TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 294
March 2005

# Spam: Nuisance or Menace, Prevention or Cure?

Rob McCusker

*Unfettered global communication through the internet has facilitated a massive intrusion of unsolicited commercial email messages, commonly known as spam. Currently accounting for as much as 65 per cent of all email, spam leads to productivity costs for businesses each year and is increasingly being used for the commission of crime. This paper discusses the increasing sophistication of the techniques used to obtain email addresses, and outlines and critiques a selection of legislation which aims to reduce or remove spam. It also examines a range of measures aimed at preventing spam from reaching its intended targets. It is argued that the mitigation of spam can only be achieved through a holistic approach taken by governments, law enforcement agencies, internet service providers, corporations and consumers.*

**Toni Makkai**
**Director**

## Context

'Spam' is an electronic version of the direct 'junk mail' placed in domestic and business post, and/or in newspapers and magazines on a daily basis. The key differences between spam and junk mail are that the volume of spam is far greater, the intrusion of spam is far greater and the avoidance of spam is far more difficult. Spam is email sent to a large number of people who do not request it, detailing products or services in which they may have no interest. It is sent by people who disguise their identity and whom it is difficult, if not impossible, to locate or deter. About 95 per cent of spam is concerned with marketing the provision of goods and/or services (Gaudette & Chouinard 2004). Although the United States remains the largest source of spam (an estimated 60 per cent of spam messages originate from the US), it is clearly a global phenomenon (Gaudette & Chouinard 2004).

Figures concerning the volume of spam tend to be produced by email filtering companies and/or from projections based on current spam activity identified by such filtering. Because the volume and nature of spam filters differ, so too do the figures produced. However, what remains clear is that the proportion of spam present in ordinary email is rising. A global filtering company, Symantec (2004), noted that in June 2003, 49 per cent of the email messages it filtered were spam. In June 2004, of the 104 billion email messages it filtered, 65 per cent were spam. By December 2004 that figure was 67 per cent (Dunn 2005).

## Why send spam?

Spam is simply a more pervasive form of direct marketing and works on the simple premise that, although the vast number of recipients will reject it, a minority will read and/or respond to the message. The costs of communicating via email are very competitive, the response rate required to generate a profit is minuscule, and the likelihood of some responses being received is a

ISSN 0817-8542

ISBN 0 642 53875 1

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9221
Fax: 02 6260 9201

For a complete list and the full text of the papers in the Trends & issues in crime and criminal justice series, visit the AIC web site at: http://www.aic.gov.au

**Disclaimer:**
**This research paper does not necessarily reflect the policy position of the Australian Government**

**Project no. 0038**

certainty. For example, the cost of sending a single email has been estimated at between US$0.000082 and US$0.000030 (McCurley 1998) and the cost of obtaining a single email address has been estimated at US$0.00032 (Cerf & Swindle 2002). In one case, a response rate of 0.0023 per cent led to sales of US$1,500 at a cost to the spammer of only US$350 (Wall Street Journal 2002, cited in OECD 2004: 9). In a recent US study, 33 per cent of respondents clicked on the spam email to solicit further details and seven per cent actually ordered a product or service (Fallows 2003: 26). If spam recipients respond in any way to the emails they receive, they will inevitably assist in the continued perpetuation of spam.

## Dissemination

Spam can only be sent to genuine email addresses. Although spammers originally obtained their addresses from internet sites such as chat rooms, they have begun to use a more complex range of methods. Some of these rely upon the reaction of the email recipient to the action of the spammer. Thus, a spammer may target corporate email addresses, such as <helpdesk@company.com> or <customerservices@company.com>. Because such sites are created to facilitate customer relations, all emails receive a response and confirm the validity of the email address. Alternatively, the spammer may ensure that once the email is opened, a message confirming its receipt is sent to the spammer – this confirms for the spammer that the email address is valid. Finally, the spammer may launch a 'directory harvest attack' by attempting to deliver emails to corporate addresses using all possible name combinations such as <adam.smith@company.com>, <asmith@company.com> or <a.smith@company.com>. By a process of elimination, those email addresses which are not rejected by the companies' servers will be accurate (Blackspider Technologies 2004).

