THE AUSTRALIAN ANTI- SPAM REGIME
A FIRST YEAR REVIEW

Abstract

In April 2005 the enforcement of the Australian anti spam regime celebrated its first anniversary. The year has been a full one for the very small team charged with its implementation and development of skills, tools and practices to best deliver results that were the goal of the Parliament's passing of the legislation. From the outset the legislation was seen as a part of the regime and not its totality – the necessary other parts were to be developed and exercised by the Australian Communications Authority (ACA), the anti-spam regulator. In this the ACA was expected to draw its previous experiences managing the telecommunications industry, of which the ISP industry is seen to be a part.

The regime had some early successes but the ACA is under no illusions about the necessity for ongoing, long-term action based around a multifaceted anti-spam strategy, of which the law is a part. The roles that can be played by technology developers, local industry, international peers and colleagues and especially consumers make them valuable partners. This review provides an outline of current efforts, and offers some views about the future, especially in relation to international features of the fight to contain spam.

John M Haydon

Executive Manager, Consumer Group

Australian Communications Authority

June 2005

Introduction

1. Definitions of and responses to spam vary across jurisdictions. However, all over the world, spam in its various forms is acknowledged as a problem for users, employers, ISPs and legitimate e-marketers. Spam statistics are also subject to variation; however, in 2004-2005, spam was estimated to make up between 50 and 60 per cent of global email traffic. The annual cost to business is estimated at over $1,000 per employee per year, due to lost productivity and additional IT resources required to deal with spam and its flow-on effects. It is an even larger problem in developing economies as its volume clogs narrow band-width access channels and is a barrier to access to key market information and education. Some surveys have suggested that spam is causing consumers to lose trust in email as a social and business tool.

2. Spam is identified in the Australian *Spam Act 2003* as 'unsolicited commercial electronic messages'. The Spam Act applies to email, SMS, MMS, instant messaging and other future forms of electronic messaging. Voice telemarketing, fax messages and Internet pop-ups are not covered by the Act.

3. Additionally, through 2004–05, spam was used increasingly as a mechanism for criminal activity—particularly fraud and 'cybercrime', including a rise in the percentage of spam that carried harmful computer codes such as viruses, spyware and 'trojan horses'.

4. Spam is a global problem that requires a global solution. Indeed, the Australian experience is that 99 per cent of spam received by Australians in 2004–05 came from offshore. Thus domestic legislation alone will not solve the problem and international cooperation is a key part of the Australian response strategy.

5. Global control of spam requires that each country start with legislation and then include other measures to combat spam originating from its own jurisdiction; to do otherwise is to risk being seen as a haven for spammers. The Australian response is built around a five-way strategy for combating spam:

- strong legislation and enforcement;
- technological measures;
- industry partnerships;
- consumer and business end-user education; and
- international cooperation.

6. The Australian anti-spam response comprises seven persons, with total resources of about AUD 800 000 in 2004, to act across all of these five areas. With this limit on resources, it is necessary to be inventive, innovative and apply the best technology to achieve the maximum effectiveness for money spent.

Strong legislation

7. The *Spam Act 2003*, which was signed into law on 12 December 2003 but was enforceable from 10 April 2004, prohibits the sending of unsolicited commercial electronic messages (as commercial messages are the largest volume component of the spam problem). This sets the framework for Australia's spam response, although the government and the enforcement agency appreciate that spam is both a vehicle for, and a technology foundation of, more malicious phenomena (phishing, viruses, trojans). The Spam Act states that all commercial electronic messages must be sent with the recipient's consent, and must include accurate information about

the sender and a functional unsubscribe facility. The Act also prohibits the use of address-harvesting software and harvested address lists to send spam. Focussing on consent obviates all debate about volume of messages, and other complicating issues. ‘Consent’ is defined to include both express and inferred consent, and so does not prevent normal contact by businesses with ongoing customers. This careful delineation in the Act between true junk mail and legitimate customer contact has been important in achieving the support of ordinary business in Australia.

8. The Australian Communications Authority (ACA) is the agency assigned the responsibility of enforcing the legislation and developing the other components of the overall response strategy. On 1 July 2005, the ACA will be merged into the new Australian Communications and Media Authority, which will then become the responsible regulator.

