The Senate

Environment, Communications, Information Technology and the Arts Legislation Committee

Provisions of the Spam Bill 2003 and the Spam (Consequential Amendments) Bill 2003

October 2003

ISBN 0 642 71329 4

This document was printed by the Senate Printing Unit, Parliament House, Canberra

Committee membership

Members

Senator Alan Eggleston, Chair (LP, WA)
Senator Sue Mackay, Deputy Chair (ALP, TAS)
Senator Andrew Bartlett (AD, QLD)
Senate Kate Lundy (ALP, ACT)
Senator Santo Santoro (LP, QLD)
Senator Tsebin Tchen (LP, VIC)

Substitute Member for the inquiry
Senator Brian Greig (AD, WA)

Participating Members

Senator the Hon Eric Abetz (LP, TAS)
Senator the Hon Nick Bolkus (ALP, SA)
Senator the Hon Ron Boswell (NATS, QLD)
Senator Bob Brown (AG, TAS)
Senator George Campbell (ALP, NSW)
Senator Kim Carr (ALP, VIC)
Senator Grant Chapman (LP, SA)
Senator John Cherry (AD, QLD) for matters relating to the Communications portfolio
Senator Stephen Conroy (ALP, VIC)
Senator the Hon Helen Coonan (LP, NSW)
Senator Christopher Evans (ALP, WA)
Senator the Hon John Faulkner (ALP, NSW)
Senator Alan Ferguson (LP, SA)
Senator Jeannie Ferris (LP, SA)
Senator Brian Harradine (IND, TAS)
Senator Leonard Harris (PHON, QLD)
Senator Gary Humphries (LP, ACT)
Senator Susan Knowles (LP, WA)
Senator Meg Lees (AD, SA)
Senator Ross Lightfoot (LP, WA)
Senator Jan McLucas (ALP, QLD)
Senator Brett Mason (LP, QLD)
Senator Julian McGauran (NATS, VIC)
Senator Clair Moore (QLD, ALP)
Senator Shayne Murphy (IND, TAS)
Senator Kerry Nettle (AG, NSW
Senator Robert Ray (ALP, VIC)
Senator John Watson (LP, TAS)
Senator Penny Wong (ALP, SA)

Committee Secretariat

Mr Michael McLean, Secretary
Ms Sharon Babyack, Research Assistant

Committee Address

Environment, Communications, Information Technology and the Arts Legislation Committee
S1.57, Parliament House
Canberra ACT 2600

Tel: 02 6277 3526
Fax: 02 6277 5818

Email: ecita.sen@aph.gov.au

Internet: http://www.aph.gov.au/senate/committee/ecita_ctte/index.htm

Table of Contents

Referral and conduct of the inquiry

1.1 On the recommendation of the Selection of Bills Committee, on 8 October 2003 the Senate resolved that the provisions of the Spam Bill 2003 and the Spam (Consequential Amendments) Bill 2003 be referred to the Environment, Communications, Information Technology and the Arts Legislation Committee for inquiry and report by 27 October 2003.[1] The Senate subsequently agreed to extend this reporting deadline to 29 October.

1.2 The Committee invited submissions on the Bills in an advertisement in the major national newspapers on Tuesday 14 October 2003. It also wrote directly to a number of relevant organisations inviting submissions. The Committee received 19 submissions which are listed at Appendix 1. It also held a public hearing in Canberra on Thursday, 23 October 2003, details of which are shown in Appendix 2.

1.3 The Committee thanks all those who contributed to its inquiry by preparing submissions and appearing at the hearings.

The Bills

1.4 The Bills were introduced into the House of Representatives on 18 September 2003. The Second Reading Speech for the Spam Bill 2003 states that the Bill intends to protect Australian online users from the increasing costs and disruptive occurrence of unsolicited commercial electronic messages, or "spam" and its threat to effective and efficient electronic communications and legitimate online business. Some of the key issues surrounding spam help to understand the community resentment and outrage at its increasing appearance; these issues include illegal or offensive content, invasion of privacy and misleading and deceptive trade practices.[2]

1.5 The cost of spam to business is estimated to be around $900 per employee per year. It can cost loss of productivity, customers and business opportunities, as well as damage reputations.[3] The Bill states that the Courts will be able to compensate businesses that have suffered loss due to spammers, and recover financial gains made by spammers. Enforcement of the legislation will be through the Australian Communications Authority (the ACA). The ACA will also participate in education campaigns to inform individuals and businesses about methods of reducing spam.[4]