## Awareness

Spam is not universally regarded as a problem. In a recent US study of consumers, 92 per cent of respondents agreed that spam was 'unsolicited commercial email from a sender they do not know or cannot identify' (Fallows 2003: 9). However, 65 per cent of respondents did not consider email to be spam if it originated from a sender with whom they had previously conducted business (Fallows 2003: 10). The same study found that 59 per cent of the respondents found spam 'annoying but not a big problem', 27 per cent found it to be a 'big problem' and 14 per cent believed it to be 'no problem at all' (Fallows 2003: 27). This lack of negative perception renders it difficult to apply uniform anti-spam solutions.

The volume of spam, however, does cause consternation to business users. Corporations, which rely upon the speed, global outreach and versatility of email, cannot simply delete incoming email messages without first being aware of their content. Checking that content, manually or automatically via filtering technology, raises the risk of exposure to offensive content and to viral contamination. There are also significant costs associated with checking content. One study estimated that in a company of 500 employees, each taking 40 seconds to deal with four emails a day, 166 working days per annum will be lost (Blackspider Technologies 2004). For an Australian company of similar size that loss would be in the order of A$11.9 million per year.

Spam may also emanate from email sent to employees by their friends and families, and between employees within the workplace. A company with 10,000 employees may lose more than US$13 million in lost productivity each year as a direct result of this internally generated and disseminated 'friendly fire' spam (Gartner 2002, cited in Trudeau 2003). In addition, the corporation that facilitates the exchange of friendly fire spam may become subject to legal action. In 2001, 8.3 per cent of US firms had to deal with sexual harassment and 1.6 per cent with discrimination claims because of the inappropriate use of email and the internet by employees (American Management Association 2001).

Whilst the majority of spam concerns legitimate products, entrepreneurial criminals recognised quite rapidly the potential of spam for the facilitation of established crimes. Thus, for example, the US Federal Trade Commission (1998) has compiled a list of the 12 most common scams perpetrated through spam. These include the offering of business opportunities, chain letters, health and diet scams and get-rich-quick schemes. Perpetrators of advance fee fraud (Smith, Holmes & Kaufmann 1999) have of course fully embraced the advantages that email dissemination has provided.

## Adaptation

Criminals have also sought to exploit the vulnerability of some email users by developing the art of 'phishing', a process whereby official-looking 'spoofed' (or trick) emails, typically purporting to come from banks, attempt to persuade a user to click on a false web link leading to a fraudulent web site. Once there, the user is asked to provide their online password, user name and/or other personal information in response to a fake but convincing security check. The Anti-Phishing Working Group (2004) notes that by selecting well-known banks, online retailers and credit card companies, the phishers are able to fool five per cent of users into responding to them.

In addition, techniques currently employed to disseminate viruses have been used to disseminate spam, through a process known as 'convergence' (Wood 2003; Roberts 2003). A key example of this phenomenon was the Sobig virus which appeared in January 2003. Basic viral contamination occurred when:

- the Sobig virus, in a worm, was placed in an email attachment and sent;
- the recipient opened the attachment and released the worm;
- the worm sent copies of itself to email addresses stored on the recipient's computer; and
- the worm installed a copy of itself upon networks shared by the recipient's computer.

Convergence occurred when:

- the Sobig worm was modified to allow a 'Trojan horse' program to be downloaded;
- the Trojan horse program allowed open proxies (or gateways) to be installed on the recipient's computer; and
- the recipient's computer could then be used by spammers to relay spam to other computers without the recipient (or 'zombie') knowing or the spammer being detected.

In short, the success of spam has acted as a catalyst for further spam-based criminal activity. This, in turn, has helped to further perpetuate spam *per se*.

## Solutions

Any strategy that attempts to mitigate the impact of spam needs to be holistic in nature and consider the route by which spam is disseminated and the various actors who participate in that dissemination process. Essentially, there are five key stakeholders involved:

1. governments, that are in a position to create legislation to prevent spam;
2. law enforcement agencies which are responsible for investigating spam;
3. internet service providers (ISPs) that can filter all email to remove spam prior to releasing it to customers' inboxes;
4. corporations, that can filter all email for spam and govern appropriate use of email via an applied email policy; and
5. consumers, who can filter their email and elect never to respond to unknown email.

