

CONFIDENTIAL DRAFT

SPAM REVIEW: INTERIM REPORT BY NOIE

Introduction

The Government wants to ensure that, with the continuing expansion of Internet usage in Australia, spamming does not get out of hand.

Senator Richard Alston, Minister for Communications,
Information Technology and the Arts

At the request of the Minister for Communications, Information Technology and the Arts, the National Office for the Information Economy has reviewed the extent of the “spam” problem, the adequacy of current measures to counter it and possible additional measures. Spam is essentially unsolicited electronic messages sent in bulk, usually indiscriminately.

Summary of Draft Recommendations

A clear and widely accepted working definition of “spam” to better inform and empower anti-spam enforcement at the consumer, ISP, industry and government levels should be developed for consistent interpretation.

The IIA and its ISP members should be encouraged to:

- *build on existing work done by the IIA and implement Codes of Practice to deal with spam;*
- *develop better practice guidelines for ISPs (and their customers) to combat spam; and*
- *further develop strategies to close open relays.*

Reduce the capacity for spammers to hide behind anonymous accounts, through the implementation of technologies such as Caller Line Identification (CLI) and an identification requirement (under the proposed Better Practice Guide for ISPs) for prepaid accounts.

It is recommended that the Internet industry consider managing a self-regulated list of known spammers through which ISPs may make better informed decisions about whether or not to provide Internet services to individuals with a record of sending spam.

Filtering options and products should be properly evaluated and publicised by the Internet industry to better inform Internet users of the technical options available to them. ISPs should be encouraged to offer their customers cost-effective filter and firewall products. Government, industry and the community should remain aware of the anti-spam opportunities presented by new technologies.

CONFIDENTIAL DRAFT

Regulatory agencies, in particular ACCC, ASIC and the OFPC, are encouraged to be pro-active in interpreting and applying existing laws to spam and provide additional resources to this task.

NOIE and ACCC should work with other Australian agencies and partner-country agencies such as the FTC and the International Marketing Supervision Network to improve international co-operative mechanisms in relation to anti-spam enforcement operations.

NOIE and the Attorney-General's Department should work with the OECD, APEC and/or other relevant IGOs or foreign governments to develop international guidelines and co-operative mechanisms for dealing with spam.

Clarification of the application of the NPPs to spam should be obtained during the upcoming 2003 review of the Privacy (Private Sector) Amendment Act 2001.

The NPPs should be adjusted during the upcoming review in 2003 to close loopholes detailed in this review and thereby ensure Privacy legislation best protects the privacy of Australians as it relates to spam.

The Trade Practices Act should be reviewed to optimise its potential as an effective tool against spam that is misleading or deceptive. For example, with regards to:

- Spoofing under section 52; and*
- Misleading privacy statements (with a view to being consistent with the Privacy Act).*

“Extraordinary e-mail” should be defined, during the upcoming review into the operation of Schedule 5 “Online Services” of the Broadcasting Services Act, so that spam that may be offensive is covered by any complaint regime.

The Government should consider three new legislative options in further detail, consulting with stakeholders and the public, to determine if new legislation is in the public interest and, if so, what form this should take.

In conjunction with stakeholders, such as the ACA, IIA, Treasury, ASIC, ACCC and the OFPC, NOIE should design and manage a campaign geared towards spam that creates awareness, provides accurate information and useful resources to consumers (possibly developed in conjunction with related e-security campaigns)

Regulatory agencies and NOIE should develop together a comprehensive guidance on how existing legislation can be applied to counter spam.

In the interest of continued monitoring of spam and the effectiveness of any counter-measures, NOIE should continue to obtain similar data each year and develop longitudinal analyses of progress of various measures in combating spam.

CONFIDENTIAL DRAFT

Why a review into spam?

While spam is an increasing problem for the ICT industry and business users of the Internet, it has become a major and costly nuisance to individual Internet users (consumers). Here are some typical responses to NOIE's online survey from Australian firms and individuals:

Some Australians' Opinion on Spam

It requires Internet resources and user time to deal with. It costs real money to support and those that send it bear none of the costs.

**Alistair James
STM Consulting**

I would love to see a technical equivalent of the "No Junk Mail" sign, that would signal to the e-mail delivery mechanism that junk mail was not wanted here.

**Michael Jerkovic
Orica**

The increase is more than tenfold, in my experience. Where once I might receive perhaps one spam in thirty messages, now it is more like twelve spam in thirty messages.

Roman Orszanski

I have never requested to be put on any mailing list for porn or gambling [spam] yet I receive spam every day. I don't want it, I never asked for it, and I can't stop it.

Jason Cuffe

Spam is an incremental cost, but still an increasing one. The misguided advocates of the "just hit delete" philosophy don't seem to realise that we have to do this between twenty and one hundred times per day.

Andrew Harcourt

An AC Nielson survey commissioned by NOIE shows that by April 2002 more Australian consumers see spam as a bigger problem when using the Internet than anything else including privacy and computer viruses¹. About 38% of consumers surveyed (up from 11% in November 2000) put the combination of spam and privacy (often associated with spam as a problem) ahead of viruses (about 13%).

Furthermore, other figures suggest that the amount of spam being received by Australians is rapidly escalating. The Coalition Against Bulk E-mail (CAUBE) survey on spam suggests that the amount of spam being received is doubling every 4 ½ months and that amount increased sixfold between 2000 and 2001². CAUBE has recently advised NOIE

¹ Attachment A page 6

² <http://www.caube.org.au/spamstats.html>

CONFIDENTIAL DRAFT

that the amount of spam received in their survey is continuing to grow with approximately a 20% in the year to date (19 June 2002). "Brightmail estimated a year ago that spam constituted 10% of all e-mail. That figure has jumped to 20%"³.

Spamming is the scourge of electronic-mail and newsgroups on the Internet. It can seriously interfere with the operation of public services, to say nothing of the effect it may have on any individual's e-mail mail system. ... Spammers are, in effect, taking resources away from users and service suppliers without compensation and without authorization.

**Vint Cerf, Senior Vice President, MCI
and acknowledged "Father of the Internet"**

How was the review conducted?

This review has been conducted in close consultation with a range of Commonwealth agencies, industry, community organisations and the general public.

Initially a meeting of relevant government agencies was held to develop a better understanding of how existing Commonwealth legislation dealt with spam. Following this meeting, consultations with the Internet Industry Association (IIA) representing the Internet Service Provider (ISP) industry and some of its members were held. Their input is central to developing a better understanding of the technical and commercial conditions in which spam operates and in designing strategies to better manage spam.

The second stage of the review centred on a comprehensive roundtable of key stakeholders from government, industry and community sectors in response to a Preliminary Issues Paper prepared by NOIE. Additionally, the public were invited to submit comments and/or complete an online NOIE survey. As of mid June 2002, about 350 members of the public had provided input to the spam review.

The Minister has considered NOIE's review and has decided that its findings and preliminary recommendations be released for industry and community reaction and to test their commercial, technical and consumer feasibility. He will then announce the Government's approaches to tackling the spam problem in cooperation with stakeholder groups and international bodies.