> This Bill will send a powerful message to those engaged in the activities associated with sending spam. It tackles head-on the problem of Australian-

---

1 Selection of Bill Committee, Report No. 12 of 2003, 8 October 2003.

2 Spam Bill 2003, Second Reading Speech, p. 1.

3 Spam Bill 2003, Second Reading Speech, p. 2.

4 Spam Bill 2003, Second Reading Speech, p. 3.

> originated spam and sends a strong message to overseas spammers. Coupled with relevant industry codes of practice it defines acceptable future conduct and demonstrates the seriousness of Australia's intent in seeking to develop international cooperation to achieve longer term solutions to a growing world-wide problem.[5]

1.6 The proposed provisions of the Bill deal with the following broad issues:

- a consent-based, or "opt-in", basis for commercial electronic messaging;
- a recognition of existing customer-business relationships;
- restricted, and appropriate, recognition of implied consent, where people advertise their electronic address;
- a requirement for accurate sender's details and a functional unsubscribe facility;
- support for the development of complementary industry codes; and
- a flexible and scalable civil sanctions regime for breaches.[6]

1.7 To allow time for individuals and businesses to adjust to the new legislation, the Bill provides that the penalty provisions will be enforced 120 days after Royal Assent, and will be accompanied by a significant national awareness and education campaign.[7] Exemptions to the Bill apply to government bodies and the charitable sector.

1.8 The Second Reading Speech for the Spam (Consequential Amendments) Bill 2003 states that the Bill makes amendments to the *Telecommunications Act 1997* and the *Australian Communications Authority Act 1997* to enable effective enforcement and investigation of breaches of the Spam Bill.[8]

1.9 The proposed provisions of the Spam (Consequential Amendments) Bill deal with the following broad issues:

- A framework for spam-related industry codes to be established and registered;
- Appropriate powers for the ACA to investigate possible breaches of the Spam Bill; and
- Monitoring and investigatory warrants relating to compliance with and breaches of the Spam Bill.[9]

---

5 Spam Bill 2003, Second Reading Speech, p. 4.

6 Spam Bill 2003, Second Reading Speech, p. 2.

7 Spam Bill 2003, Second Reading Speech, p. 3.

8 Spam (Consequential Amendments) Bill 2003, Second Reading Speech, p. 1.

9 Spam (Consequential Amendments) Bill 2003, Second Reading Speech, p. 1.

1.10 Mr Keith Besgrove from the National Office for the Information Economy (NOIE) stated at the public hearing in Canberra:

> The bills are intended to implement the government's decision to include a legislative and regulatory component in its multilayered strategy against spam. Just briefly, the other elements of that strategy include awareness campaigns, industry codes of conduct and work by various groups within the community to focus on filtering mechanisms. They also encompass work in international fora to endeavour to try to achieve greater levels of collaboration between countries that are all facing a common problem. The view that we have taken with our recommendations to government is that spam is a multilayered problem and that, while legislation is an important component, it is only one component of a broader strategy.[10]

1.11 Submitters generally welcomed the overall thrust of the Bills, however some submitters including Electronic Frontiers Australia Inc. (EFA), the Australian Computer Society (ACS), Australian Direct Marketing Association (ADMA) and Coalition Against Unsolicited Bulk Email, Australia (CAUBE.AU) had reservations about certain elements of the Bills which are discussed further in this report.

Defining spam as only 'bulk' messages

1.12 Many submissions contested the Bill's definition of spam, particularly in relation to its reference to unsolicited commercial emails, not just emails sent in bulk. Some argue that defining spam as simply messages sent in bulk would sufficiently catch the majority of spam in the legislation. Mr Rollo from the Coalition Against Unsolicited Bulk Email, Australia (CAUBE.AU) explained how CAUBE.AU would define bulk, and why it is a useful definition of spam:

> The way we define it, as a rule of thumb, is that it is not bulk if a person has spent time determining that the message is going to be relevant to the particular recipient. That would be consistent with one of the amendments suggested by the Australian Computer Society, where there was a defence if there was a reasonably held view of relevance.[11]

1.13 NOIE's submission expands on the reasoning behind the Bills inclusion of single, commercial emails being defined as spam, as well as emails sent in bulk.