Ultimately, the individuals targeted by spam might assist in the anti-spam effort by:

- avoiding placing email addresses in a public domain, for example a chat room;
- if placing an email address in a public domain, disguising it so that, for example <johndoe@fakesite.com> becomes 'johndoe at fakesite.com';
- using multiple email addresses so that in the event of receiving spam the targeted email address can be discarded;
- installing and updating spam filters on home computers;
- using longer and more complicated email addresses; and
- never responding to spam in any way (including clicking on an unsubscribe button), but simply deleting it.

The continued volume and apparent success of spam suggests that many of the above rules are not being observed by some individuals. For that reason it is imperative that other actors in the chain of spam (ISPs, corporations and governments) continue striving to reduce the amount of spam that penetrates computer systems in the first instance. Thus, corporations require an email policy in which the right to, and extent of, internet and email usage is clearly delineated. ISPs, which already filter vast numbers of emails, might also elect to follow America Online's (AOL's) action in simply denying their customers access to certain web sites prone to spam (Krim 2004), or Microsoft's suggestion of requiring senders to devote 10 seconds of their computing time to the solution of a mathematical puzzle prior to being able to send an email (CNN 2004). Finally, governments might continue to cooperate with one another in anti-spam campaigns, such as *Operation secure your server* (Australian IT 2004), and to establish memoranda of understanding as Australia, the US and UK have done (Cullen 2004).

## Legislative responses

Legislation to counter spam has been introduced in more than 30 countries (OECD 2004) but there is no mutual agreement on the definition of spam. Furthermore, some jurisdictions have legislation dedicated to spam whilst others prefer to incorporate spam offences into pre-existing legislation. Thus the US has the *CAN SPAM Act* (*Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003*) and Australia has the *Spam Act 2003* (Cth), whereas Austria has the *Telecommunications Regulation Act* and Mexico the *Federal Law for Consumer Protection*.

There is as yet no universal approach for dealing with spam, although the United Nations (2004) has recently called for such an approach to be adopted. The closest example of legislative universality thus far is the European Union's Directive on privacy and electronic communications (2002/58/EC) which came into effect on 12 July 2002. However, the range of offences it contains is relatively low and the directive has still not been fully incorporated into the legislative frameworks of all member states (Institute for Information Law 2004). A failure to fully implement the directive may lead to the establishment of 'spam havens' within non-compliant states to which spammers could migrate. Since the enforcement regimes between member states also differ, there is a danger that spammers will gravitate towards those states with less harsh regimes. As the approaches taken by the US, UK and Australia in relation to spam illustrate (see Table 1), there are both common threads in terms of approach but also common loopholes which potentially may undermine that approach.

**Table 1: Features of spam legislation in the United States, United Kingdom and Australia**

| | United States | United Kingdom | Australia |
|---|---|---|---|
| Name of legislation | *Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act 2003* | *Privacy and Electronic Communications (EC Directive) Regulations 2003* | *Spam Act 2003* |
| Definition of spam | Commercial electronic message – email only | Electronic mail – including text, voice sound or message sent over a public electronic communication network | Unsolicited commercial electronic message – including email, mobile phone text messages, multimedia messages and instant messages |
| Opt-out or opt-in? | Opt-out | Opt-in | Opt-in |
| Offence to use false or misleading header? | Yes (s 5(a)(1)) | Yes (reg 23) | Yes (s 17) |
| Offence to use deceptive subject headings? | Yes (s 5(a)(2)) | No | No |
| Offence not to state that message is an advertisement of solicitation? | Yes (s 5(a)(5)) | No | No |
| Offence not to have a functioning return electronic address? | Yes (s 5(a)(3)) | Yes (reg 23) | Yes (s 17) |
| Offence not to provide an unsubscribe facility? | Yes (s 5(a)(5)) | Yes (reg 23) | Yes (s 18) |
| Offence not to provide a valid physical postal address? | Yes (s 5(a)(5)) | No | No |
| Offence to transmit commercial email after recipient has objected to its transmission? | Yes (s 5(a)(4)) | No | Yes (Schedule 2, s 6) |
| Offence to use email addresses obtained from a harvest or dictionary attack? | No – however, it can be an aggravating factor during sentencing (s 5(b)(1)) | No | Yes (ss 20, 21 and 22) |
| Offence not to have warning labels placed on commercial email if it contains sexually oriented material? | Yes (s 5(d)) | No | No |
| Civil or criminal penalties? | Civil and criminal | Criminal | Civil |
| Maximum penalties? | Criminal: five years imprisonment; forfeiture of property used in the commission of an offence<br>Civil: US$1 million fine | £5,000 fine if dealt with in the magistrates' court; unlimited fine if dealt with in the Crown court | For breaches which occur on a single day:<br>Individuals: $44,000 fine<br>Bodies corporate: $220,000 fine<br>For repeat offenders the fines could be increased by a factor of five |

