Spam Act review an opportunity to update anti-spam **framework**

A review of the operations of the *Spam Act 2003* and the relevant parts of the *Telecommunications Act 1997* that support it was announced by the Minister for Communications, Information Technology and the Arts, Senator Helen Coonan, in December 2005.

ACMA provided a submission to the review, which is being conducted by the Department of Communications, Information Technology and the Arts (DCITA), in February 2006. ACMA's submission concluded that the legislation has generally been successful, appropriate and 'a model for spam legislation around the world'.

Most professional spammers that were active in Australia prior to the commencement of the Telecommunications Act have ceased operations, and Australia has dropped from tenth to twenty-third on the list of worldwide spamming nations.

However, the activities and methods utilised by spammers are continually evolving and the ACMA submission recommended amendments to the Spam Act to capture some practices recently adopted by professional spammers, such as the inclusion of misleading or deceptive sender or subject information, and the use of compromised machines to send emails.

The Spam Act places considerable obligations on business in appropriately controlling its email communications. Most businesses made the required changes to their practices when the Act was passed, and many incurred considerable cost in doing so. As there is no evidence that the Spam Act is insufficient in this regard, ACMA did not recommend any changes to the Act that would further impact on such businesses.

However, businesses still face some areas of uncertainty. In particular, the rules for determining customer 'consent' for the receipt of commercial electronic messages could be more fully prescribed in some areas. SMS marketing also is creating some problems. ACMA suggested in its submission that a body representative of industry and consumers (such as the eMarketing Code Body) could be asked to develop detailed practices that could become 'safe harbour' provisions for businesses.

The ACMA submission also recommended that several powers and obligations of ACMA related to the administration and enforcement of the Spam Act be clarified. It was recommended that ACMA be given a legislative power to share information with international regulators, similar to the power held by the Australian Securities and Investments Commission, and that the complaint provisions of the Telecommunications Act be amended to make them more appropriate to the spam context.

While the Spam Act has been generally successful in combating the problem of spam originating in Australia, the challenge now is to accelerate the global fight against spam. There must be appropriate regulatory, enforcement, technological and cooperative frameworks in place to detect and punish professional spammers wherever they are located. This will become increasingly important if spam continues its rise as the main delivery mechanism for e-security threats and crime.

The ACMA submission to the review of the Spam Act is on the ACMA website (www.acma.gov.au), and all submissions to the review are on the DCITA website (www.dcita.gov.au).

Retreat of the zombies

A trial of the Australian Internet Security Initiative (AISI), an ACMA database containing up-to-date data on 'compromised' personal computers, was launched on November 2005 by the Minister for Communications, Information Technology and the Arts, Senator Helen Coonan. The data is supplied to internet service providers (ISPs) for them to take action to rectify the problems caused by these PCs.

These are generally 'zombie' PCs—computers that have been infected by a computer virus, trojan horse or similar intrusion, including hacking. Once infected, zombies can be used to commit online crimes, such as sending spam or hosting offensive material, remotely from anywhere in the world without the computer owner knowing—hence the term 'zombie'. In addition to the detrimental impact zombie PCs have on the safety and security of the internet, owners of these PCs may find themselves paying for bandwidth they did not know they were using.

Six Australian ISPs are currently participating in the trial: Telstra BigPond, OptusNet, Westnet, Uecomm, Pacific Internet and West Australian Networks. These ISPs receive daily reports from ACMA on infected PCs on their networks. The ISPs then contact the customers operating these PCs to advise them of actions they can take to fix the problem. If the problem is not fixed and the PC remains a threat to other internet users, the computer may be disconnected from the internet until the problem is resolved.

Preliminary results from the AISI trial indicate it is having a positive impact, in conjunction with other internet security activities, in reducing the incidence of compromised PCs on the Australian internet. The chart records the total number of events or instances of compromised PCs reported daily by ACMA to participant ISPs. The trend has reduced from more than 60 events daily at the start of the trial to fewer than 20 per day at the end of March 2006.

ACMA, in collaboration with other government agencies, is assessing the outcome of the AISI trial to decide whether to commence a wider rollout of the initiative. ACMA commends participant ISPs in assisting with the trial and assisting in efforts to make the internet a more safe and secure environment, to the mutual benefit of business and consumers.

Internet Security Initiative – Reportable Events – 1 Nov 2005 to 1 April 2006