While the review has focussed on domestic regulatory frameworks we should bear in mind that the bulk of spam is sourced outside Australian jurisdiction and is therefore difficult to control. The Australian Consumer and Competition Commission has some experience in participating in cross-border co-operative arrangements with the US Federal Trade Commission (FTC) to combat Internet scams, and this review proposes further bilateral and multilateral cooperation, both at government and industry level. At the same time, we should not expect that beneficial international results will occur until the medium term.

³ <http://stacks.snbc.com/news/713079.asp>

Spam Review by NOIE: Terms of Reference

1. Investigate and Assess Nature and Extent of Spam

- Define "spam" - Government is concerned about bulk e-mailing that is clearly inappropriate or unwanted in particular but not exclusively those containing illegal, offensive or deceptive content, or those that incorporate personal information collected or used in breach of legislated privacy obligations.
- Identify major problems or risks with spam - inappropriate content, privacy breaches, vehicle for fraud or deceptive commercial conduct (including spoofing), undue cost to ISPs and recipients, damage to Internet functionality (eg overload or slowing of Internet network and sites, denial of service attacks) - what are the major sources and risks warranting priority attention?
- Assess relative extent of problem with various types of spam.
- Assess trends in spam - estimated growth, type and source.

2. Identify and Assess Existing Australian Counter-Measures

- Content-based legislation (Broadcasting Services Act, Interactive Gambling Act)
- Privacy legislation
- Crimes Act (and Cybercrimes Act).
- Consumer protection legislation (Trade Practices Act and Corporations Act) and ACCC and ASIC investigations
- Industry codes - both co- and self-regulatory – could the ISP industry do more?
- ISP action against spammers, and commercial terms in subscriber contracts
- Technical tools such as filters and Caller ID, browser settings.
- Consumer awareness measures by consumer movement, industry and government
- Others?

3. Identify and Assess Overseas Counter-Measures

- For example the US and EU.

4. Possible New or Improved Counter-Measures

- Identify most likely and cost-effective counter-measures—the most appropriate balance of regulatory, co-regulatory, self-regulatory, user awareness
- International cooperation measures; eg multilateral guidelines, bilateral enforcement arrangements.

CONFIDENTIAL DRAFT

What is spam?

An agreed working definition, or at least criteria for characterising spam, is important to making many anti-spam provisions effective. ISPs and law enforcement authorities need to be reasonably confident of this definition before they enforce their terms and conditions or any laws against spammers as would legitimate direct marketers who want to ensure their activities remain ethical or appropriate.

The definition of spam, an almost exclusively negative term, is contentious with ISPs, the direct marketing industry, spammers, blacklisters and consumer groups all taking positions. However, key stakeholders appear to have an interest in establishing a working definition that is widely recognised:

- The Internet industry has specifically requested that the Commonwealth provide some official support in this matter through the development of a definition that enjoys wide acceptance; and
- The direct marketing industry has an interest in differentiating its communications and legitimate products from spam.

Outlined below is a working definition developed by NOIE for the purposes of the review.

Working Spam Definition

Spam is the common reference to unsolicited bulk electronic messages, usually electronic mail messages but increasingly "pop-up messages on web pages and SMS messages (text messages delivered to mobile phones), that are transmitted to a large number of recipients who generally have not requested those messages. They are usually - but not necessarily - commercial in nature; ie, they generally promote or sell products or services.

The bulk of spam messages also share one or more of the following characteristics:

- they are sent in a largely untargeted and indiscriminate manner;
- they include or promote illegal or offensive content;
- their purpose is fraudulent or otherwise deceptive;
- they collect or use personal information in breach of the National Privacy Principles (the recent extensions of the Privacy Act to business);
- they are sent in a manner that disguises the originator; eg, from an Internet address other than that shown in the message as received, often involving the unauthorised use of an innocent third party's e-mail server; and
- they do not offer a working address to which recipients may send messages opting-out of receiving further unsolicited messages.

While such characteristics are not essential to whether a message should be regarded as "unsolicited" or sent in "bulk", most commentators would probably *not* regard as spam direct marketing communications with *all* the following characteristics:

- they do not include promote or include illegal content;
- they are not deceptive in any way that would breach common law or statute law;

CONFIDENTIAL DRAFT

- they do not collect or use personal information in breach of the NPPs; and
- they are sent to recipients who have dealt voluntarily with the sender before and, on the basis of that existing relationship, can reasonably be assumed by the sender as prepared to accept messages of the type being sent (ie, the messages would not be unwelcome or unexpected).

Clearly, when an informed decision is made by Internet users to accept commercial e-mail it, by definition, is not unsolicited and can be an effective marketing communications and customer relationship tool.

Whilst e-mail is the most significant channel of spam through the sending of Unsolicited Bulk E-mail (UBE) or the more narrowly defined Unsolicited Commercial E-mail (UCE), spamming can occur using other vehicles, in particular SMS messages to mobile phones and through “pop-up” Internet messages.

SMS spamming is currently less problematic than e-mail spam, largely because of the cost of this channel to the sender. Should the cost of SMS be reduced, as some telecommunication companies have considered, SMS spam could become a greater problem. An official definition of spam therefore needs to cover, probably in a technologically neutral way, these various delivery channels.

SMS Spam

NOIE does not view SMS spam as a significant issue for Australians at the moment, largely due to the different cost structures it faces to e-mail spam. Nevertheless, NOIE will continue monitor developments and respond/report accordingly.

Thought also needs to be given as to who is defined as a spammer or at least who is held responsible for spam from a regulatory standpoint. Often the person(s) physically sending a spam message and the beneficiaries of the spam message are different. For example professional spamming outfits are frequently contracted to send spam on behalf of third party beneficiaries. As such, further consideration needs to be given as to how the regulatory regime deals with each of these parties.

Major Problems Caused by Spam

Spam poses a series of challenges to both Internet users and regulatory agencies. It is a medium that is characteristically anonymous, indiscriminate and global. As such spam has become a popular vehicle for promotions that may be illegal or unscrupulous using tactics that would not be commercially viable outside the virtual environment.

The key issues raised by spam include **privacy, illegal and/or offensive content, misleading and deceptive trade practices** and **network issues**. The US Federal Trade Commission estimates roughly half of all unsolicited commercial e-mail contains fraudulent or deceptive content.

CONFIDENTIAL DRAFT

Content- Pornography, Illegal Online Gambling and Unlawful Trade Practices

There are obvious community and regulatory agency concerns with the illicit content of a considerable amount of spam— including those that promote pornography⁴, illegal online gambling services, pyramid selling, get rich quick schemes or misleading and deceptive trade practices.

Privacy

There are significant privacy issues surrounding the manner by which e-mail addresses and personal information are collected and handled. Address collectors harvest e-mail addresses off the Internet, collect them as users visit certain Internet sites, and buy and sell them in bulk without the consent of the owner.

Spoofing

Some Australian businesses are being 'spoofed' by spammers. When nuisance e-mail is being routed through, and appears to come from, those firms, their commercial reputation is then at risk, and their owners and managers are obliged to allocate significant time and resources rectifying this, including responding to annoyed spam recipients.

Employer Costs

It is estimated that the cost of time spent in opening and reading spam in the workplace averages \$960 per employee p.a.⁵.