Source: *CAN SPAM Act 2003* available at http://www.spamlaws.com/federal/108s877enrolled.pdf; the *Privacy and Electronic Communications (EC Directive) Regulations 2003* available at http://www.hmso.gov.uk/si/si2003/20032426.htm; the *Spam Act 2003* available at http://scaleplus.law.gov.au/html/comact/11/6735/rtf/1292003.rtf

The issue of whether to adopt an 'opt-out' or 'opt-in' approach remains the collective legislations' Achilles' heel. The opt-out approach (adopted by the *CAN SPAM Act*) allows unsolicited commercial email to be sent until the recipient requests such mailings to cease. The opt-in approach (adopted by both the Australian and UK legislation) requires the permission of the recipient to be obtained before any email is sent. A disadvantage of the opt-out approach is that many customers may not have the time or inclination to click on 'unsubscribe' buttons within each of their incoming emails in order to alert the sender that they no longer wish to receive such messages. In addition, many spammers routinely insert false unsubscribe buttons into their emails.

However, the opt-in approach is subject to a different but equally exploitable loophole. In the UK regulations there is an exception to the opt-in rule known as a 'soft opt-in' (reg 22(3)). This allows for unsolicited email to be sent to recipients if:

- their contact details were obtained in the course of negotiations for, or sale of, a product or service;
- the marketing email concerns only 'similar products and services'; and
- the recipients have been provided with a means of refusing future email direct marketing.

It is not clear what is meant by the phrase 'similar products and services'. The Information Commissioner argues, for example, that a consumer who has shopped online at a supermarket's web site '…would expect at some point in the future to receive further emails promoting the diverse range of goods available at that supermarket' (Information Commissioner 2004). It is possible, therefore, that a business may conclude that the sale of a computer entitles it to contact the consumer about products ranging from computer software to computer furniture and stationery.

Under the Australian legislation a person must not send any unsolicited commercial email unless consent (defined in Schedule 2) has been obtained beforehand (s 16). Consent may also be inferred from the previous relationship between an individual and an organisation. The parameters of that previous business relationship may be interpreted widely by the organisation to the detriment of the consumer. Theoretically, in both cases the consumer will be forced to judge the appropriateness of the offers, opting-out if necessary, and undermining the opt-in system. The extent to which this proves to be a practical problem will only become apparent over time.

Ultimately, legislation merely provides the framework under which intercepted perpetrators of spam might be proceeded against in court. Perhaps, therefore, a proactive rather than a reactive approach towards spam will be most beneficial. Consequently, the interception of spam via technical counter-measures prior to its infiltration of computer networks must remain a key focus. Counter-measures change constantly but comprise four broad categories.

### 1 Characteristics of internet addresses

Counter-measures targeting internet addresses include the use of black lists, white lists and reverse DNS (domain name server) lookup. A black list is a list of internet addresses that are known to disseminate spam. Servers will block spam from those addresses but the list needs constant updating as spammers regularly change their IP addresses.

A white list is a list of internet addresses that are known to *not* disseminate spam. Servers will accept email from those addresses but will still need to filter for spam from non-white list addresses which may exclude genuine business opportunities.

Standard DNS changes a host address (for example, <www.eg.com>) into an IP address (for example, 191.0.1.50). Spammers may use fake host addresses which resemble real addresses. Reverse DNS lookup turns the IP address back into a hostname. If the IP address and hostname do not match, it is probably spam. Using this counter-measure, spam which has a false host address would be blocked and spam which has a real address would not be blocked.