> The concept of bulk was avoided because it would increase the compliance cost by increasing the scope for ambiguity and argument by spammers in the legal arena. It would have no practical benefit for legitimate business, and

10 Mr Besgrove, *Proof Committee Hansard*, 23October 2003, p. 1. (Henceforth, references to the Proof Hansard in this report are references to this date).

11 Mr Rollo, *Proof Committee Hansard*, p. 25.

> could disempower consumers from reporting spam where they had no knowledge of whether an e-mail had been sent to one person or a million.[12]

1.14 NOIE further explained in its submission how the concept of bulk-messaging has been side-stepped in other countries by spammers in the legal arena. Generally speaking, bulk has been defined as around 100 emails sent. In some cases spammers would send multiple address lists of a size just under the number classed as bulk. Another method to avoid spam legislation was to use different multiple addresses. Spammers would also change one or two characters in the given email, arguing that since no two messages are the same, they couldn't be defined as 'bulk'.[13]

> Given that the concept of "bulk messaging" appeared to reduce the efficacy and applicability of anti-spam legislation, it was decided to focus on the core issue involved in the penalty provision – the sending of unwanted commercial electronic messages in spite of the recipient's wishes or consent.[14]

Defining spam to include single messages

Protecting legitimate exchange of business

1.15 Many submitters were concerned that the inclusion of commercial emails and the definition of 'consent' were not clearly defined in the Bill and, because of this, there was potential for the prohibition of legitimate exchange of business. Professional Way Pty Ltd, an internet based business made the following comment:

> The principal problem with the Bills from a small business perspective is that they fail to recognise the benefit of small scale, unsolicited, highly targeted emails as a legitimate business development tool.[15]

1.16 As Mr Philip Argy from the Australian Computer Society (ACS) stated, 'spam is hard to describe but you know it when you see it.'[16] Despite the difficulties in defining spam, NOIE has taken measures to protect legitimate business practice from being prohibited.

> A key concern in drafting the Bill was to prevent spam without prohibiting legitimate business communications. The provisions relating to express and inferred consent provide the basis for deciding whether a message is spam - an unsolicited commercial electronic message.[17]

---

12 Submission No. 14, (National Office for the Information Economy – NOIE), p. 15.

13 Submission No. 14, NOIE, p. 14.

14 Submission No. 14, NOIE, p. 15.

15 Submission No. 3 (Professional Way Pty Ltd), p. 4.

16 Mr Argy, *Proof Committee Hansard*, p. 13.

17 Submission No. 14, NOIE, p. 8.

Protecting un-intending offenders

1.17 Furthermore, there was concern that the victimisation of innocent persons would occur under the legislation. As Ms Irene Graham of Electronic Frontiers Australia Inc (EFA) argued at the public hearing the Bills should, "at least discourage attempts to, in effect, victimise individuals who have sent a single message that is arguably caught by this definition."[18]

1.18 NOIE has taken measures to safe guard against victimisation of un-intending offenders under the legislation. NOIE explained that the Bills give the ACA a measure of discretion in enforcement to ensure that the penalty is in proportion to the level of offence. The Bills will allow the ACA to have a graduated tier of penalties beginning with formal warnings for minor offences, and then infringement notices, which can detail one or many breaches of the legislation.

> As with its other enforcement roles, the ACA would establish internal guidelines and governance procedures to ensure the consistent, reasonable and appropriate application of this discretion.[19]

The penalty amounts are defined as being per contravention. As Mr Barton from NOIE explained at the public hearing, 'The point to make about the infringements regime is that it is there to achieve behaviour change rather than anything else.'[20]

Conspicuous publication

1.19 Another cause for concern in the Bill was the term 'conspicuous publication'. NOIE explains the term in its submission:

> The publication of electronic addresses (particularly e-mail and SMS addresses) on websites, journals, newspapers, the yellow pages and through other media is a common method of inviting communications in respect of a business or particular work-related function. Schedule 2, clause 4 provides the assurance that such communications are not prohibited by the Spam Bill, and clarifies that the consent that may be inferred is not a universal consent. It is a consent in relation to the business or work function that pertains to the published address.[21]