9. Breaches of the Spam Act can incur civil penalties in the Federal Court of up to $220,000 per day for first-time corporate offenders and $1.1 million per day for repeat corporate offenders. In addition, offenders can be required to forfeit profits and pay compensation to spam victims. The Federal Court may also issue injunctions.

10. The ACA can issue warnings, infringement notices (which set out financial penalties) and enforceable undertakings.

11. Although the legislation was enforceable from 10 April 2004, the ACA began pre-emptive action in the prior amnesty period. It sought out, contacted and advised known spammers in Australia of the provisions of the legislation and of the ACA intentions on enforcement. This had a significant and quick response.

Legislation Awareness

12. A Spam Act awareness-raising campaign was commenced in advance of the enforcement date. It was launched by the ACA and the Department of Communications, Information Technology and the Arts (DCITA, the communications ministry) in early 2004 and continued in 2004-2005. The campaign included giving seminars and media interviews around the country, contributing articles to consumer and industry publications, distributing official government guides for business and providing comprehensive information through the ACA website.

13. The ACA, in conjunction with DCITA, continued to run an information campaign about the Spam Act’s requirements for business, especially small business. The ACA and DCITA sponsored the delivery of small business seminars throughout regional Australia on how to comply with the Spam Act and improve internet security. The seminar program also provided a valuable channel for distributing ACA and DCITA information guides specifically developed for business users.

14. Answers to specific enquiries from business are regularly posted on the ACA website as ‘frequently asked questions’ to provide further detail about the operation of the Act. Other enquiries are dealt with by email or through a telephone enquiry hotline.

15. From 1 July 2004 to 30 June 2005, the spam section of the ACA website averaged 40,000 hits per month and more than 1500 enquiries were answered by email, letter or phone.

Complaints – Triggers for Enforcement

16. End-users who receive spam from any source can report it to the ACA. Most spam reports are sent to reportingspam@aca.gov.au via the ACA website, but reports can also be lodged using a world-pioneering automatic reporting tool launched by the ACA in December 2004. The ACA worked with two private companies, a software developer and an internet service provider (ISP), to develop and trial this tool. (Further details can be found under the ‘Technological measures’.)

17. Complaints about spam sent by Australian businesses can also be lodged via an electronic form on the ACA website. This detailed information may be used later as forensic evidence, particularly the necessary ‘header information’ data, which reveals the origin and path of a spam email. Formal spam complaints are presently separately channelled into an internal customer relationship management system used to process compliance-related behaviours of businesses.

18. In the period from 30 June 2004 to 30 June 2005, the ACA received 200,000 reported spam and 2000 formal complaints. Complaints about mobile phone spam made up 10 per cent of the total spam complaints lodged by Australian consumers in 2004-2005.

Enforcement

19. The ACA’s first priority targets are major spammers who clearly do not intend to comply with the Spam Act, or repeatedly fail to comply after complaints are made. Legitimate businesses who intend to comply, and who take practical and satisfactory steps to do so, are addressed in the first instance by the ACA’s compliance and education program.

20. When the ACA receives complaints about spam sent by a business or individual, the ACA sends a letter advising them about the Spam Act, requesting information about their compliance policies and warning that future non-compliance could attract significant penalties. These letters also direct the business to remove the complainant’s details from their mailing databases, where the complainant had given the ACA permission to disclose this information. In 2004-2005 the ACA formally wrote about 220 letters to companies, most of whom responded by satisfactorily demonstrating their intention to comply with the Act.

Enforcement statistics for the financial year 2004-2005:

- Companies/individuals issued with advice or warnings to comply: 80
- Companies/individuals fined: 3
- Enforceable undertakings accepted: 2
- Search warrants executed: 5
- Formal demands for information (Section 522 notices) issued: 4
- There are also ongoing investigations.

Enforcement Outcomes

21. Australian enforcement strategy has focussed energies in the first instance on prominent and profligate spammers; such action on the part of the ACA generally constitutes use of the legislation and its penalty provisions, or the threat to do so. However the legislation and its provisions are but one of a suite of available anti-spam tools, and the mix of the tools used and the emphasis in each instance will vary with time. In particular, emphasis can be expected to shift to industry action and user education as the focus changes from accessible spammers to, for example, compromised and vulnerable computers which are inadvertent sources of spam.

22. As a result of this active enforcement and education programme, the proportion of global spam sent from Australia has fallen to approximately one per cent, and international anti spam organisation SpamHaus reports that several major global spammers formerly based in Australia have halted or left the country. The ACA continues to actively investigate alleged spammers based in Australia.