### 2 Characteristics of words within emails

Counter-measures targeting words within emails include keyword analysis, lexical analysis and Bayesian analysis. Keyword analysis is where the text of an email is analysed for key words and phrases, such as ‘Viagra’, which do not usually appear in genuine emails. Emails containing those typical spam identifiers will be blocked. However, there is a high ‘false-positive’ rate with this method, resulting in genuine email being incorrectly diagnosed as spam.

Lexical analysis is where words are analysed in the context in which they appear. A word which appears in a group of unrelated words should trigger an alarm and the spam will be blocked. This analysis relies upon spam email being of low complexity, which is increasingly unlikely.

Bayesian analysis is where a group of spam emails and a group of non-spam emails are compared and a probability of a word or phrase being spam, or not, is assigned. The overall probability of the email being spam, or not, is ascertained. If it is deemed likely to be spam, the message is blocked. This is less time-consuming and more accurate than other forms of filtering, and Bayesian filters can also adapt to new spam words and alter their probability curves. However, while probability can be used to determine the *likelihood* of an email being spam, it cannot be more precise than that.

### 3 Characteristics of spam

Heuristics involves a particular email being examined for spam-like characteristics. Each of those characteristics is assigned a spam probability factor and then a total spam probability score is determined. If the score reaches a pre-determined level, the email is deemed to be spam and blocked. Individual emails are subject to precise scrutiny but filtering a large volume of individual emails is time-consuming. As with Bayesian analysis, probability is not the same as precision.

Spammers who send large numbers of spam email create a detectable pattern. ISPs can close network connections when such mass mailings are detected. Mass mailings are prevented and, therefore, so is spam. However, spammers may circumvent this by altering their mode of attack, for example by sending smaller but faster spam mailings.

### 4 Characteristics of the sender

Counter-measures can also be targeted at the characteristics of the sender, for example through sender authentication. This allows for the identification of senders of email, once fully on stream, based on their email or IP addresses. Emails with sender information that cannot be authenticated by the domain can be blocked or left for further checking. Forged email can be detected and spammers who re-route spam and forge its true origin can be discovered. However, sender authentication only verifies that the email address is genuine. It does not prevent spam sent from a genuine address.

Another counter-measure is known as challenge/response. Senders of email are required to provide confirmation before their emails are delivered to inboxes. If confirmation is not provided, the emails are not delivered. The number of bulk emails delivered to inboxes is reduced. However, a disadvantage is that legitimate senders of email are deemed to be spammers until they prove otherwise (Levitt et al. 2004; Tschabitscher 2004; MessageLabs 2004).

Businesses should avoid the temptation of adopting only one technical solution. Instead, they should choose a combination of approaches which best matches:

- the nature of spam typically received;
- the nature and size of the business concerned; and
- the potential threat that might be caused by not intercepting spam.

## Conclusion

Despite a raft of legislation in a range of countries, spam remains a relatively low-risk, cost-effective and profitable marketing method. Spam is a complex multi-faceted issue that demands a complex multi-lateral response. Governments alone cannot tackle spam. Individuals and businesses also need to increase their awareness of the dangers of spam and of the importance of establishing effective policies to prevent its dissemination. Although prosecution of major spam producers should be a priority, it should be recognised that investigatory, evidentiary and jurisdictional difficulties may arise. Consequently, a more proactive response using technological filtering applications should continue to be a key focus of the fight against spam. It should also be recognised that the perpetrators of spam, especially those with criminal intentions, are likely to continue trying to undermine such applications and may at times exploit system vulnerabilities.

## References

American Management Association 2001. *Workplace monitoring and surveillance: policies and practices*. New York: American Management Association. http://www.amanet.org/research/pdfs/emsfu_short.pdf

Anti-Phishing Working Group 2004. *Phishing attack trends report*. http://www.antiphishing.org/APWG_Phishing_Attack_Report-Mar2004.pdf

Australian IT 2004. Australia joins open relay fight. *Australian IT* 30 January. http://australianit.news.com.au/articles/0,7204,8534310%5e15306%5e%5enbv%5e,00.html

Blackspider Technologies 2004. *Spam: now a corporate concern*. Reading: Blackspider Technologies. http://www.blackspider.com/services/spam_whitepaper.pdf