Technical and Network Issues

Regardless of the content of a spam message, there are series of technical and network issues created by it. The cost of spam is born by the recipient in the form of larger downloads (and/or by the ISP in terms of greater bandwidth costs) and the time cost of deletion. Many businesses are starting to appreciate the significant cost of spam through lost employee time. The increased volume of e-mail can significantly slow Internet speeds, overload servers and threaten network integrity. Spam may also be used maliciously as a means of transmitting viruses or for use in Denial of Service (DoS) attacks.

Blacklists and Blockades

Spam issues are also complicated by anti-spam blockades, established by some online groups in reaction to growing netizen concerns about spam. These blockades often have the effect of arbitrarily blocking innocent Internet users that are connected through blocked ISPs. There have even been cases of entire country domains being blockaded.

⁴ Pursuant to the Broadcasting Services Act, the ABA received 215 complaints and took action against 190 items of prohibited and potentially prohibited content both in Australia and abroad in the six months to June 2001.

⁵ Joey Gardiner "Spam Costs UK £ 3bn a Year"(4 December 2001):
<http://www.silicon.com/bin/bladerunner?30REQEVENT=&REQAUTH=21046&14001REQSUB=REQINT1=49713>

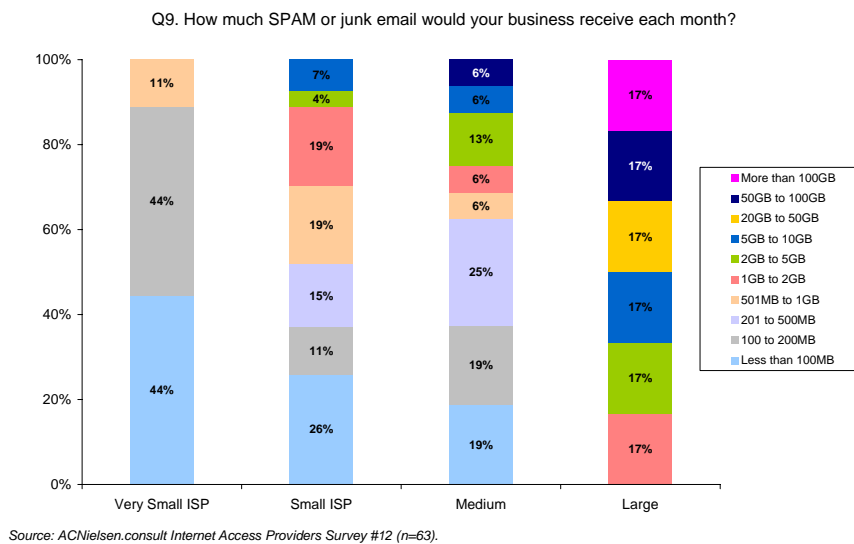
CONFIDENTIAL DRAFT

Larger Australian ISPs especially are concerned about the operation of anti-spam "blacklists" and "blockades". These are seen by ISPs as unregulated groups that have established websites where complaints about spammers can be sent by Internet users. Based on their own criteria (often without due regard for due process) IP addresses, often encompassing large numbers of innocent individuals that reside online near the alleged spammer, are listed and blocked by subscribing webmasters. Whilst some users have felt empowered by these groups, many ISPs argue that it has had the effect of victimising the wrong people, including:

- ISPs that host spammers unawares;
- Internet users that may have been spoofed by a spammer— an increasingly common tactic used by net savvy spammers. In effect they get victimised twice;
- Internet users that neighbour the address the blacklists perceive the spammer to be using and are blocked in addition to the perceived spammers address; and
- Anyone accused of spam that does not enjoy due process from these groups.

Size and Shape of the Problem

ISP Research (excluding Very Large ISPs)



The figure above shows that the spam being received by ISPs is using significant amounts of bandwidth.

CONFIDENTIAL DRAFT

Based on the estimate that the average e-mail is 5 kilobytes each⁶, a gigabyte of spam represents 200000 individual messages. The table above shows that many of the medium to large ISPs are receiving 4 million plus spam messages a month on behalf of their customers.

The Coalition Against Bulk E-mail (CAUBE) tracking of the amount of spam received at their survey e-mail address grew in volume by a factor of six in 2001⁷.

Spammers bear very few of the costs associated of sending spam, with the bulk of these being transferred to the recipient, the recipient's employer and/or their ISP.

What percentage of e-mails are spam?

A June 2001 Gallop Poll Study on e-mail usage in the US (and we are assuming the situation in Australia reflects this by virtue of the global nature of the Internet) found that spam accounted for 20% or more of all e-mail received for 54% of US e-mail users. It is likely that this proportion is increasing if spam volumes are indeed rapidly growing as is widely believed. Figures put out by Brightmail Inc, the spam filtering company to WorldNet, similarly estimate that spam volume has doubled in the past 12 months accounting for 20% of all e-mail.

What content does spam contain?

The tables below suggests that the Pornography and "Get Rich Quit" categories are the most dominant forms of spam.

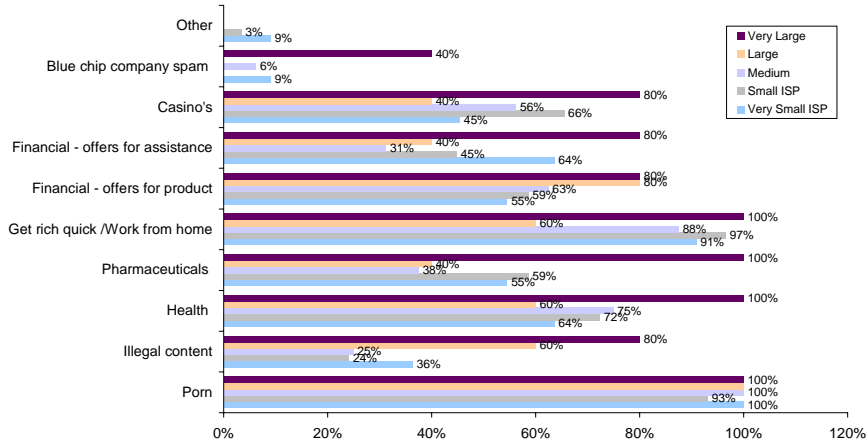
⁶ To determine the average size of a SPAM e-mail AC Neilson.consult looked into both ISP and free e-mail accounts and took the low and high point (1 and 30 kilobytes). We added up all messages in kilobytes and added overhead packets and divided by the number of messages to get the number of e-mails likely to be received by the average user each month.

⁷ <http://www.caube.org.au/spamstats.html>

CONFIDENTIAL DRAFT

ISP Research

Q13. Which industry sectors are the major source of SPAM or junk email received by your business?



Source: ACNielsen.consult Internet Access Providers Survey #12 (n=68); Very Small ISP (n=12), Small ISP (n=30), Medium ISP (n=16), Large ISP (n=5), Very Large ISP (n=5).