23. The spam currently being sent from Australia largely comes from virus-infected computers in Australia being used by spammers located elsewhere to relay spam. We understand this is the case for much of the Asian region. The ACA, DCITA and AusCERT have now launched an Internet Security Initiative, discussed in the next section, to combat this problem.

24. Because spam was increasingly used as an avenue for criminal activity, such as fraud and cybercrime, the ACA established and has continued its joint anti-spam work with the Australian High Tech Crime Centre (AHTCC), a national centre hosted by the Australian Federal Police. An ACA investigator is stationed in the AHTCC to allow sharing of intelligence and joint investigations where appropriate.

25. The ACA also worked closely with content regulators such as the Australian Competition and Consumer Commission (ACCC) and the former Australian Broadcasting Authority (ABA), and continued to exchange intelligence with foreign regulators.

26. In early February 2005 the ACA took part in an international 'Spam Sweep' initiative, driven by the ACCC and peer overseas consumer protection organisations, which aimed to identify and follow up on fraudulent content and scams distributed using spam. Participating agencies are currently compiling individual summaries of what was discovered in the sweep.

Technological measures

27. The ACA supports the development of technological measures to counter spam by the global software and Internet service provider (ISP) industries. Without favouring any provider, in its awareness and education programs the ACA promoted the use of tools for blocking spam and improving Internet security. ISPs used these tools to restrict the amount of spam on their networks and to limit the propagation of spam across national infrastructure. Corporate and residential users also used the tools to improve their Internet security, reduce incoming spam and deal appropriately with spam they do receive.

28. In specific initiatives, the ACA has been working with two Australian businesses; the software company SpamMATTERS and ISP company Pacific Internet, to trial a new type of spam forensics tool. This will empower end users in that it that enables them to report spam directly to the ACA for analysis. Consumer and business end-users can download this tool from the ACA website and use it in conjunction with their email to report spam they experience; the system automatically delivers the email header information and auto-analyses the spam for the ACA's investigations database. Several hundred Pacific Internet customers participated in the three-month trail, which concluded successfully in April 2005. The reporting tool is expected to be made available to the wider Australian public in July 2005. The particular usefulness of this tool is that the more samples of spam submitted the more rigorous the possible analysis and the better the results. This has the advantage that should it be subject to spammer attack (for example. DDoS), that attack would be turned to advantage for enforcement purposes.

29. Another imminent initiative focuses on the significant amount of spam sent unknowingly by Australians whose computers have been infected, or 'compromised', by a virus, when the true originator of the spam may be located in another country. Professional spammers deliberately spread viruses and other malicious code, and seek out compromised computers, as a means of sending bulk spam while concealing their own identities. The Australian Internet Security Initiative is to be a joint ISP-Government project that aims to reduce the number of compromised computers in Australia. The ACA, DCITA and AusCERT have built a system to search for the IP addresses of these computers. Information about any infected computer is passed to the ISP whose customer has the infected machine, and the ISP in turn works with their customer to resolve the

problem. The specific course of action is determined by factors such as the ISP's operating policies, Acceptable Use Policy (AUP), terms of supply contract or customer's circumstances. The ISP may, depending on the circumstances, ask the computer owner to immediately fix the problem; or if the computer is causing serious damage, it may be quarantined or redirected to an advice website. The ISP could also provide advice or a clean-up service for the customer.

30. The initiative will be trialled at first with a small number of ISPs and is expected to be extended nationally in 2005-06. The ACA is also working with AusCERT to extend the project with partners across the Asia-Pacific region.

Industry partnerships

31. Because the industry is best placed to address spam, the Australian legislation provides that the ACA can encourage (or compel) the creation of industry codes about the origination, transmission or delivery of electronic messages. The originators are prospectively the e-Marketing industry and the ISP industry, which are respectively the bases for the transmission or delivery of these messages. Codes for these activity areas were an early focus for the ACA.

32. The e-Marketing industry is potentially a major source of commercial electronic messages. However the industry has a vested interest in ensuring reasonable and responsible behaviour from its members, as this will ensure that electronic messaging remains a viable marketing channel. In the Australian context, the industry includes specialist e-Marketing firms, and firms who principally market their products using this means. In 2004, an e-Marketing Code of Practice was developed by an industry committee of relevant peak bodies, chaired by the Australian Direct Marketing Association (ADMA). The code aims to complement the Spam Act and provide e-Marketers with specific situations and compliance guidelines.