Cerf V & Swindle O 2002. *Spam: can it be stopped?* Global internet project. http://www.gip.org/publications/papers/Spam061802.asp

CNN 2004. Gates: buy stamps to send email. *CNN.com* 5 March. http://www.cnn.com/2004/TECH/internet/03/05/spam.charge.ap/

Cullen D 2004. US, UK and Australia sign anti-spam act. *The register* 2 July. http://www.theregister.co.uk/2004/07/02/anti-spam_pact/print.html

Dunn JE 2005. Symantec: spam growth slowing at last. *Infoworld* 12 January. http://www.infoworld.com/article/05/01/12/HNspamslowing_1.html

Fallows D 2003. *Spam: how it is hurting email and degrading life on the internet*. Pew internet and American life project. http://www.pewinternet.org/pdfs/PIP_Spam_Report.pdf

Gaudette M & Chouinard M 2004. *Facing consequences: analysing the impacts of spam on unprotected enterprise networks*. Vircom white paper. http://www.vircom.com

Information Commissioner 2004. *Guidance to the Privacy and Electronic Communications (EC Directive) Regulations 2003*. London: Information Commissioner.

Institute for Information Law 2004. *Regulating spam: Directive 2002/58 and beyond*. Amsterdam: Institute for Information Law. http://www.solidground.nl/IViR-sybari/ivir-sybari-final.PDF

Krim J 2004. AOL blocks spammers' web sites. *Washington post.com* 20 March. http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A9449-2004Mar19&notFound=true

Levitt M, Mahowald RP, Burke BE & Christiansen CA 2004. *What you can and should do about the rising cost of spam*. Framingham MA: International Data Corporation. http://www.surfcontrol.com/general/assets/whitepapers/rising_cost_of_spam.pdf

McCurley K 1998. *Deterrence measures for spam*. IBM Almaden Research Center. http://www.almaden.ibm.com/cs/k53/pmail/pmail.ppt

MessageLabs 2004. Sender authentication: an end to the spam problem? *MessageLabs monthly report: March 2004*. http://www.messagelabs.com/emailthreats/intelligence/reports/monthlies/march04/default.asp

OECD 2004. *Background paper for the OECD workshop on spam, Annex II*. Paris: Organisation for Economic Cooperation and Development. http://www.olis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/edfc2255d6a8a51ac1256e240030f5b6/$FILE/JT00157096.PDF

Roberts P 2003. Sobig worm getting even bigger. *PC world* 14 January. http://www.pcworld.com/resource/printable/article/o,aid.108793,00.asp

Smith RG, Holmes MN & Kaufmann P 1999. Nigerian advance fee fraud. *Trends & issues in crime and criminal justice* no 121. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/tandi/ti121.pdf

Symantec 2004. *Spam statistics 2004*. http://www.brightmail.com/spamstats.html

Tschabitscher H 2004. What you need to know about Bayesian spam filtering. *About.com*. http://www.email.about.com/cs/Bayesianfilters/a/Bayesian_filter_p.htm

Trudeau P 2003. *Fighting the new face of spam*. Surfcontrol. http://www.surfcontrol.com/general/assets/whitepapers/New_Face_of_Spam.pdf

United Nations 2004. UN meeting looks to fight spam globally. *UN news service* 7 July. http://www.un.org/apps/news/story.asp?NewsID=11266&Cr=information&Cr1=technology

US Federal Trade Commission 1998. FTC names its dirty dozen: 12 scams most likely to arrive via bulk email. *FTC consumer alert* July. http://www.ftc.gov/bcp/conline/pubs/alerts/doznalrt.pdf

Wood P 2003. *The convergence of viruses and spam*. MessageLabs white paper. http://www.security.iia.net.au/downloads/sobigwhitepaper.pdf

Note: All URLs were operational on 1 July 2004

**Rob McCusker is a research analyst in the Global, economic and electronic crime program at the Australian Institute of Criminology**

**General editor, Trends & issues in crime and criminal justice series:**
**Dr Toni Makkai, Director, Australian Institute of Criminology, GPO Box 2944 Canberra ACT 2601**
**Note: Trends & issues in crime and criminal justice are peer reviewed**

**The AIC is a statutory body with a Board of Management comprising Australian, state and territory government representatives, administered under the *Criminology Research Act 1971***