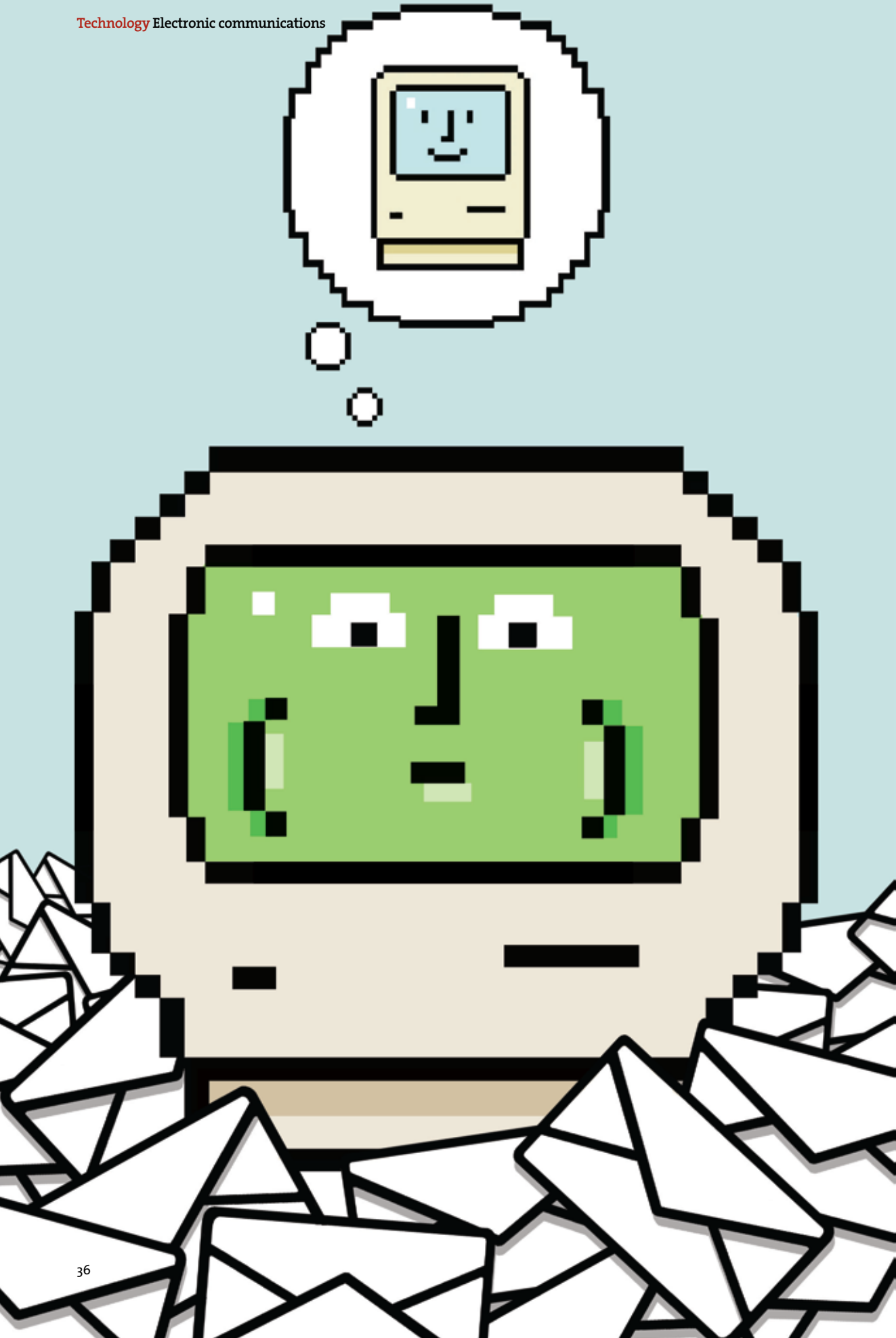

Can Spam

Anyone with an email account would acknowledge there is a significant and growing spam problem. *Mark Bender* looks at how our legislation aims to deal with it.