33. This code was registered by the ACA in March 2005, and under provisions of the Australian legislation, the ACA now has the power to direct individual e-Marketing firms to comply with it. The ACA provided support and advice for the code committee towards the finalisation and registration of the code, but did not otherwise influence the content of the code.

Signatories to the code

34. Under the e-Marketing code of practice, an organisation that is a member of the industry may sign up to the code, thus indicating its willingness and commitment to comply with the code rules. A signatory to the code may also nominate a Recognised Industry Body (usually an industry association), of which they are a member, to handle complaints about the signatory's compliance with the code. In the three months since the code was registered, the ACA has approved 23 applications for signatory status under the code.

Complaint handling

35. The code allows for an industry-based complaint handling process, with safety-net provisions so that complaints can be referred to the ACA as a last resort. Escalated complaints can be referred to ACA-accredited Recognised Industry Bodies that have been nominated by signatories to the code to handle complaints on their behalf where they have not been able to resolve the concern. By June 2005 the ACA had accredited three industry organisations to deal with complaints against e-Marketers.

36. In the first instance, a complaint about a breach of the code will be handled by the e-Marketing company to which the complaint relates – generally the organisation that sent the commercial electronic message, or authorised it to be sent. If the complaint is not handled to the satisfaction of the complainant it will be referred to the Recognised Industry Body nominated by

the e-Marketing company. However, if the complaint relates to an e-Marketing company that is not a signatory to the code, or if they are a signatory to the code but have not nominated a Recognised Industry Body, the ACA will deal with the complaint. A complainant may request that his/her complaint be referred to the ACA for consideration at any stage of the complaint-handling process.

Code enforcement

37. The ACA is monitoring e-Marketers' performance against the code rules and may require a company whose compliance appears to be inadequate to address any process problems or difficulties.

38. ACA registration of the code means that the ACA also has powers under the Telecommunications Act to deal with serious instances of non-compliance. The ACA's powers enable it to direct any members of the e-Marketing industry to comply with the code; not just signatories to the code. If an e-Marketer fails to comply with a direction, the ACA can take the matter to the Federal Court, which can impose penalties of up to $250,000 for each contravention (i.e. each day of continued non compliance).

39. The ISP industry began developing a code of practice in mid-2004, through an alliance of Internet Industry Associations. The code committee included major players in the ISP industry. Again the ACA provided comment during the code development process but did not otherwise influence the industry processes. The code was intended to set out the steps that ISPs should take, as carriers of email traffic, to reduce the amount of spam entering or being sent over the Australian network.

40. Registration of this code by the ACA is expected to be completed in 2005-06. Registration would allow the ACA to direct individual ISPs to comply with it.

41. Electronic messages delivered by mobile phones (SMS, MMS etc) are now a focus for the ACA. Mobile phone spam has not yet become a problem to the extent of e-mail spam, but the ACA is watching developments in this area. In the Australian regime there has been a code of practice about SMS messages which focussed on content but had the additional effect of managing SMS spam. This code is being supplanted by a Regulatory Instrument about Premium Services content and high bills for consumers and the industry response to this instrument will determine any further ACA action in this area.

42. Consumers seem to find SMS spam even more intrusive than email spam. The ACA fined one Australian company for SMS spam in March and two others in June and worked closely with an international provider of mobile phone content to ensure its practices complied fully with the Act.

Consumer and business end-user education

Reducing spam and its harmful effects

43. Consumers and businesses who are the prospective victims of spam can and should take steps to reduce the amount of spam they receive and protect themselves from its harmful effects. They can also follow good Internet security practices, which reduce the risk of their own computer or server being taken over by a spammer and used to send spam without their knowledge. In encouraging these end users to take such measures the ACA and others are promoting the improved security of the Australian Internet, which will benefit the wider user community and potential overseas recipients of spam from Trojan-infected computers.

44. The message to Australian computer users is that *"My Computer's security is my responsibility. Just as I ensure that my car is safe and fit for the roads, I must ensure that my computer is safe and fit for use on the Internet."* This message seems to be getting through to consumers – it has been independently estimated that 80 per cent of them now use a firewall and anti-virus software.

