

# What the *Spam Act* means for Australian businesses

(...and what you need to know to be compliant with the Act)



**Ivan Trundle**

Manager, publishing  
and communications  
ivan.trundle@alia.org.au

In last month's *inCite*, my regular technology article discussed the various legislative attempts that have been implemented around the world. I also mentioned that, in my view, no legislation is likely to reduce spam — at least until the spammer in each instance is properly identified and brought to trial.

The legislation that will be introduced on 11 April 2004 in Australia will have an impact on people who send genuine e-mails as part of their business. Communicative business-related e-mail must now not only be written to avoid being labelled spam by the various spam-detecting algorithms, but also to clearly demonstrate to the user that the e-mail is genuine, important, and worth reading — and above all, compliant with the imminent *Spam Act* and *Spam (Consequential Amendments) Act*.

The Act prohibits the sending of unsolicited commercial electronic messages, but is subject to a handful of exceptions. Those exceptions are unusual in themselves, but before delving into what they might be, let's look at what businesses must consider when sending e-mail to individuals:

1. The recipient must have given prior consent to the message. This consent can be express or implied, which is where it gets tricky, since the mere act of 'conspicuous' publishing of your e-mail address (such as in e-list archives on the net, or in places that I would not normally consider as 'giving consent') is enough. Having conducted any prior business with the sender is enough, as well.
2. The e-mail must include a 'functional unsubscribe facility' — which is awkward, since the recipient might not have been subscribed in the first place, but one should interpret this sloppy legislative writing by the intent: the recipient must be able to opt out of further mailings. Not that this precludes other businesses from using the data.
3. The e-mail must include accurate information that identifies the sender. No argument there, although the amount of spam that I receive means that I rarely venture into the message itself, and only read the 'From' and 'Subject' lines (the former of which can easily be forged). The mere act of actually reading the 200 or more spam messages that I get per day makes it impossible for me to contemplate trying to identify the sender via these means. However, in all fairness, legitimate businesses in Australia should have no trouble in complying with this.

I mentioned exceptions: not at all surprisingly, those who lobbied the government had a say in the drafting the legislation. Therefore,

messages from government bodies, registered political parties, registered charities, religious organisations and educational institutions (when contacting alumni) and so-called 'purely factual messages' are all exempt from both the consent ruling, and the opt-out requirements. Sigh.

Those businesses or individuals who do not comply with the above rules will find themselves in line for prosecution, to the tune of up to \$1.1 million per day, and the Act empowers the Federal Court to take out injunctions against those who breach the Act.

I doubt if many Australian businesses will be too much troubled by the impending legislation, and it will not trouble genuine spammers either. In the real world, spammers have plenty of tools at their disposal to get their messages across, with relative ease and impunity.

Even Microsoft has stepped into the ring, declaring that all spam will be beaten in two years time. Wishful thinking, and entirely reliant on Microsoft's ability to control the world (and use the recently-patented anti-spam system that it has just developed). In other words, it will not happen. The inability to stop spam is because of the underlying transport mechanism. Firstly, it is insecure, and easily forged. Bill Clinton, ex-president of the United States, has only ever sent two e-mail messages — one of which was an internal message — and yet there are millions of messages purportedly written by bill.clinton@whitehouse.gov (any mail half-reasonable administrator can show you how to spoof addresses), and secondly, mail is charged per byte received. This is highly unlikely to change either — and no scheme for charging to send mail will possibly work until the underlying security is resolved (in other words, if I can spoof your address — and send you the bill for allegedly sending messages around the world — then there is no way that you, or the wider community, would accept paying to send mail that you really did not send).

In all, the spam problem is complex, but legislation should be driven to resolving the issue (technical resolution is not possible for quite a while to come). What baffles me is why international legislation is not enacted universally that penalises the business or person that sends spam, as identified in the spam. Perhaps international courts are too busy on free trade deals and catching war criminals to bother with such trivial affairs. Until the legislators and politicians are as overwhelmed with spam as we are, little movement will occur. ■

*I doubt if many Australian businesses will be too much troubled by the impending legislation, and it will not trouble genuine spammers either...*