Illustration by Steven Moore

Email has been described as the 'killer application' of the internet, not because of how lethal it may be but because of its compelling usefulness and immense value, but its efficiency is being undermined by the insidious scourge of unsolicited commercial email (UCE), or spam.

It has been suggested that the volume of spam 'threaten[s] the effectiveness and efficiency of electronic communication and legitimate online business' and is 'tearing at the very fabric' of the internet.

The National Office for the Information Economy (NOIE) cites data estimating that in 2005, 50 per cent of all inbound business emails were spam. The cost to Australian businesses was estimated in 2005-06 at $900 per employee per year or more than $9.5bn for the country's 10.605 million employees, according to the Australian Bureau of Statistics (ABS).

The *Spam Act 2003* ("The Act") was introduced to cover internet-based messaging – email and instant messaging (IM) – as well as mobile phone-based messaging – short message service (SMS) and multimedia message service (MMS). Responsibility for the enforcement of the Act rests with the Australian Communications and Media Authority (ACMA). Australia's Act has adopted an 'Opt-In' approach which requires the consent of the receiver before sending any messages to them. In contrast, the US legislation has taken an 'Opt-Out' approach, requiring the recipient of an unsolicited message to specifically request removal from the sender's database and that such requests are acted on by the sender in refraining from sending messages in the future.

Penalties for contravening the Act can range from formal warnings and infringement notices to fines to business of up to $220,000 for a single day's contravention, or up to $1.1 million for a subsequent contravention.

In June 2006, the Department of Communications, Information Technology and the Arts published a review of the 2003 Act after receiving submissions from a wide range of industry, consumer and government groups. Of the recommendations relating directly to spam, the status quo was effectively proposed to be maintained.

Recommendations were also accepted to maintain other non-legislative measures, so that domestic education programs, directed to businesses and consumers, will be maintained and international cooperative efforts will be increased.

Some issues with the Australian legislative approach are:

Spam largely originates outside Australia: Former Attorney General, Daryl Williams, encapsulated the problem when he said: "Enforcement of the new law against overseas-based spammers will be dependent on the cooperation of other jurisdictions." Only around 2 per cent of spam is generated in Australia. Recent US actions against spammers are likely to drive them offshore to jurisdictions where there is less regulation, rather than deter them altogether. Growth in spam is expected from China and India as more of their populations come online. Relying on domestic legislation alone (even if coupled with other 'soft' measures, such as education), and indeed any unilateral legislative-only approach

taken by other national governments, will obviously not be a solution in isolation.

Adequacy of penalties to act as effective deterrent: The *Spam Act 2003* provides for civil rather than criminal penalties, allowing infringement notices to be issued followed with applications for injunctions, civil penalty provisions and seizure of equipment. However, the Government's 2006 review of this Act noted that spam levels continued to increase significantly. As of October 2006, ACMA had issued 13 fines to five companies and individuals, conducted one successful prosecution under the Act and issued three warning letters for less serious breaches. Would harsher penalties act as more powerful deterrents? Some jurisdictions (Italy and the US) provide for imprisonment in their legislation. Nevertheless, given the global nature of the problem, any deterrent effect is likely to shift the sending of spam to other jurisdictions as mentioned above, further reinforcing the need for global responses to the problem.

Exceptions provided for by the Act: The Act provides for certain exemptions from its prohibitions such as designated commercial electronic messages (DCEMs) (messages from charities, political parties, governments and religious groups) and factual messages that include the logo and address of the sender if such messages would not have been commercial in nature if they did not contain the logo and address. It is suggested that this provision, at worst, could permit spam from many commercial senders and at best will remain an unclear provision, giving rise to much difficulty in distinguishing between exempt factual DCEMs and prohibited commercial messages.

Certain provisions of the Act may undermine the Opt-In principle, notably the conspicuous publication provision which effectively deems consent for messages relevant to work-related business, functions or duties of an employee, if the address has been conspicuously published and the publication is not accompanied by:

(i) A statement to the effect that the relevant electronic account holder does not want to receive unsolicited commercial electronic messages at that electronic address; or

(ii) A statement to similar effect.