Do not copy without permission Copyright 1996 - 2002 ACNielsen.consult

18

A sample database by the Spam Recycling Centre, 1999, showed the following spam categories:

| Spam categories | No. of messages | % of total |
|--|-----------------|---------------|
| Pornography | 29,884 | 30.2% |
| Money making/Get rich/Work from home | 29,365 | 29.6% |
| Other direct product or service/Misc. | 23,326 | 23.5% |
| Become a spammer | 4,200 | 4.2% |
| Gambling/Sweepstakes | 3,279 | 3.3% |
| Health/Cures/Weight loss (including Viagra at 2,103) | 9,804 | 9.9% |
| Totals | 99,858 | 100.7% |

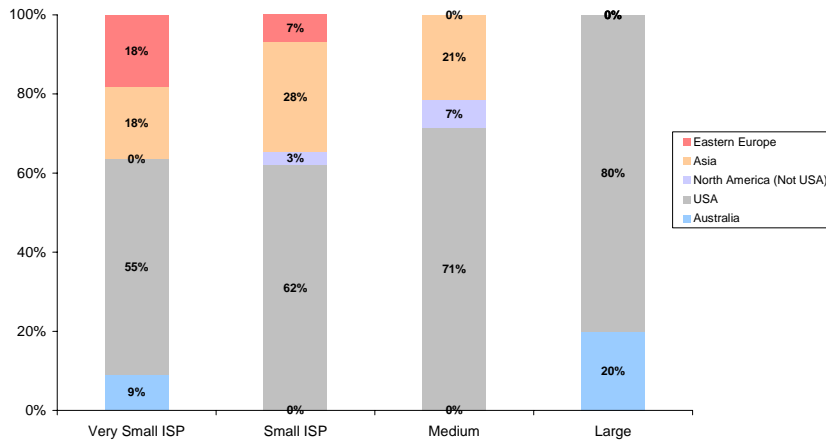
Source: eMarketeer

Note: Category totals exceed sample total due to records appearing in multiple categories.

Where is spam coming from?

ISP Research (excluding Very Large ISPs)

Q12. Where does the majority of SPAM or junk email your business receives originate from?



Source: ACNielsen.consult Internet Access Providers Survey #12 (n=63).



Do not copy without permission Copyright 1996 - 2002 ACNielsen.consult

17

The Table above shows the majority of spam received by Australian ISPs originate from the United States with Australia, Asia and Eastern Europe sending lesser amounts.

Another estimate by CAUBE states that Australia accounts for about 16% of all spam sent globally, far in excess of its share of the online population⁸.

Notably Western Europe, which traditionally has had relatively strong laws regarding privacy and has recently passed an EU directive requiring a qualified Opt-In for commercial e-mail, was not regarded by any Australian ISP as being the majority source of spam they receive.

How quickly is the volume of spam in Australia growing?

Whilst users will receive different quantities of spam depending on the availability of their e-mail address, their Internet use habits and security awareness, there is evidence to suggest that the average incidence of spam received by each Australian Internet user is

⁸ <http://www.caube.org.au/australia.htm>

CONFIDENTIAL DRAFT

growing rapidly. One survey, by the Coalition Against Unsolicited Bulk E-mail (CAUBE), states that spam has grown sixfold during 2001⁹.

This growth may partially be a product of the length of time Australian users spend on the Internet and have possessed their e-mail address for.

Additionally, the number of Australian businesses now online is very high. According to the Australian Bureau of Statistics (ABS), Internet connectivity levels reached 69% of all businesses (nearly 500,000 businesses) at June 2001. This was an increase of 175 per cent since June 1998. For businesses employing 20 or more persons, connectivity levels were above 90 per cent.

At the same time, in this environment of high levels of adoption of the Internet by the business sector, Australian firms are increasingly using the Internet for marketing purposes in order to reach the growing online audience in Australia and overseas.

The ABS estimates that at June 2001, 125,221 businesses (26 per cent of all online businesses in Australia) reported using the Internet for marketing purposes. This was a 221 per cent increase over the June 1998 estimate. It is therefore safe to assume that the demand for the specialist services of direct marketers will also increase as more and more businesses seek assistance in maximising the benefits of the Internet as a relatively inexpensive mass-marketing tool.

| Australian business using the Internet for promotional activities | | | | |
|--|---------------|---------------|---------------|-------------------------------|
| | <i>Jun-98</i> | <i>Jun-00</i> | <i>Jun-01</i> | <i>% change since June 98</i> |
| Number of businesses online | 174,870 | 358,960 | 481,620 | 175.4 |
| % of businesses online | 29% | 56% | 69% | |
| Number of businesses using Internet for marketing / promotional activities | 40,220 | 96,919 | 125,221 | 211.3 |
| % of businesses online using Internet for marketing / promotional activities | 23% | 27% | 26% | |

(Source: Australian Bureau of Statistics. Business Use of Information Technology, Australia (ABS catalogue no: 8123.0))

⁹ <http://www.caube.org.au/survey.htm>

CONFIDENTIAL DRAFT

How much does spam cost?

Overseas studies are showing that spam has a real economic cost. An EU study estimates that the worldwide cost to Internet subscribers of spam is in the vicinity of A\$16.8 billion a year¹⁰. According to the latest figures from ISP Star Internet the cost to business in lost productivity is A\$960 per employee each year¹¹. These sort of costs are usually born by Internet users (and/or employers), through increased download times and costs and lost productivity, rather than the spammers themselves.

Conversely evidence suggest it only costs the sender of spam 0.00032 cents to obtain one e-mail address¹².

Spam Review: Key Findings

1. **Spam is a significant and growing problem.** Already it accounts for something in the order of 20% of all e-mail sent and evidence suggests that this is growing rapidly. There are significant productivity costs born by the community as well as challenges to regulators in a variety of policy areas as a result of spam.
2. The **core challenge of spam is the low cost to the sender** as the recipients of spam pick up the vast majority of the cost of sending it. This is the result of Internet architecture and is unlikely to be easily resolved. Nevertheless there may be some scope for the industry to reverse this anomaly in some way.
3. Whilst many in the community are calling for **legislation**, this is **no silver bullet**. Although, legislation may, form part of a strategy to control spam, legislation banning spam outright (as many have called for) will not eradicate or minimise spam given the difficulties in identifying spammers, the global nature of the Internet and the competing enforcement priorities faced by regulatory agencies.
4. Nevertheless, **Australia can establish a strategy to reduce spam** that finds the right balance of regulatory, self-regulatory, technical and consumer awareness approaches. Ideally, this would involve:
 - proactive interpretation, application and enforcement of *existing* criminal and consumer protection laws that can assist in more serious or blatant cases;
 - development of technical and consumer awareness strategies which should at least be moderately effective in reducing nuisance to consumers if it does little to reduce the total flow of spam. This may include:

¹⁰ Commission of the European Communities Unsolicited Commercial Communications and Data Protection: Summary of Study Findings January 2001 page 9 (Note: Currency Conversion from Euros to Australian Dollars on 22 February 2002).

¹¹ Joey Gardiner "Spam Costs UK £ 3bn a Year"(4 December 2001):
<http://www.silicon.com/bin/bladerunner?30REQEVENT=&REQAUTH=21046&14001REQSUB=REQIN T1=49713> 4 December 2001.

¹² <http://www.gip.org/publications/papers/Spam061802.asp>

CONFIDENTIAL DRAFT

- the development of more broadly available and used consumer guides to careful Internet behaviour and anti-spam products
 - the encouragement of third party testing of standards and seals; and
 - Possible linking of anti-spam approaches with a more general e-security campaign to capitalise on synergies between the two issues.
5. The international dimension of spam makes it necessary that this strategy fit in with **broader international counter-measures** that need to be developed. These will inevitably take longer to design, negotiate and implement. Australia may wish to make a contribution to this process.

