

Spamspamspamspamspamspam The law responds

Dr Alan Davidson

We all receive junk email. Sometimes it is humorous or helpful.
Mostly it is an unwelcome nuisance.

Sspam can be offensive, intrusive, misleading and an invasion of privacy. It clogs mail boxes, obscures legitimate emails and slows down email systems. It is also costly, due to both increased download times and lost productivity.

THE PROBLEM

According to Star Internet, a large internet service-provider in the UK, the cost in lost productivity is A\$915 per employee each year.¹ Other studies suggest this figure may be conservative. A European Union study in 2001 estimated that the worldwide cost of spam is approximately A\$18.4 billion,² while Ferris Research estimates that US companies lost US\$8.9 billion in 2002.³ Conversely, for the spammer it can cost as little as 0.003 cents to send a single email, and only 0.00032 cents to obtain one email address using appropriate harvesting software. Positive responses from less than 1% of the 'mail out' can prove profitable for the spammer.⁴

The origin of the word 'spam', according to a number of reputable dictionaries, stems from a comedy routine by Monty Python. In the routine, the word 'spam', meaning the tinned processed meat product available in supermarkets, is used continuously and ludicrously to the point of monotony. The use of the word to refer to the continuous stream of nuisance email was coined by persons unknown (but no doubt Monty Python fans).

THE SPAM ACT 2003

In 2003 the federal government gave credence to the word, by passing the *Spam Act 2003*. Curiously, the word 'spam' does not appear in the body of the Act, except for the title

section. A more accurate, but cumbersome title could have been the 'Unsolicited Commercial Electronic Messages Act'. The Act was passed on 12 December 2003; however, its operation was deferred for 120 days, until 10 April 2004, to allow affected parties to change their email practices so that they would not fall foul of the Act.

The Act sets up a scheme for regulating commercial email and other types of commercial electronic messages. Its main provisions are set out below.

Unsolicited commercial electronic messages must not be sent.

A person must not send, or cause to be sent, a commercial electronic message unless the recipient has consented. Consent can be inferred from an existing business relationship. Further, a person is deemed to consent to spam if their email address has been 'conspicuously published'. Note that the term 'message' is used rather than email, so that the legislation extends to other electronic communications, such as SMS messages.

Commercial electronic messages must include information about the individual or organisation who authorised the sending of the message.

All commercial electronic messages must:

- clearly and accurately identify the person who authorised the sending of the message;
- include accurate information about how the recipient can readily contact the sender;
- comply with the regulations; and
- be reasonably likely to be valid for at least 30 days after the message has been sent. >>

Commercial electronic messages must contain a functional 'unsubscribe' facility.

All commercial electronic messages (solicited and unsolicited) must include the statement that the recipient may unsubscribe by replying using an electronic address that must be set out in the message. The statement must be presented in a clear and conspicuous manner and the electronic address must be reasonably likely to be capable of receiving for a period of at least 30 days after the message is sent. In addition, the section requires that the electronic address was legitimately obtained. An 'unsubscribe' message is defined as an electronic message to the effect that the relevant electronic account-holder does not want to receive any further commercial electronic messages from the sender.

Address-harvesting software must not be supplied, acquired or used.

Likewise, an electronic address list produced using address-harvesting software must not be supplied, acquired or used.

ENFORCEMENT

The main remedies for breaches of this Act are civil penalties and injunctions.

The Act anticipates a tiered enforcement regime available to the Australian Communications Authority (ACA), including:

- a formal warning;
- acceptance of an enforceable undertaking;
- the issuing of an infringement notice;
- application to the federal court for an injunction; and
- the commencement of proceedings in the federal court for breach of a civil penalty provision.

Courts will be able to compensate businesses that have suffered from spamming and are able to recover profits from spamming.

SEARCH AND SEIZURE

A second Act, the *Spam (Consequential Amendments) Act 2003*, makes amendments to enable investigation and enforcement of breaches of the *Spam Act*. The amendments make it legal, in certain circumstances, for inspectors and police to enter homes and search and seize computers and other possessions without a search warrant and without the consent of the person whose home was entered.

EXEMPTIONS

The Act exempts Australian and foreign government bodies, political parties, religious organisations, and charities and educational institutions in certain circumstances.

The greatest weakness in the legislation is the exemption for sending 'factual information'. The Act does not regard email as spam if it contains factual information (with or without directly related comment) and additional peripheral information such as the sender's name, logo and contact details.

'Factual information' is not defined in the Act. However, the explanatory memorandum states that the provision is designed 'to ensure that messages which may be seen to have

some form of commercial element, but which are primarily aimed at providing factual information, are not covered by the rules'. The explanatory memorandum cites the following examples:

- an electronic message from a private law firm which includes an information sheet outlining the effects of a particular court decision. While the message may be designed to promote the interests of the private law firm, however, 'the messages primary intent is to provide factual information';
- an electronic version of a neighbourhood watch newsletter, which is sponsored by the local newsagent;
- an electronic newsletter from the local chamber of commerce, which is sponsored by one of their members; and
- an e-mail message promoting a birdwatching enthusiasts' website with a link to the website, where the website provides purely factual information relating to birdwatching but is sponsored by a commercial entity.