For example, spammers frequently make tantalising offers of career enhancing academic qualifications without any classes, lectures, assessment or theses. Under this loophole, any recipient whose functions or duties could be enhanced by a bogus doctorate or masters degree and who had not appended a no-spam disclaimer when their address appears on their employer's website would be fair game for spammers. Clearly this is a completely unsatisfactory situation and may possibly provide some indication of the power of the pro-marketing lobby group during the consultation process that preceded the drafting of this Act. The relevance of the message to the recipient again seems to introduce a murky test that will presumably require clarification by the courts.

The 2006 Review of the Spam Act did consider the matter of the exceptions for certain senders and messages in the Act and the decision was made that they remain unchanged.

No grounds for civil action under the Act: The Act does not provide grounds for civil action by individuals or corporations against spammers. The ACMA is the only party with such standing to bring actions. The importance of this issue has been highlighted by the OECD Task Force on Spam.

In the US there is a legal doctrine, not presently accepted in Australia, known as trespass to chattels. This doctrine can provide redress for individuals or corporations for conduct where unauthorised interference or use of property, including computer systems occurs, if such action results in actual injury.

Spam Slam

The first case to be brought under the *Spam Act 2003* was in 2005 against West Australian company, Clarity1, and its director, Wayne Mansfield. The ACMA alleged Clarity1 had sent 56 million unsolicited email messages, harvested email addresses and not obtained consent from email address account holders. The penalties awarded were $4.5m against Clarity1 and $1m against Mansfield and took into consideration: the nature and extent of the contraventions, the loss or damage caused, respondents' financial position and capacity to pay and the appropriateness of the penalty.

The spammer in this case raised a number of unsuccessful arguments in their defence, including:

- That they could infer consent from recipients' failure to respond – the court held that no such consent could be inferred
- That the services promoted related to education/training and so fell under the education exemptions in the Act – these clearly only apply to recognised institutions communicating with former/current students about their courses of study

Resources allocated to the spam problem have been increased in subsequent budgets, including increases in the 2007-08 Budget, although information as to specific operating budgets for spam counter-measures are not publicly available.

- That there was a business relationship with the recipients, based on the fact that the recipients had not unsubscribed to previous messages – the court holding that non-response to unsolicited messages could not constitute a business relationship
- That recipients had conspicuously published their addresses and messages related to their employment – there was inadequate evidence to support this claim and evidence to the contrary in a number of instances.

There have been successful private actions brought against spammers in other jurisdictions under anti-spam legislation and other law. As the OECD Task Force on Spam points out, the availability of private actions against spammers needs to be coupled with an appropriate legal framework for determining and facilitating restitution of costs to damaged parties.

Adequacy of resources to support the Act: The ACMA has been charged with administering the Act however the funding allocated to administer the Act may seem somewhat disproportionate to the extent of the problem. The Minister at the time the Act was introduced, after stating that spam costs $900 per employee per year suggested that 'this bill shows the Government is serious about addressing the problem'. However, only $300,000 was allocated in the first year of the Act to combat an $8.5 billion dollar (at the time) pandemic.

Resources allocated to the spam problem have been increased in subsequent budgets, including increases in the 2007-08 Budget, although information as to specific operating budgets for spam counter-measures are not publicly available. The 2007-08 Budget also provided funding of $73.6 million over four years to a range of agencies for an e-security national agenda to 'be implemented to secure Australia's online environment and the critical infrastructure it supports, such as ...telecommunications systems'. Some of this funding will support the Australian Internet Security Initiative (AISI).

One novel approach unsuccessfully proposed in the US to overcome resource constraints was a bounty system to entice highly-skilled specialists to be involved in identifying spammers through technical investigations by offering a portion of the penalities paid by spammers as a reward.

Obligations on the ISP industry: The consultative process leading up to the Act's drafting included heavy involvement by internet industry groups, notably the Internet Industry Association (IIA). The Act as presently drafted does not directly place any liability on Internet Service Providers (ISP's), however, there are two codes of practice which have been developed and registered in relation to spam.

The Australian eMarketing Code of Practice establishes rules and guidelines for the sending of commercial electronic messages (CEMs) in compliance with the Act and provides a framework by which industry can deal with complaints about spam and monitor compliance with the provisions of the code.