Key Issues and Draft Recommendations

Whilst there is no single solution to combating spam, this review seeks to develop a strategy that is aimed at increasing the costs faced by spammers—the minimal costs faced by spammers being the key enabler of their business. NOIE proposes a strategy that employs regulatory, self-regulatory, technical and consumer awareness approaches and closely works with key players, such as the ISP industry, to do so.

The strategy provides both short and long term options. In the short term the strategy provides a series of options to counter domestic spammers. For the longer term the Government and industry might work on developing, in co-operation with other states, an international strategy that can more effectively deal with spam as an international issue.

Government Agencies and Spam

The Commonwealth Government requires all agencies in its jurisdiction to implement the long-standing privacy standards for government websites incorporated in the Federal Privacy Commissioner's Guidelines for Federal, ACT and Government Websites (ref: <http://www.privacy.gov.au/internet/web/index.html>).

The Guidelines suggest a model privacy policy be posted to all agency websites along these lines:

We will only record your e-mail address if you send us a message. It will only be used for the purpose for which you have provided it and will not be added to a mailing list. We will not use your e-mail address for any other purpose, and will not disclose it, without your consent.

How should regulators define spam?

NOIE has established a working definition for the purposes of this paper (as detailed on pages 6 and 7) and in response to stakeholder requests to develop a clearer working definition of spam to advance more coherent regulatory action.

Recognising that this is a contentious issue, NOIE is mooted that the working definition outlined earlier in this paper serve as a starting point for further discussion amongst stakeholders. Operational issues about how and when consent is expressed or implied may benefit from clarification between marketers and consumers, facilitated as appropriate by agencies such as the NOIE, Treasury, Attorney General's Department and the Office of the Federal Privacy Commissioner (OFPC).

CONFIDENTIAL DRAFT

DRAFT RECOMMENDATION:

A clear and widely accepted working definition of “spam” to better inform and empower anti-spam enforcement at the consumer, ISP, industry body and government levels should be developed for consistent interpretation, based on the above analysis.

Encouragement to Industry to Introduce more Effective Counter Measures against Spam

The IIA has developed a comprehensive draft Code of Practice that covered spam. However this Code was superseded by a series of Codes of Practice that dealt with other specific regulatory issues— none of which included spam. As such NOIE recommends the IIA implement Codes of Practice that deal with spam, possibly building on past work.

Telstra Bigpond's Terms of Use Regarding Spam

2.1 You must not:

- (a) use telstra.com for any activities or post or transmit to or via telstra.com any information or materials which breach any laws or regulations, infringe a third party's rights, or are contrary to any relevant standards or codes;
- (b) use telstra.com in a way or post to or transmit to or via telstra.com any material which interferes with other users or defames, harasses, threatens, menaces, offends or restricts any person or which inhibits any other user from using or enjoying telstra.com;
- (c) use telstra.com to send unsolicited electronic mail messages to anyone;
- (d) to make any fraudulent or speculative enquiries, bookings, reservations or requests using telstra.com;
- (e) use another's name, username or password without permission;
- (f) post, or transmit via telstra.com, any obscene, indecent, inflammatory or pornographic material or material that could give rise to civil or criminal proceedings;
- (g) tamper with, hinder the operation of or make unauthorised modifications to telstra.com;
- (h) knowingly transmit any virus or other disabling feature to telstra.com; and
- (i) attempt any of the above acts or permit another person to do any of the above acts.

The clauses of Telstra's terms of use (or AUP) detailed above is typical of Australian ISPs and demonstrates the Internet industry's commitment to reducing spam and the kinds of suspect goods and services that spam often promotes. Nevertheless, this review would like to see better practice guidelines on spam for ISPs be developed and included in the IIA Codes of practice.

Amongst other things, these guidelines would ideally encourage ISPs:

- to remain vigilant against customers that are found to be sending spam and enforce anti-spam conditions in their Authorised Use Policies (AUPs);
- to report spammers hosted by other ISPs to their hosts;
- to continue improvement, within the confines of cost-effectiveness, of filtering technologies as part of the technical "arms race" with spammers;
- to make filtering options readily available to consumers possibly bundled with other products to ensure ease of access and affordability; and,

CONFIDENTIAL DRAFT

- to restrict the availability of pre-paid accounts without the presentation of evidence of identity sufficient to allow the ISP or law enforcement agency to investigate breaches of commercial terms or regulatory requirements.

In the context of developing these guidelines consideration needs to be given to combating open relaying, preferably at the industry level. Open relays have been identified as a significant enabler of spam. Individual ISPs are devoting considerable resources to assisting customers in shutting these down in an effort to reduce spam and prevent customers from being spoofed. This strategy may include aspects of consumer awareness, changes to AUPs or, in association with US ISPs, further efforts to encourage Microsoft to make its mail servers and associated products significantly more secure against hacking and spoofing.

Although it is recognised that hackers (which includes many spammers) can readily hack into a computer to open a closed relay, developing a strategy to have Internet users keep these closed makes:

- spamming more difficult; and,
- should the spammer hack into another person's computer to change their relay settings, places them in breach of the criminal law under provisions in the Crimes Act.

DRAFT RECOMENDATIONS:

The IIA and its ISP members should be encouraged to:

- *Build on existing work done by the IIA and implement Codes of Practice to deal with spam;*
- *develop better practice guidelines for ISPs (and their customers) to combat spam; and*
- *further develop strategies to close open relays.*

The IIA and its ISP members should be encouraged to reduce the capacity for spammers to hide behind anonymous accounts, through the implementation of technologies such as Caller Line Identification (CLI) and an identification requirement (under the proposed Better Practice Guide for ISPs) for prepaid accounts.

NOTE: DCITA, Telstra and the IIA are currently discussing CLI in the context of the Law Enforcement Agencies Council (LEAC). These discussions have yet to be concluded and therefore this recommendation is **NOT FOR PUBLIC RELEASE** at this stage.

It is recommended that the Internet industry consider managing a self-regulated list of known spammers through which ISPs may make better informed decisions about whether or not to provide Internet services to individuals with a track record of sending spam.

This draft recommendation is reliant on:

- reducing the ability of individuals to obtain access to the Internet anonymously. This would require:

CONFIDENTIAL DRAFT

- ISPs to obtain identification of users when selling prepaid accounts (possibly to be included in a Better Practice Guide on spam for ISPs); and
- the implementation of tracing technology such as Caller line Identification (CLI);
- establishing a widely accepted working definition of spam; and
- establishing due processes for adding and removing individuals from the list.

This list would be a significant improvement on unregulated blacklists that currently operate. Consultations with ISPs have suggested that these blacklists have been a blunt tool that in effect often victimised innocent Internet users, many of whom had already been spoofed by the offending spammer.

What role can technical tools play in countering spam?

There are several types of technical tools that may help filter or block unwanted e-mail messages. Several software makers and distributors approached the inquiry, with claims about their products. NOIE was not in a position to assess these products and is not aware of any third party objective criteria for evaluating products. It would however be useful for consumers to have ready access to a trusted source of advice about such products; eg an independent testing authority or industry association.

Filters may be applied either by ISPs at the level they receive mail or by consumers at their own level. The recent AC Nielsen.consult survey of Australian ISPs found that, of the five largest ISPs, only one filtered for spam before their mail servers forwarded mail to customers. One of the remaining four said it is active in encouraging its customers to employ filter products (provided through the ISP at a discounted price). Of the other smaller Australian ISPs, most employed filters before forwarding mail, but many did not filter for *all* spam - see further AC Nielsen.consult survey, table 15.

