Spamming and the law

This information is provided by the Entrepreneur Business Centre. For small business products and services, visit www.ebc.com.au.

Spamming is Internet slang for unsolicited e-mail, mostly advertising or commercial e-mail. It is effectively electronic junk-mail, just like the unsolicited mail you receive in your letterbox. And just to clear up any possible misinterpretation, spam is also a canned meat product, which is sold under the Hormel trademark.

According to a number of sources, using the term "spam" to describe unsolicited e-mails derives from a Monty Python restaurant sketch in which Spam is included in every dish. However, there really isn't a funny side to spamming. Most people who receive this type of bombardment regard it as a major intrusion.

Spamming - an annoying practice

Spamming is a cheap alternative to sending out information rather than paying for bulk mail-outs. An advertiser could spam about 10,000 recipients for much less that paying for 10,000 stamps and the result is instant.

However, spam is costly for Internet Service Providers (ISPs) as it clutters the ISP’s net space. This slows down the user’s internet access, so the ISP must pay to install filtering software.

Hence, spamming is viewed by ISPs as annoying as it can block and slow computer systems. They also do not want their name associated with this spam, particularly if the spammer is using the ISPs name in the e-mail address, such as advertising@bigpond.com. Some providers will cut off service to spamming customers.

Fraudulent business schemes, chain letters and offensive sexual and political messages are also quite often linked with spam.

Not all spam takes the form of bulk e-mail though. Some regular e-mail is based on the subscriber's permission to receive it.

If a consumer has requested the information, this is not spamming and rarely is spam sent directly by an advertiser. Online marketing companies, specifically set up to spam, are usually the main culprits.

Software programs known as "harvesters" pluck names randomly from Web sites, newsgroups and other services. To protect against e-mail address harvesters, a "poison", in the form of specially designed software, is available. This "poisoned" software, for example, generates bogus e-mail addresses or directs the harvester to a nonexistent site.

The legal ramifications

There are a number of government policy directives and industry codes, which do carry some weight when it comes to the law and spamming.

There is no specific law governing the use of spam, however penalties can apply for breaching the industry codes.

In particular, the Federal Government’s new e-commerce best practice model and the National Privacy Principles can be used as blanket principles applicable for most online businesses.

In 2000, the Federal Government launched electronic commerce guidelines for business titled "Building Consumer Sovereignty in Electronic Commerce (A Best Practice Model for Business)".

While the document is not automatically binding, the government is encouraging businesses and industry associations involved in e-commerce to adopt the Best Practice Model.
The document is clear on its stand that spamming is not acceptable. When it comes to commercial e-mail the document states:

"Businesses should not send commercial e-mail except:

• to people with whom they have an existing relationship; or
• to people who have already said they want to receive commercial e-mail
• Businesses should have simple procedures so consumers can let businesses know they do not want to receive commercial e-mail."

The Federal Government has also introduced legislation based on the National Privacy Principles, the Privacy Amendment (Private Sector) Act 2000.

The new provision, set out in the Bill, came into effect on December 2001 for organisations holding health information. Smaller businesses, which are not involved in the health sector and have an annual turnover of less than $2 million, have an additional 12 months to December 2002 to come under the new provisions.

The Act regulates the way private sector organisations collect, keep, secure and disclose personal/consumer information. A consumer now has the right to know what a private sector organisation is collecting. Consumers can make a complaint if they think their information is not being handled properly.

They can apply to the Federal Court or the Federal Magistrate’s Court for an order to stop an organisation from engaging in conduct that breaches the National Privacy Provisions (www.privacy.gov.au/publications/).

The Australian Direct Marketing Association Code of Practice also enforces its code and non-members can be ordered to comply with the code.

E-mail communication is part of the Australian Federation of Advertisers privacy guidelines and calls for strict opt-in choices for consumer e-mails.

Industry stand on spamming
The Internet Industry Association Code of Practice (www.iia.net.au) also is a watchdog for online merchants and provides guidelines for businesses.

• IIA members and code subscribers must not spam and must not encourage spam, with exception of pre-existing relations or acquaintance spam.
• IIA members and code subscribers who use acquaintance spam must provide recipients with the capability to opt-out and must include the opt-out instructions in the spam.
• IIA members and code subscribers must not send even acquaintance spam containing prohibited content (prohibited content is mostly pornographic in nature).
• IIA members and code subscriber ISPs should have Acceptable Use Policy that prohibits spam and further prohibits services that depend on spam.
• ISPs should have a working contact address for spam complaints.
• ISPs should install relay protection on their mail servers, to prevent spammers from using the relay to evade detection or penalty.

According to the Australian Coalition Against Unsolicited Bulk E-mail, (www.caube.org.au), Australia secured its first conviction in relation to spamming in November 2000.

The offender faced charges for relaying spam off third party computer systems without permission.

The offender was charged under Section 76E of the Commonwealth Crimes Act 1914 (which carries a maximum penalty of 10 years imprisonment). The CAUBE campaigns to stop spamming and to tighten regulations and laws regarding the practice.
**Spamming "dos"**

When a customer’s e-mail address is given it is usually for a reason. Make sure you use that customer’s e-mail address only for that specific reason.

Other "spamming" dos to consider:

- When asking a customer whether they are willing to receive regular mailings it is important to make sure you give them a choice. A good way to do this is via a check box on an e-mail format. The customer is then asked three basic questions:
  1. Subscribe me to the newsletter
  2. Send me critical notices/information only (this is for important information that may have a direct impact on them or their ability to use your service)
  3. Don’t send me announcements of any kind.

If you are going to use a check box system make sure you have the software in place to only allow the check box to be e-mailed back after it has been touched. You should also have the subscribed box ticked as your default. That then forces the customer to make a choice.

There are quite a few ways of keeping in touch with current customers and scouting for new ones without resorting to spamming.

- Ask people to subscribe to a newsletter via a sign-up form available on your website. Make sure you explain that you will only send informative and timely e-mails to subscribers.
- Include late breaking, useful information in the e-mail you send to your subscribing customers. Package it with enough informative information so the subscriber will feel happy about the information and not view it as junk mail.
- Make it easy for customers/subscribers to quit receiving e-mail. Every message should include brief instructions for getting off your mailing list.

**What not to do**

- Try to avoid sending e-mails to a large group of people you don’t know. They may rub potential customers the wrong way. They may think you will keep "badgering" them until they are willing to commit to buying your products. In effect, it could scare them away, which was not the intention of your original e-mail.
- If you decide to e-mail a large number of people who weren't expecting it, even if they are your customers who have ordered from your Web site in the past or willingly given you their e-mail address, it may be perceived by some of the recipients as spamming. In fact, it is. This is acquaintance spam. There is unlikely to be a law against this kind of spamming, but done consistently it could lose you customers.
- The general perception in the cyber community is that spam is downright annoying and an invasion of privacy. If someone e-mails you telling you to stop sending them information, do it.

This information is provided by the Entrepreneur Business Centre. For small business products and services, visit [www.ebc.com.au](http://www.ebc.com.au).

Disclaimer: All material on the Small Business Site is provided as a general information service only and should not be relied upon as a substitute for the advice of a properly qualified professional. ninemsn does not assume or accept any responsibility for, and shall not be liable for the accuracy or appropriate application of any information on the site.