

Spam — Remedies against the crime not the ham

By The Henry Davis York iTEAM

Unsolicited snail mail is usually a nuisance, but there are only so many people who are prepared to fit so many pieces of 'junk mail' in your letterbox — and often it is relatively simple to uncover the identity of the sender. But in cyberspace 'SPAM' (unsolicited electronic mail) can bring a whole new dimension to the word 'nuisance' — and the remedies against such conduct are costly and at times ineffective. So is 'SPAM' a real problem for individuals and businesses and if so what remedies are available?

The retaliatory spammer

SPAM was initially introduced to us by individuals or companies promoting goods or services, seeking financial contributions or conveying religious or political beliefs. With the availability of email services and email lists, the cost and ease associated with sending SPAM is minimal, therefore, making it a highly attractive tool. Increasingly, however, SPAM is being sent as a retaliatory measure — large messages are sent which cause overflow of the receiver's storage facility, crashing the system, denying access to all other users of the system and in some cases destroying valuable data. To avoid detection spammers often do not send a 'reply to' address and may even masquerade using a third party's sender address. Depending on how vindictive a spammer is feeling, the SPAM may also attach a virus.

Remedies

When determining the remedies available for loss and damage caused by SPAM there are two main considerations:

1. the content of the SPAM and

2. the damage to data and computer systems, as an offence.

It goes without saying that traditional causes of action are available with respect to the content of SPAM — for example is the SPAM false and misleading? Is it defamatory or discriminatory? Is there infringement of a party's intellectual property rights? As with all civil litigation, however, the problem is one of cost, and then of course the likelihood of recovery. This perhaps explains why there are only a few cases (most of which are from the United States) in this area, and most appear to settle under a cloud of confidentiality.

Current offences under the Crimes Acts

In Australia, offences relating to computers may be found in our various State Crimes Acts. For example, ss 309 and 310 of the Crimes Act 1900 (NSW) makes it a crime for any person without authority or lawful excuse to:

- intentionally access data in a computer (s 309)
- destroy, erase or alter data in a computer (s 310(a)) or
- interfere with, interrupt or obstruct the lawful use of a computer (s 310(b)).

Section 310 of the Crimes Act 1900 (NSW) carries a ten year prison sentence, a penalty of \$110,000 or both.

Very few cases involving a breach of these provisions seem to be reported, possibly because very few cases are run unless loss and damage is substantial or issues of social justice are involved.

One recent exception is the Victorian case of *R v Hourmouzis* in which a man was sentenced in October of last year for, amongst other things, sending approximately

4000 SPAMS in a bid to manipulate to the stock price of a US company. The charges were brought by the Australian Securities and Investments Commission under various sections of the Corporations Law dealing with false and misleading information and s 76E of the Crimes Act (Vic) 1914 relating to the interference, interruption or obstruction of the lawful use of a computer. Mr Hourmouzis was sentenced to two years jail on each count, to be served concurrently with a 21 month suspended sentence upon entering into a \$500 two year good behaviour bond. In addition, the United States Securities and Exchange Commission has obtained judgment against Mr Hourmouzis for the amount of approximately \$17,000 being the profit made by Mr Hourmouzis from selling the shares purchased on the first day of trading after transmission of the SPAMS.

Proposed cyber crime legislation

In January this year the Federal Government's Model Criminal Code Offences Committee prepared a discussion paper dealing with the area of law which criminalises the harming of computers and the breach of security systems. The recommendations made by the Committee include:

- a prison term of five years or more for unauthorised access to computers with the intention of committing a serious offence
- a maximum prison term of ten years for modification of data in a computer for the purpose of impairing access to or the reliability, security or operation of data and
- a maximum term of ten years for unauthorised impairment of electronic communications to or from a computer.

The New South Wales Attorney-General is currently considering the Committee's report with a view to drafting recommendations to be put to Parliament. We will keep you informed of any progress.