"the over riding thoughts of the five largest ISPs in Australia on spam was that filtering it isn't a core issue at product level. Stopping customers sending and abusing open relay servers and sending SPAM is a core issue".

AC Neilson (ATTACHMENT A)

This partly reflects the fact that filtering messages costs ISPs time and money and slows network performance without reducing the number of spam messages being sent. Another general perception among ISPs is that filter products are worthwhile using at least at the consumer level but are not always easy to design, configure or install in a way which would block most spam but without blocking wanted messages. Generally speaking spammers have been adept at overcoming filtering technologies.

Customer use of other, privacy-related, tools such as anonymisers and more careful Internet habits would be expected to produce better anti-spam results; but filters still have a useful role. Another technical tool suggested as having good anti-spam potential (although not yet widely available to consumers) is to set one's e-mail client to accept only messages signed with trusted digital certificates. However, this would only be practical from a time when such certificates were being widely used.

DRAFT RECOMMENDATIONS:

Filtering options and products should be properly evaluated and publicised by the Internet industry to better inform Internet users of the technical options available to them.

ISPs should be encouraged to offer their customers cost-effective filter and firewall products.

Government, industry and community stakeholders should remain aware of the anti-spam opportunities presented by new technologies.

CONFIDENTIAL DRAFT

What scope is there to more strongly enforce existing laws against spam?

The figure below demonstrates that significant powers exist under *existing* civil and criminal laws to deter or punish the sending in Australia of electronic communications that:

- breach the National Privacy Principles in the Privacy Act
- breach the prohibitions against promoting x-rated content on websites or most forms of interactive gambling
- breach fair trading, anti-fraud and investor protection provisions in the Trade Practices Act and the Corporations Law
- breach recent Cybercrime laws such as through hacking and possibly spoofing.

Existing Regulatory and Self-Regulatory Framework Surrounding Spam

There are also a number of regulatory, self-regulatory and consumer awareness mechanisms already in place to deal with many aspects of spam. These include:

- extension of the Privacy Act to place some spam-related-restrictions on business;
- provisions in the Broadcasting Services Act for handling complaints about illegal and offensive material online;
- prohibitions in the Interactive Gambling Act of certain forms of online gambling and of advertising those services;
- measures in the Crimes Act to prevent a person being menaced or harassed or offended;
- consumer protection provisions in the Trade Practices Act;
- the Internet Industry Association (IIA) codes of practice which prohibit IIA member Internet Service Providers from sending direct marketing messages without the recipient's permission and which require the service providers to advise consumers on how to minimise spam problems; and
- The Australian Competition and Consumer Commission and the Australian Securities and Investments Commission regularly investigate e-mail scams involving financial products and therapeutic goods.

Because spam is a relatively recent problem, more thought is needed to adapt the interpretation and implementation of these provisions to electronic messages. Enforcement of existing laws has already proved possible in several Australian criminal cases such as.....(cite several recent and current Australian court cases...plus civil claim by CAUBE)

DRAFT RECOMMENDATION:

Regulatory agencies in particular ACCC, ASIC and the OFPC are encouraged to be pro-active in interpreting and applying existing laws to spam and provide additional resources to this task.

CONFIDENTIAL DRAFT

What scope is there for international co-operation in dealing with spam?

Spam is a global problem. Establishing a domestic strategy for dealing with it can alleviate the problem only in terms of spam sent from Australia. Clearly internationally co-operative measures are likely to be more effective for the majority of spam that originates outside Australia. Inevitably this will take longer to design, negotiate and implement. Nevertheless, the Government may wish to consider the following draft recommendations.

DRAFT RECOMMENDATIONS:

NOIE and ACCC should work with other Australian agencies and partner-country agencies such as the FTC and the International Marketing Supervision Network to improve international co-operative mechanisms in relation to anti-spam enforcement operations.

NOIE and AGD should work with the OECD, APEC and/or other relevant IGOs or foreign governments to develop international guidelines and co-operative mechanisms for dealing with spam.

Australia may wish to present the proposed framework of recommendations in this review, should the Government choose to accept it, as a model for further bilateral or multilateral consideration.

The EU example detailed below shows that other key trading partners are starting to take action against spam. The time may be ripe for an international standard to be established.

The OECD's *Working Party on Information Security and Privacy* may be an appropriate vehicle through which model principles may be established for consistent adoption throughout the Internet world.

Another idea, suggested by one stakeholder, was for Australia to propose an international system of government licensing for commercial UBE, something that Australia could facilitate by leading by example.

European Union Anti-Spam Measures

The European Parliament has voted to ban spamming . The Parliament agreed in May this year with the position taken earlier by the Council that unsolicited commercial communications sent by email, SMS, fax or by automated calling machines are not allowed without the prior permission of the user.

As part of the [Legislative proposals for a new Regulatory Framework for electronic communications](#) arising from the 1999 Telecommunications Review, the European Commission proposes a ban on Unsolicited Commercial Email. Specifically, this is to take the form of a requirement that advertising email be sent only to those subscribers who have given their prior consent, the same as for automated calling systems and fax.

Final Text of "E.Privacy" Directive as Passed by European Parliament

Recital 40

Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

Recital 41

Within the context of an existing customer relationship, it is reasonable to allow the use of electronic contact details for the offering of products or services, but only by the same company that has obtained the communication details in accordance with Directive 95/46/EC). When contact details are obtained, the customer should be informed about their further use for direct marketing in a clear and distinct manner, and be given the opportunity to refuse such usage. This opportunity should continue to be offered with each subsequent direct marketing message, free of charge, except for any costs for the transmission of this refusal.

Recital 44

Certain electronic mail systems allow subscribers to view the sender and subject line of an electronic mail, and also to delete the message without having to download the rest of the electronic mail's content or any attachments, thereby reducing costs which could arise from downloading unsolicited electronic mails or attachments. These modalities may continue to be useful in certain cases as an additional tool to the general obligations established in this Directive.

CONFIDENTIAL DRAFT

Article 2 - Definitions

(h) "electronic mail" means any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Unsolicited communications

Article 13.1

The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.

Article 13.2

Notwithstanding paragraph 1, where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with Directive 95/46/EC, the same natural or legal person may use these electronic contact details for direct marketing of its own products or services, provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, such use of electronic contact details when they are collected and on the occasion of each message in case the customer has not initially refused such use.

Article 13.3

Member States shall take appropriate measures to ensure that, free of charge, unsolicited communications for purposes of direct marketing, in cases other than those referred to in paragraphs 1 and 2, are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between these options to be determined by national legislation

Article 13.4

In any event, the practice of sending electronic mail for purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.

There is however an exception for legitimate direct marketing with an existing customer service relationship. Companies will be allowed to send unsolicited commercial mails where they have received the e-mail address directly from the consumer in the context of a purchase and on conditions that:

- the unsolicited e-mail only concerns their own similar products; and
- that the consumer is given the opportunity to object free of charge in an easy manner.

The Directive, however, will only apply to messages sent in Europe.

