and contact you directly, you do have to remove them from the list yourself.

This is just common sense, and I would recommend that anyway. However, I **have** seen mailing lists where the list owner flatly refuses to unsubscribe people from their list manually, insisting that they use the automatic unsubscribe facility. To me, this is just plain stupid. When you've got somebody who doesn't want to receive any further e-mail from you, why antagonise them further by sending them another message telling them to follow **your** rules for stopping future e-mail? It's just common sense to remove them from the list yourself. And from 10<sup>th</sup> April 2004, it's the law.

### ***Mismatched e-mail addresses***

Occasionally, a subscriber to your mailing list will ask to be unsubscribed, but you won't be able to find their e-mail address in your list, because their subscription address is different from the address they used to send the unsubscribe request.

Sometimes this is easy to resolve; at other times, it's not so easy. Strictly speaking, the Act **does** require you to find them and unsubscribe them, so I'll give you some guidelines here on how to find their address.

First, check the body of the unsubscribe request that they sent to you. Sometimes they simply reply to you, including the original message that you sent them, and that original message might identify their address. If so, you're in luck, and you can unsubscribe them, and skip the rest of this section.

Next, consider that sometimes the addresses are very similar, even though they might not be exactly the same. So even though you can't find the **exact** address in your database, you can find it by searching for **part** of the address. For example:

- Some mail servers insert "mail." or "smtp." into an e-mail address. So somebody subscribes as fred@example.com, but their unsubscribe request comes from fred@mail.example.com.
- Some companies register two (or more) domain names, with matching e-mail addresses for both names. For example, somebody subscribes as fred@example.com, but their unsubscribe request comes from fred@example.com.au.
- Some companies set up multiple aliases for people within their company. For example, somebody subscribes as JohnSmith@example.com, but their unsubscribe request comes from jsmith@example.com.

Those are the easy cases. It gets more complicated if you try these things and they still don't turn up a match.

Next, it's possible that the person has two e-mail addresses. The only way to know for sure is to ask the person, so write back to them and ask.

Another possibility is that the person has changed their e-mail address since they subscribed, and has forwarded e-mail from their old address to their new address. Again, the only way to know for sure is to ask.

If you do have to ask them for help, be sincere and apologetic. Remember that they don't really want to hear from you any more! So explain that you've searched your database, can't find their address or anything like it, and you'd like their help in finding their address so that you can remove it. Don't be brusque or off-hand; otherwise they'll think that you're a spammer who has no real intention of removing them from your list. It's **your** responsibility to remove them from your list, so the law is on their side.

### ***Five-day turnaround***

The Act says that you must honour unsubscribe requests within five working days.

If you have an automatic unsubscribe facility, this isn't an issue, because people will be removed from your list immediately when they unsubscribe.

However, if you have to remove people from your database manually (and in most cases, you **will**, because people can unsubscribe from

receiving your normal e-mail messages, not just your mailing list messages), it gives you a five-day grace period.

For example, you could have a standard procedure where you handle all the unsubscribe requests every Monday morning. That relieves you of the burden of having to handle every unsubscribe request immediately, just in case you're sending them e-mail later in the week.

Even though the Act gives you a five-day grace period, most people won't know this. Some will expect you to unsubscribe them immediately, and will get upset if you send them further e-mail within those five days. To prevent this from happening, when you tell people how to unsubscribe, set their expectations clearly by also saying "All unsubscribe requests are processed within 5 working days", or something along these lines.

#### NETIQUETTE SAYS ...

There is no "standard" grace period that's been established for unsubscribing people from your e-mail database. Most people do expect you to honour their unsubscribe requests immediately, and will be surprised to receive any further e-mail from you. Even if you tell them that there might be a delay, a few **will** still get upset with you.



So I recommend that you do whatever you can to remove people from your database as soon as possible. If it's relatively easy to remove somebody from your database immediately, do so. Or if you can do it daily rather than weekly, do so. Anything you can do to reduce the delay is worth doing, and keeps you squeaky clean and free from any possible complaint.

I know that this is a small point, but it's an important one, because the people who are most likely to complain about you are those who've **asked** you to remove them from your database but still receive e-mail from you.

## Penalties

---

For completeness, I'll include a brief summary of how the Act will be policed, and the penalties for breaking the law – though I hope you will never have to worry about this!

The Act gives the Australian Communications Authority (ACA) the responsibility of enforcing the provisions of the Act.

The ACA can take action against alleged spammers in three ways:

- Issue a **formal warning**, which could typically be done if the ACA decided that the spam was sent by mistake;
- Issue an **infringement notice**, which carries a financial penalty;
- Initiate **court proceedings**, which also carry a financial penalty if the person or organisation is found guilty.

The financial penalties are deliberately set high, to discourage spammers. For example, an infringement notice carries a maximum penalty of \$22,000 per day for individuals or \$110,000 for companies. If it goes to court, the court can hand down even more severe penalties – up to \$44,000 per day for individuals and \$220,000 for companies. Past offenders can be fined up to five times that amount.

The Act **is** tolerant towards honest mistakes, with clauses that excuse people who send spam by mistake. However, it still puts the burden of proof on you to prove that it was a mistake.

It's expected that the ACA will issue a lot of formal warnings – rather than infringement notices or court orders – especially in the early days of the Act, when organisations are still learning about it. However, you certainly shouldn't rely on the ACA being lenient. Get it right **now** so that the issue doesn't even arise later.

## More Information

---

### The Spam Act

These Web sites are useful for further information about the Spam Act and related laws:

- The National Office for the Information Economy (NOIE), at [www.noie.gov.au](http://www.noie.gov.au), carries comprehensive information about the Act and its implications for organisations.
- The Privacy Commissioner's Web site, at [www.privacy.gov.au](http://www.privacy.gov.au), has information about the privacy requirements when sending e-mail.
- As mentioned earlier, you can also obtain our special report *The National Privacy Principles and the Internet* from [www.firststep.com.au](http://www.firststep.com.au).

If you'd like to see the Spam Act itself, you can download and read it in all its gory detail from the Attorney-General's Department's Web site:

- [scaleplus.law.gov.au/html/comact/11/6735/rtf/1292003.rtf](http://scaleplus.law.gov.au/html/comact/11/6735/rtf/1292003.rtf)  
(the Spam Bill itself)
- [scaleplus.law.gov.au/html/ems/0/2003/0/2003092501.htm](http://scaleplus.law.gov.au/html/ems/0/2003/0/2003092501.htm)  
(Explanatory Memorandum)

### Netiquette

By its very nature, the rules of netiquette are not set in stone. However, you can search Google [www.google.com](http://www.google.com) for various Web sites that talk about netiquette.

One of them is "RFC 1855", which is about the closest thing you'll get to an "official" document about netiquette:

- [www.dtcc.edu/cs/rfc1855.html](http://www.dtcc.edu/cs/rfc1855.html)