45. The ACA's educational material recommends that consumers and business:

- install filtering and anti-virus software, and ensure it is regularly updated;
- install personal firewalls;
- download security patches;
- protect email addresses and mobile phone numbers;
- choose long and random passwords;
- treat email attachments with caution;
- not reply to spam emails; and
- beware of email scams and fraud.

46. Businesses with their own mail server need to ensure their server is not incorrectly configured as an open relay or open proxy, which can be used by spammers to send spam while hiding their own identity. Good Internet security practices are also important for both consumers and business in guarding against other spam-related threats, such as viruses.

47. In 2004–05, the ACA published and distributed an updated version of the educational resource *Fighting spam in Australia – A consumer guide*, and continued to distribute its partner guide, *Protecting your business from spam*. Both these are available from the ACA web site at http://www.spam.aca.gov.au .

48. As part of its general telecommunications consumer education program the ACA has produced and promotes a number of consumer "tool kits". The consumer guide about reducing spam was incorporated into the ACA's Internet Tool Kit. This tool kit is available in printed and CD forms and also from the spam section of the ACA website (listed above).

49. General information for consumers and businesses is also available on the spam section of the ACA website, including an update of the comprehensive frequently asked questions. A consumer education slideshow about Australia's spam laws, including tips on how to reduce spam is also available through the website.

50. The ACA has produced a short educational radio script about how to reduce spam, directing consumers to visit the ACA website for more information. The script has been broadcast by radio stations.

Compliance with the Spam Act

51. In addition to ensuring that their computer systems are not likely to become spam victims, businesses that use email and SMS for marketing need to know how to use these mediums responsibly. Information to business on how to comply with the Spam Act was delivered through the ACA website, the distribution of printed material, seminars for small business, media campaigns and the ACA's online enquiries facility and telephone hotline.

52. The ACA, in conjunction with DCITA, sponsored delivery of a series of small-business seminars throughout regional Australia on how to comply with the Spam Act and how to improve internet security. The seminars covered 50 regional towns across Australia.

53. The focus of the seminars was to provide small business with useful tools to ensure compliance with the Spam Act, reduce the amount of spam they receive and safeguard their computer systems so they cannot be exploited by spammers. Feedback from this program was generally good with the majority of attendees reporting that the seminar was relevant and that the information would be useful to them.

54. The seminar program also provided a valuable channel for distributing ACA and DCITA information guides specifically developed for business users. All of this material is available upon request from the ACA or from the ACA website.

55. In response to particular emergent types of spam, or particular industries involved in sending spam, the ACA also ran small, targeted media campaigns and produced educational articles for industry publications outlining the compliance requirements and giving specific details relevant to the particular industry or practice in question. For example, the emergence of mobile phone spam relating to nightclub promotion, and mobile phone spam promoting car sales companies, were tackled in this manner.

International cooperation

56. Spam is a global problem that requires a global solution. While each country needs to start by combating spam within its own jurisdiction, as Australia and others are doing, it is also important to work internationally to share solutions and intelligence, improve the security of the network and cooperate to close down international spam havens. The objectives of international cooperation can, subject to the legal provisions of the cooperating regimes, include direct law enforcement co-operation; however, the overall objective is to make the sending of spam simply bad business. If this can be achieved the practice will stop, regardless of legislation.

57. Through 2004 and 2005, the Australian anti spam regulator has engaged in regular bilateral discussions with regulators in like-minded countries. At a broader multilateral level, Australia's agency worked cooperatively with regulators around the world to share information on technical, policy and educational solutions to the spam problem, as well as intelligence sharing and cross-border enforcement.

58. In April 2005, the ACA and the Korea Information Security Agency (KISA) became two of the founding signatories to a multilateral agreement to cooperate against spam, which was based on the existing bilateral Memorandum of Understanding (MoU) signed by the two agencies in October 2003 (before Australia had any anti-spam legislation). The Seoul-Melbourne Agreement, which is being promoted by the ACA and KISA, brings together 12 anti-spam agencies from 10 Asian region jurisdictions. The ACA was pleased to provide the first secretary to the MoU.