Legislative Reform

Privacy Act

While it is not yet clear the extent to which the Privacy Act will provide an effective remedy to spam recipients (despite the Commissioner's pro-active interpretation of NPP 2.1 - see box below), the Act is generally an appropriate vehicle for dealing with consumer concerns about how e-mail addresses and other personal data are collected and used.

Relevant National Privacy Principles (NPP) 1.5 and 2.1

Under **NPP 1.5**, if an organisation collects personal information about an individual from someone else other than the individual, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3. NPP 1.3 says:

At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

- (a) the identity of the organisation and how to contact it; and*
- (b) the fact that he or she is able to gain access to the information; and*
- (c) the purposes for which the information is collected; and*
- (d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and*
- (e) any law that requires the particular information to be collected; and*
- (f) the main consequences (if any) for the individual if all or part of the information is not provided.*

The matters in (a)-(f) of NPP 1.3 can be addressed in the first contact an organisation has with the individual.

Further, if an organisation has obtained one's personal information for the purpose of direct marketing, the NPPs allow it to use the information for that purpose, (the 'primary purpose' of collection) and there is in fact no legal obligation for it to offer the individual an opportunity to opt out of further offers (NPP 2.1), or for it to delete information it holds about you.

NPP 2.1

NPP 2.1(a) states that an organisation can use or disclose personal information for a new purpose if (i) the new purpose is related to the original purpose and (ii) use for the new purpose is within the 'reasonable expectations' of the individual.

NPP 2.1(c) states:

An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

(iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically;

Privacy Commissioner's Guideline Tip on NPP 2.1(c)

This allows organisations to use non-sensitive personal information for direct marketing where, among other things, it is impracticable to seek the individual's consent and where the individual is told that they can opt out of receiving any more marketing from the organisation.

This principle only applies to the use of non-sensitive information for direct marketing and does not permit an organisation to disclose personal information for the purpose of direct marketing.

Impracticable to seek consent

Considering whether it is impracticable to seek the individual's consent involves balancing a number of factors that could include:

- how often the organisation is in contact with an individual;
- the way an organisation communicates with an individual;
- the consequences for the individual of receiving the information without having consented; and
- the cost to the organisation of seeking consent.

The question of impracticability would generally be considered at the time of the proposed use of the personal information for direct marketing - not the time the personal information was collected.

As the cost of e-mailing is negligible, ordinarily it will not be 'impracticable' to seek consent where an organisation chooses on-line methods of contact or communication. This means that generally an organisation could not rely on NPP 2.1(c) for techniques such as e-mail marketing or SMS marketing. The option of using 2.1(b) is still available. However, in most cases, this will require express consent

Tips for compliance

An organisation does not necessarily need to rely on NPP 2.1(c) for use of personal information for direct marketing. An organisation could get the individual's consent at the time of collection to use information about them for direct marketing or the use might be related to the primary purpose and within the individual's reasonable expectations.

CONFIDENTIAL DRAFT

There are several components of the Privacy Act and/or the National Privacy Principles (NPPs) that could be clarified and/or tightened to better regulate the way in which spammers collect and use e-mail addresses.

- The NPPs do not prevent a business from using personal information for the primary purpose for which it is collected. Therefore if a spammer collects personal information from the individual for the primary purpose of spamming there is nothing in the Privacy Act to prevent the spammer from using this information in that way. An exception is that most spammers as such will not have gained the personal information, eg personalised e-mail address, directly from the individual so will be required to inform the individual the specified details. Also in practice, ethical direct marketers will provide a legitimate opt-out.
- The Privacy Act currently does not extend to many spammers, including those that send spam from overseas and small businesses that do not trade in personal information.
- Where e-mail addresses do not contain an individual's name they may not be regarded as personal information under the Privacy Act and therefore not covered by it.
- Clarification is needed as to what level of consent is required in the online environment. Specifically, whether the NPPs require opt-out or opt-in for Unsolicited Commercial E-mail (UCE). Any decision made on this should reflect the common perception amongst Internet users that replying to spam, as opt-out requires, may encourage more spam to be sent as the user's e-mail address has been confirmed as active.

In an "opt-in" regime, merchants must give consumers the opportunity at the start of a possible commercial relationship to veto the sending of any messages. In an "opt-out" regime, consumers may properly be sent messages as long as they have not expressed a wish not to be sent any more. It is widely perceived that the NPPs support opt-out-based marketing, but the Federal Privacy Commissioner's formal guidance on NPP 2.1 clarifies that, *in practice*, an opt-in model is preferred.

There is an opportunity for these sorts of issues to be addressed during the upcoming 2003 review of the Act. The Commissioner's qualified "opt-in" interpretation of NPP 2.1 indicates that he would want to clarify and improve the Act's applicability to spam. For example, there is evidence that direct marketers are increasingly turning to "permission-based" marketing online, but there is confusion, and differences of opinion, over when permission is given. This debate often boils down to "opt-out" versus "opt-in" as a model for consumer permission.

DRAFT RECOMMENDATIONS:

Clarify the current application of the NPPs to spam, in straightforward publicly available advice.

CONFIDENTIAL DRAFT

The NPPs should be adjusted during the upcoming review in 2003 to close the loopholes detailed above and thereby ensure Privacy legislation best protects the privacy of Australians as it relates to spam.

Trade Practices Act

DRAFT RECOMMENDATION:

The Trade Practices Act should be reviewed to optimise its potential as an effective tool against spam that is misleading or deceptive. For example, with regards to:

- *Spoofing under section 52; and*
- *Misleading privacy statements (with a view to being consistent with the Privacy Act).*

Online Content Scheme

The Online Content Scheme regulates Internet Content, under *the Broadcasting Services Act 1992* (BSA). 'Internet content' is defined as stored information which is accessed using an Internet carriage service, including material on the World Wide Web, postings on newsgroups and bulletin boards, and other files that can be downloaded from an archive or library. "Ordinary" electronic mail is specifically excluded from the definition of Internet content under the scheme, although extraordinary e-mail may fall under the scheme. In this context, extraordinary e-mail may include certain spam; however, to date this has not been established.

As part of its upcoming review of the Online Content Scheme, DCITA will be calling for public submissions in regard to providing some clarification of what extraordinary e-mail is under the Scheme.

It may be appropriate for NOIE to work with DCITA to develop a definition that includes e-mail that may be regarded by a reasonable person as offensive. This definition may also want to provide for improved protection for minors given the indiscriminate methods by which spam, including that which promotes pornography and other inappropriate content, is sent.

DRAFT RECOMMENDATION:

"Extraordinary e-mail" should be defined, during the upcoming review into the operation of Schedule 5 "Online Services" of the Broadcasting Services Act, so that spam that may be offensive is covered by any complaint regime.

Is there a case for new legislation?

NOIE believes each of the following three options have some merit but further work needs to be done to determine which option or suite of options, if any, are in the public interest. Before NOIE could make any recommendation regarding introducing new legislation detailed analysis of each option would need to be conducted (including of international experiences where similar laws have been enacted) and proposals put to stakeholders.

Further to this the Government may wish, after public consultation, to develop legislation that uses a combination of options. For example there may be overlaps between Options 1 and 2.

The three new legislative options NOIE has received in submissions, include:

- Option 1:** An outright ban of spam as proposed by CAUBE;
- Option 2:** Legislation requiring spam to be transparent similar to laws enacted in the United States; and
- Option 3:** The proposal from the Australian Securities and Investment Commission to introduce a new Commonwealth offence of using an electronic carriage service to commit any (other) Commonwealth offence.

