Federal Court decision a warning to spammers

ACMA welcomed the decision of Justice Nicholson in the Federal Court in Perth in October 2006 to award a pecuniary penalty of $4.5 million against Clarity1 Pty Ltd and $1 million against its managing director, Mr Wayne Mansfield, for contravening the *Spam Act 2003*. The judgement provided a strong warning to Australian spammers that contraventions of the Spam Act can result in substantial penalties being awarded against individuals and organisations.

The prosecution of Clarity1 is ACMA's first prosecution under the Spam Act. The legislation sets out penalties of up to $1.1 million a day for repeat corporate offenders.

On 13 April 2006, Justice Nicholson found that both Clarity1 and Mr Mansfield were in breach of the Act for both sending unsolicited commercial electronic messages, and for using harvested address lists. Among other matters, ACMA submitted to the Federal Court that Clarity1 Pty Ltd and Mr Mansfield sent out at least 231 million commercial emails in the twelve months after the Spam Act commenced in April 2004, with most of these unsolicited and in breach of the Act.

The Spam Act makes it illegal to send, or cause to be sent, unsolicited commercial electronic messages that have an Australian link—if it originates or was commissioned in Australia, or originates overseas but was sent to an address accessed in Australia. Commercial electronic messages include emails, mobile phone messages (text and multi-media) and instant messaging. The Act also prohibits the use of address-harvesting software and harvested address lists to send spam, but does not cover voice or fax telemarketing.

To comply with the Spam Act, a commercial electronic message must meet all the following conditions:

Consent—the message must be sent with the recipient's consent.

Identify—the message must contain accurate information about the person or organisation that authorised the sending of the message.

Unsubscribe—the message must contain a functional unsubscribe facility to allow the person to opt out from receiving messages from that source in the future.

More information about ACMA's anti-spam activities, including the SpamMATTERS tool, is on the ACMA website at **www.spam.acma.gov.au.**

Fight against zombies extended

ACMA is stepping up the fight against spam by extending its Australian internet security initiative, following completion of a successful trial. The trial began in November 2005 with six ISPs participating. ACMA is now extending the initiative to other ISPs.

The initiative operates by forwarding information about 'zombie' computers (computers that have been infected by a computer virus or other form of malware) to Australian internet service providers (ISPs). These ISPs then contact their customers to assist them to 'disinfect' their computer. Experience from the trial indicates that the vast majority of customers are unaware that their computers are infected and are grateful for assistance in making them secure.

Since the trial commenced, the *Internet Industry Spam Code Of Practice – A Code for Internet and Email Service Providers* has been registered by ACMA and came into effect on 16 July 2006. The code complements the initiative with provisions that enable ISPs to disconnect a customer's computer if the problem is not resolved by the customer.

Zombie computers are now the major source of spam and can also be used to commit online crimes remotely from anywhere in the world without the computer owner knowing. Personal identity information can be obtained and zombies can infect other computers and mount assaults on internet sites. Without effective security measures, a computer may be infected through various means, such as opening spam containing a virus or visiting websites where malicious programs are downloaded.

Avoid becoming an accidental spammer

- Use anti-virus and other security software, and ensure this is updated regularly.
- Regularly download and install the latest security patches for their computer software and use automatic software security updates where possible.
- Use personal firewall software.
- Only open an attachment to an email where the sender and the contents of the attachment are known by the email recipient. Suspect emails should be deleted immediately. If an attachment needs to be opened, it should be checked by anti-virus software before opening.
- Use long and random passwords and change these regularly.
- Do not visit 'suspect' websites.

The substantially higher bandwidth provided by broadband relative to dial-up internet services significantly increases the amount of spam that can be disseminated. The 'always-on' characteristic of broadband services also makes insecure computers more vulnerable to infection and more capable of spam dissemination without user knowledge. The increasing take-up rate of broadband in Australia has increased the need for action against zombie computers.

The ISP participants in the Australian internet security initiative trial were OptusNet, Pacific Internet, Telstra Bigpond, Uecomm, West Australian Networks and Westnet. The following ISPs have now jined the initiative: Access Net Australia, Agile, AOL, AUSTARnet, Bekkers, Chariot, Hotkey, ihug, iinet, Internode, iPrimus, Neighborhood Cable, OzEmail, Powerup, Primusonline, Reynolds Technology, Riverland Internet, SeNet and Soul.

ACMA's work on the initiative was supported by the Department of Communications, Information Technology and the Arts, the Western Australian Internet Association and AusCERT.