59. Other international anti-spam work of the ACA has included:

- Cooperation on cross-border enforcement under a trilateral MoU between regulators in Australia, the United Kingdom and the United States;
- Continued participation in the London Action Plan network of law enforcers, involving regular communication and intelligence communications between members of LAP
- Support to anti-spam programs launched by other jurisdictions, such as the US Federal Trade Commission's Operation Zombie Drone;
- Promoting the debate among global regulators on spam at the ITU. The ACA also supported other anti-spam discussions and activities organised under the auspices of the ITU, OECD, APEC TEL and ASEAN;

- Facilitation and encouragement of future agreements between the Australian Internet Industry Association and ISP bodies in other Asian region jurisdictions;
- Referral of spam originating outside Australia to relevant overseas agencies;

60. Looking to the future, it is possible to make some observations about prospectively useful actions. The following is a collection of such observations and some suggestions about how Australia's anti-spam work could align with that of other nations that have an anti spam objective.

61. The fact that multiple international bodies (such as ITU, OECD and APEC among others) run largely parallel streams of activity on spam is demanding of the resources of the bodies themselves, and also of their members, to the extent that memberships overlap. Like many countries, the resource demands experienced by the Australian regulator in the course of supporting these worthwhile initiatives are a challenge. The following proposals could be useful in this regard:

- Members of such organisations could encourage a practical sharing of the tasks and the holding of common meetings on respective anti spam tasks. Members could then plan a single meeting attendance schedule for relevant meetings to best use available resources and maximise effect.
- The five layer strategy enunciated in the Resolution from the ITU World Telecommunication Standardization Assembly (Florianópolis, 2004) should be the basis of continued international efforts, and may offer a means of partitioning tasks.
- One urgent focus of international efforts should be to encourage and assist jurisdictions to pass laws and adopt anti-spam policies. In many smaller jurisdictions, legislation may never be used against a local spammer if almost all the spam they receive comes from international sources but legislation will be necessary across the board to underpin local and coordinated international action. Additionally, legislation will act as a deterrent to ensure the jurisdiction does not become a future spammer haven; legitimise action by ISPs within networks; and signal to ISPs and mobile carriers that they are not expected to carry the entire burden of the fight against spam.
- Another necessary goal is to assist national anti spam regulators to focus efforts at the industry, operational and practitioner level of international cooperation. Alongside the need for legislation, there is a clear parallel need for ISP action within networks. International activities in the field of technical work and ISP operational action could be based on:
    - Encouragement and facilitation of international cooperation between national Internet Industry Associations and members;
    - Increased liaison between the national regulators and national CERT bodies on IT security threats, possibly involving coordination with the international CERT community on specific issues directly relevant to spam or communications network integrity and for example the Japanese and S. Korean ISACs (ISP Information Sharing and Analysis Centres);
    - Direct coordination among practitioner-level regulators to share successful anti-spam programmes, including those of ISPs, relevant codes of practice, public reporting systems (e.g. the SpamMATTERS system in Australia) and other relevant programs (e.g. the Australian Internet Security Initiative);

- Separately, discussions on international enforcement cooperation have highlighted that there are broad policy-level concerns that inhibit enforcement action. These will need to be steered internationally at Ministry level, possibly in fora not linked to the anti-spam debate. Matters to consider include cross-border enforcement of judgments and court orders; and the ability of regulators to share information across international borders where that information was obtained under judicial or statutory powers.

62. For its part the Australian anti-spam regulator has its near-term operational and practical focus as follows.

- Continue to engage in, and expand, the Seoul-Melbourne MoU of agencies with the near-term target of including those jurisdictions that are already part of APCERT (the Asia-Pacific CERT network). The MoU was constructed for easy extension, for both operational use and to support the action and cooperation message to jurisdictions yet to address spam;
- Continue to engage with the US, UK and Australia MoU or any successor of that agreement; and
- Continue to participate in the London Action Plan network of law enforcers, and relevant actions that flow from it.

63. Our experience has been that investigations into global spam operations are highly resource-intensive, and that there may be real benefits to regulators if they are able to pool resources and share investigative tasks. As international agreements extend, we will be looking to see whether we can work jointly with our MoU partners on investigations into global spam operations that have Australian connections; and to discover to what extent the inhibitors mentioned above (for example, restrictions on sharing information) may need to be referred to Ministries for international policy consideration. Examples of global spam operations of interest could be former Australian spammers who have moved offshore; and foreign spam operations with Australian associates, using Australian servers or Australian fulfilment companies, or moving money through Australia.