Option 1: An outright ban of spam as proposed by CAUBE

Given the difficulties in regulating spam, CAUBE has proposed a legislative ban on spam, with tough penalty provisions to act as a deterrent. Under this proposal recipients of spam would have a right of seeking legal redress with spammers facing significant liability.

Recognising that these laws are difficult to enforce in other jurisdictions, where the majority of spam received by Australians is from, CAUBE is working with its overseas affiliates to have similar laws enacted in their jurisdictions.

Option 2: Legislation requiring spam to be transparent similar to laws enacted in the United States

There have been a range of laws implemented in the United States that require greater transparency in e-mail. Whilst any option to implement similar legislation here would require a more detailed analysis of what has been effective overseas (two examples have been detailed in the box below), some options identified include laws that:

- Require standard letters such as “ADV” in the header;
- Require that a real contact details (e-mail, fax, postal address, street address, toll-free number etc) be included to allow for opt-out;
- Make it unlawful to use a third party’s domain name without permission;
- Make it unlawful to use a misleading or false header; and/or
- Require all UBE to use a special domain name (as an alternative or in addition to ADV).

CONFIDENTIAL DRAFT

The examples outlined below demonstrate that no clear model exists in other jurisdictions yet. Should the Government wish to pursue this option more work would be needed to ensure its efficacy.

Examples of Transparency Laws in Other Jurisdictions

Californian “ADV” Laws

California has passed laws require both the inclusion of the letters ADV in the header of unsolicited e-mail and the provision of real return addresses (both e-mail and postal).

We have however been advised that there has been little action made on in relation to the Californian Laws.

Washington State Laws Banning Spoofing

Washington State has passed laws to make it illegal to send a commercial e-mail message that uses a third party's domain name without permission; that contains false or missing routing information; or with a false or misleading subject line. The law applies if a message is sent from within Washington; if the sender knows that the recipient is a Washington resident; or if the registrant of the domain name contained in the recipient's address will confirm upon request that the recipient is a Washington resident.

Whilst there has been litigation under these laws they do not provide for a consolidation of actions against one spammer and claims can only be lodged in the Small Claims Tribunal which is ill-equipped for dealing with spam.

Option 3: The ASIC proposal to introduce a new Commonwealth offence of using an electronic carriage service to commit any other Commonwealth offence

The Attorney General's Department has advised that a general spamming offence would not be appropriate under the criminal law because the elements which define the conduct of spamming have no obvious connection with ulterior criminal objectives. However, other agencies, including ASIC, are in favour of an offence that deals with the use of carriage services for false or fraudulent purposes. This would capture a large proportion of spam received by Australians.

ASIC, as a result of its own experience and discussions with other Commonwealth agencies, has become aware of a gap in the law where Commonwealth agencies are engaged in combating misbehaviour using computers and/or the Internet, including crimes that are advanced by spam. Specifically, it seeks to introduce a broad based electronic communication offence of misusing those communications to commit a Commonwealth offence. That would facilitate, according to ASIC, combating illegal spamming activities generally and would not necessarily be limited to the financial services area.

CONFIDENTIAL DRAFT

This proposal is not focussed on extending the substantive breadth of the law, rather it seeks to better enable Commonwealth law enforcement agencies to enforce current laws in the online environment. This could also be designed to cover both the person or organisation sending the spam and (if applicable) the person or organisation commercially benefiting from the spam.

The Commonwealth does have power to legislate for “Postal, telegraphic, telephonic, and other like services”¹³. ASIC has suggested an offence similar to a US law (Section 1343 (Wirefraud) of Title 18 of the United States Code¹⁴). This has stood the test of time and empowered US federal authorities to investigate and prosecute a fraud that would normally be a State responsibility, if the fraud is committed using the telephone system.

This kind of clause might be considered for either the Telecommunications Act or the Cybercrime Act. A periodic review of the Telecommunications Act is to be conducted shortly by DCITA. The Attorney General’s Department has advised that fairly regular reform of criminal law occurs, particularly of those laws involving technology, however the Cybercrime Act may still be too recent for an AGD review.

It should be noted that the drafting of the Cybercrime Act, the Cybercrime code committee recommended against a spam clause on the basis that:

- it was difficult to define spam; and
- they did not regard the elements which define the conduct of spamming as having an obvious connection with ulterior criminal objectives.

DRAFT RECOMMENDATION:

The Government should consider these three new legislative options (and possibly others) in further detail, consulting with stakeholders and the public, to determine if new legislation is in the public interest and, if so, what form this should take.

¹³ Extract from AGECE wirefraud discussion paper 2000.

¹⁴ Whoever, having devised or intending to devise any artifice to defraud, or for obtaining money or property by means of false or fraudulent pretences, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned for not more than five years, or both. If the violation affects a financial institution, such person shall be fined not more than \$1,000,000 or imprisoned for not more than 30 years, or both.

CONFIDENTIAL DRAFT

How can Internet users be better equipped to deal with spam?

Technical tools and consumer awareness options are likely to have a moderate but greater effect on alleviating spam, in the short and medium term, than most other approaches. They are a key component in improving consumer understanding, empowerment and therefore satisfaction with the e-mail system.

Consumer education is a key factor in any strategy to counter spam. In order to change the cost-benefit equation facing spammers consumers need to be educated and empowered so that they:

- Can make informed choices in relation to spam reduction strategies and technologies;
- Better understand the pitfalls of purchasing products promoted by spam both in terms of the risks they face given the dubious nature of many of these products and how purchase ensures the commercial viability of spam;
- Better understand how to protect their private information, such as e-mail addresses, in the online environment thereby making spamming more difficult; and
- Better understand their rights in relation to all aspects of spam and possible remedies where available.

NOIE has identified several vehicles through which consumer education may be pursued:

- The NOIE spam web page which already contains information about spam minimisation. Of course this will need to be upgraded in the light of information learned through the review process and in light of review outcomes;
- The creation of an additional fact sheet on spam to add to the “Shopping on the Internet: facts for Consumers” fact sheet series; and
- Collaborate with the IIA which is currently seeking to establish an e-security portal for SMEs and consumers possibly using ITOL funding;

DRAFT RECOMMENDATION:

In conjunction with stakeholders, such as the ACA, IIA, Treasury, ASIC, ACCC and the OFPC, NOIE should design and manage a campaign geared towards spam that creates awareness, provides accurate information and useful resources to consumers (possibly developed in conjunction with related e-security campaigns)

Regulatory agencies and NOIE should develop together a comprehensive guidance on how existing legislation can be applied to counter spam.

CONFIDENTIAL DRAFT

Monitoring of spam and measuring review outcome performance

For this review NOIE commissioned AC Nielsen.consult to obtain survey data on spam from many Australian ISPs. The findings are in Attachment A.

DRAFT RECOMMENDATION:

In the interest of continued monitoring of spam and the effectiveness of any counter-measures, NOIE should continue to obtain similar data each year and develop longitudinal analyses of progress of various measures in combating spam.

ADD -
CONCLUSIONS
NEXT ACTIONS/FOLLOW-UP
ANY ATTACHMENTS

NOIE
19 June 2002