As a result of the code being registered by ACA (ACMA's predecessor), compliance with the code is mandatory and enforceable by the ACMA.

The code applies to all individuals and organisations who are undertaking an eMarketing activity, regardless of whether they are signatories to the Code or members of a recognised industry body. EMarketing Activity is defined in the *Telecommunications Act* to cover activities undertaken to market, promote or advertise its own goods and services, or those of another party, where sending or causing to send commercial electronic communications.

The Internet Industry Spam Code of Practice was the first such legislative code of practice in the world for service providers and applies to all ISPs, Email Service Providers in Australia, and also those located outside Australia who provide services in Australia. There are a range of obligations on providers including:

- To provide subscribers with information about how to minimise spam and their obligations to comply with the *Spam Act 2003*
- To provide spam filtering options to subscribers
- To ensure that their Acceptable Use Policies prohibit the use of their networks for spamming
- Not to have open relay or open proxy servers

- To retain the right in their Acceptable Use Policies to scan their own networks for subscribers' misconfigured mail and proxy servers
- To comply with certain standards in relation to spam complaints and to have documented complaints handling processes.

While the code recognises 'that action must be taken by Service Providers to assist with the minimisation of Spam, and the detriment caused by Spam', following the 2006 review of the Act, DCITA's recommendation is that further obligations not be placed on ISP's to do more to combat spam under the Act.

There has been collaboration between ISPs and the ACMA in relation to a technical and educative countermeasure program, the AISI. This program was instigated as a pilot in late 2005 and has been expanded to include 25 ISPs. The program aims to address the threat posed by networks of 'zombie' computers, utilised for spam and other malicious activity. The AISI provides information to participating Australian ISPs about computers on their networks that have become compromised through the surreptitious installation of malicious software (malware) that enables spammers to control a compromised computer remotely and use it to send spam. Once compromised computers are identified, the ISP can advise the owner or take other counter-measures. This initiative is not just as a spam countermeasure, but also a tactic that will combat other malicious and criminal activities that are perpetrated using 'zombies'.

While the ACMA reports that ISP support for the program has been positive, at present ISP participation is voluntary. ISP's are making other contributions to the fight against spam. ABS data indicates that 75 per cent of ISPs offer spam-filtering software to their clients often at no charge. These efforts notwithstanding, investigation of further, possibly mandatory, requirements on ISP's could possibly be conducted.

MOVING FORWARD WITH SPAM

The Explanatory Memorandum to the *Spam Act 2003* suggests that 'reduction of spam in Australia from other sources' will take place 'progressively and gradually'. International cooperation, resourcing commensurate with the problem and aggressive alternative measures are necessary if domestic legislation is to have any meaningful effect against the scourge of spam.

There are a number of challenges in the fight against spam.

Measurement: To ascertain the effectiveness of any anti-spam measures (legal, educative, technical or otherwise) some consistent and meaningful measurement must be adopted. ISP cooperation requires collection and reporting of data for use by regulators, the ACMA and its international counterparts. Any attempts to record the effectiveness of countermeasures are of little practical value without some definitive data.

Global responses: Australia has anti-spam agreements with some nations but further treaties are needed that require governments to take more aggressive measures. Any nations with poor legislation or inadequate or unwilling resources to enforce anti-spam legislation remain potential havens for spammers fleeing tougher regimes elsewhere. The OECD and UN have attempted to develop spam strategies and, given the global nature of the problem, such entities are, theoretically at least, a logical option for coordinating measures against spam.

To ascertain the effectiveness of any anti-spam measures (legal, educative, technical or otherwise) some consistent and meaningful measurement must be adopted.

Mark Bender GrCertHiEd, BBus, LLB (Hons), LLM is a Legal Practitioner of the Supreme Court of the ACT, Barrister of the High Court of Australia and teaches Commercial Law and Marketing Law in the Department of Business Law and Taxation, Monash University.

MBR subscribers: to view full academic paper, email mbr@buseco.monash.edu.au

Public access: www.mbr.monash.edu/full-papers.php (six month embargo applies)