CRITICISMS

The Act bans some emails that many would not regard as spam. For example, if you publish an article, a single unsolicited email asking that the article be reprinted elsewhere for a fee would be a contravention. Critics also argue that no single email should be regarded as spam.

Conversely, the Act legitimises some email that all would agree should be regarded as spam. Using the 'factual information' loophole, a car dealer could send bulk emails stating the name and address of the dealer and that the latest model is now available.

Using the 'conspicuous publication' rule, if I publish my email address at the bottom of this article (which many writers do), I would be regarded as consenting to all spam. To avoid this, the legislation requires the addition of words such as 'legitimate correspondence only – no spam'.

Concerns have also been voiced about the lack of need for a warrant in the search and seizure requirements.

Further critics point out that the legislation will be ineffective against overseas spam. It is estimated that some 80-90% of all spam comes from overseas.

THE POSITION OVERSEAS

The US federal anti-spam legislation, known as the 'CAN-SPAM Act', became law on 1 January 2004. The Act requires senders of unsolicited email advertisements to include an 'opt-out' facility. The opt-out provision may be a reply e-mail address or an 'internet-based mechanism'. These emails must be identified as advertisements.

Recipients cannot bring civil action; instead, law enforcement authorities and internet service-providers can initiate civil actions on behalf of recipients to recover up to \$2 million in damages. The sending of multiple commercial e-mails with misleading headers, or which conceal the identity of the sender, are prohibited and attract significant fines or even imprisonment.

In contrast, EU 'marketing' emails may be sent to recipients who have not given specific consent. However, recipients may opt out after a ten-day grace period.

The EU Privacy and Electronic Communications Directive was implemented in EU member states on 31 October 2003. The Directive prohibits unsolicited direct marketing to individuals by electronic communications, including email, unless consent has been given in advance. There is an exemption for an existing customer relationship, where companies may continue to market products by email on an 'opt-out' basis. The UK version of the Directive became operative on 11 December 2003.

COULD YOUR CHRISTMAS EMAIL GREETING BREACH THE SPAM ACT?

Whether your Christmas greeting amounts to spam will depend upon whether the email is regarded as commercial or not, and whether or not one could argue that the recipient – if they are on a customer list – consented. Section 6 defines a commercial electronic message as one where, having regard to (a) the content, (b) the presentation, and (c) the content that can be located using links, telephone numbers and contact information, it would be concluded that one of the purposes of the message is an offer, advertisement or promotion of goods or services. In addition, the message is commercial if it assists or enables a person by a deception to

appropriate property, a financial advantage or a gain from another person.

CONCLUSION

While the *Spam Act* is particularly relevant to those who are involved in advertising and marketing activities, its terms are such that any electronic communication could potentially fall foul of its provisions, and so care must be taken whenever entering into such forms of communication. Specifically, all organisations should ensure that their email policy complies with the legislation in the recipient's country as well as the country of origin and ascertain if the recipient has opted out of receiving advertising by email. ■

Notes: **1** <http://www.star.net.uk/star/home.shtml> **2** European Commission, Unsolicited Commercial Communications and Data Protection (Internal Market DG – Contract no ETD/99/B5-3000/E/96) Serge Gauthronet, Etienne Drouard, January 2001. **3** 'Spam Control: Problems and Opportunities': <http://www.ferris.com/offer/spam.html> **4** IBM Almaden Research Centre: <http://www.almaden.ibm.com/>

Dr Alan Davidson is senior lecturer in law at the TC Beirne School of Law, University of Queensland. **PHONE** (07) 3365 2294

EMAIL a.davidson@law.uq.edu.au

losing sleep?

Changing obligations in compensation cases can cause plaintiff lawyers to lose sleep. How can you do the right thing by your client, and be thorough and efficient? This is where ipac can help. In one hour learn how we can:

- ~ assist your client to maximise their compensation
- ~ ensure you understand the impact of the OPC's new fee regime
- ~ compare private and public solutions
- ~ put your clients in a position of informed choice
- ~ help you satisfy your obligations under FSR
- ~ deliver better outcomes for your clients for the long term

It's one hour that costs you nothing and there are no strings attached. Don't lose more sleep, call us to find out more **1800 262 618**.

Jane Campbell is a financial adviser at ipac who specialises in personal injury compensation. Jane previously worked as a compensation lawyer and lobbied for many years to improve tax and financial outcomes for plaintiffs.



ipac securities limited ABN 30 008 587 595 AFS Licence Number 234656