---

18 Ms Graham, *Proof Committee Hansard*, p. 10.

19 Submission No. 14, NOIE, p. 14.

20 Mr Barton, *Proof Committee Hansard*, p. 28.

21 Submission No. 14, NOIE, p. 7.

1.20 EFA points out that the proposed conspicuous publication as outlined in the Bill would be difficult to enforce for addresses published prior to the legislation.[22] EFA also noted in its submission that where an individual may make an accompanying statement such as 'No UCE', it may unintentionally prohibit their receiving emails from business related offers. Furthermore EFA submitted that:

> The matter of what is relevant to a person's job function is just as open to interpretation as the matter of what is spam. … The "conspicuous publication" exception therefore enables such persons to be spammed with advertisements for e.g. insurance, office equipment, computer supplies, printer cartridges, business software, seminars about marketing, etc, etc, in addition to goods and services relevant to their specific type of business.[23]

1.21 The intention of this provision as previously stated is to protect a 'common method of inviting communications'. To include the provision, NOIE had to strike a delicate balance of deterring spam whilst allowing for a currently accepted practice to continue.[24]

> As we have stated, it really does need to be quite a conspicuously published address. The mere fact that your email address exists somewhere on the Internet does not constitute conspicuous publication. The fact that you might be listed in an old news group list or something like that is not adequate, and I think in the explanatory memorandum we have made that reasonably clear.[25]

Exemptions

1.22 The following are exempt from some of the legislation's requirements where the message is related to goods and services:

- messages from government bodies;
- messages from registered political parties;
- messages from charities;
- messages from religious organisations;
- messages from educational institutions directed to attending and former students and their households; and
- purely factual messages.[26]

---

22 Submission No. 5, EFA, p. 20.

23 Submission No. 5, EFA, p. 21.

24 Submission No. 14, NOIE, p. 8.

25 Mr Barton of NOIE, *Proof Committee Hansard*, p. 30.

26 Submission No. 14, NOIE, p. 10.

1.23 Whilst varying aspects and concerns were expressed about the exemptions, the principal one was that the listed organisations would interpret the exemption as a licence to spam. Mr Troy Rollo from CAUBE.AU used charities as an example:

> We would agree that certainly charities do depend on goodwill but it is not unheard of for them to spam. There have been a couple of isolated cases in which charities have spammed. It would certainly not be good if charities were to interpret the exemption as being a licence to spam.[27]

1.24 Mr Argy from the ACS could foresee problems arising from the exemptions relating to factual information:

> I are more concerned about how easy it is to assert that your spam has factual content; for example, the emails that I have used in my example to Senator Lundy about various mechanisms for enhancing one's anatomy are arguably containing no more than factual information—albeit facts that you do not care to receive. So it is not so much where they come from as what the content is. So I would be very concerned if those kinds of emails continued to be sent because you can identify factual content.[28]

1.25 In the Second Reading Speech it was stated that, 'This in no way gives governments a "licence to spam" – we remain bound by, and committed to, the Privacy Act.'[29] NOIE outlined some of the reasoning behind the exemptions in its submission:

> The majority of messages from the listed groups would either not be commercial in nature, or would be sent to recipients who have a relationship with the organisation. The limited exemptions have been included in an effort to ensure that there are not unintended restrictions of the legitimate operations of the groups named, while ensuring that they are not given license to spam.[30]

1.26 Furthermore, NOIE explained that religious organisations commonly reach beyond their congregations and memberships to reach the broader community. The Bill includes an exemption for these organisations to ensure the beneficial nature of these activities is able to continue.[31]

1.27 The factual content exemption is included to protect newsletters and information documents from falling foul of the legislation:

---

27 Mr Rollo, Proof Committee Hansard, p. 27.

28 Mr Argy, *Proof Committee Hansard*, p. 16.

29 Spam Bill 2003, Second Reading Speech, p. 4.

30 Submission No. 14, NOIE, p. 12.

31 Submission No. 14, NOIE, p. 11.

> The legislation focuses on commercial electronic messages. Communications that only convey ideological, political or social comment are not commercial in nature, and so are not addressed by the legislation. Newsletters, political commentary, invitations to political or religious gatherings (where there is no admission charged, or commercial activity being undertaken at the venue) are not within the scope of the legislation.[32]

Exemption from the unsubscribe facility

1.28 Exempt organisations are also permitted to send emails without including an unsubscribe facility. However, the senders are required to accurately identify the authoriser of the message and the content of the message must relate only to goods and services that the authorising agent is supplying.[33]

1.29 Some of the submitters did not agree with the provision allowing for the exemption of an unsubscribe facility for certain organisations. EFA argues that:

> …it is unacceptable that the exempt bodies are also exempt from the requirement to provide a functional unsubscribe facility the same as that applicable to commercial messages sent with the recipient's consent. There is no reason why bodies that are permitted to send commercial messages, without consent, should not be required to provide a functional means by which recipients can notify the body that they do not wish to receive their unsolicited commercial messages. Where a law creates a presumption that consent exists, a person must be able to easily withdraw consent.[34]

1.30 EFA is not alone in its argument, the Australian Direct Marketing Association (ADMA), a not-for-profit organization representing over 500 companies explained their view at the public hearing:

> From a consumer perspective, I think the important thing is to give the consumer some sort of control. If there is no unsubscribe facility then, obviously, they have a lack of control over how their data is being used.[35]

1.31 NOIE explained in its submission that the proposed legislation does not prevent exempt organisations from using the unsubscribe facility, but it does not require it.[36]

---

32 Submission No. 14, NOIE, p. 12.

33 Submission No. 14, NOIE, p. 10.

34 Submission No. 5, EFA, pp. 12-13.

35 Miss Sangster, *Proof Committee Hansard*, p. 19.

36 Submission No. 14, NOIE, p. 13.

> The fact that there would be no effective obligation for these organisations to act on an unsubscribe request would mean that mandating the inclusion of such a facility would be both illogical and create an incorrect assumption that there was an obligation for such a request to be honoured.[37]

1.32 NOIE explained that, whilst the exempt organisations are not required to include an unsubscribe facility, they do have to authorise the email by containing accurate contact details and information about the organisation.[38]

Search warrants: search and seizure of premises and property

1.33 The Bill allows for two types of searches to be conducted by the ACA, firstly with the consent of the owner or occupier and secondly with a warrant obtained through a Magistrate. A common concern amongst submitters to the inquiry was the authority given to the ACA to conduct a search without a warrant. This was primarily due to the sensitive nature of communication stored on computers:

> … it is not just the individual possessions that are being searched. When you start talking about searching computers and email and things, you are also potentially invading the privacy of anybody who has communicated with that person by email—not necessarily ever communicated, but obviously there is most likely going to be email that relates to people who have nothing to do with spamming at all. … Part of the reason is that it infringes upon the privacy of completely innocent people. In our view, email is exactly the same in terms of the potential for it to invade the privacy of innocent people.[39]

1.34 Another major concern relating to the search and seizure provisions in the Bills was the potential for a non-owner of the PC to permit a search. EFA argues that inspectors will be granted the authority to search a premises and seize property without the consent of the owner of the belongings (computers and files); but with the consent of the owner or occupier of the premises which in some cases may be the landlord or a person sharing the residence. [40]

1.35 EFA suggested that the way around this was to narrow the definition of the individual(s) who are able to give consent, such as the owner of the computer or emails that have been sent.[41]

---

37 Submission No. 14, NOIE, p. 13.

38 Submission No. 14, NOIE, p. 13.

39 Ms Graham of EFA, *Proof Committee Hansard*, p. 5.

40 Submission No.5, EFA, p 6.

41 Ms Graham, *Proof Committee Hansard*, p. 6.

1.36 In its submission, NOIE clarified the Bills' provisions regarding the search of premises:

> The Bill does not allow a search of premises without a warrant and without consent. The Bill only provides for a search of premises where an inspector (being an ACA appointed inspector or a member of the Australian Federal Police) has a warrant obtained from a magistrate, or has been given the consent of the owner or occupier of the premises. This recognises that the owner or occupier is appropriately entitled to decide who may enter the premises. It gives them the opportunity to consent, without wasting court resources, where they are willing to accede to the request. The owner or occupier may refuse consent, or may withdraw their consent at any time during the conduct of the search.[42]

1.37 NOIE further explained that the ACA has governance procedures and longstanding practices to ensure that both the search and the decision to seek a warrant is conducted responsibly and appropriately.[43] NOIE has also taken into account the possibility of approaching an individual to search their premises when they potentially could have no knowledge that their PC is being used for spamming.

> Warrants may often be required. It is inherent in the nature of spamming that the evidence is of a very fragile nature and very easily deleted. Equally, there may well be circumstances where entering with the consent of the owner is a much more preferred option. We have a situation now where an individual's home computer can be infected with trojans that send out spam without their knowledge, so there may be spamming from a particular address or a particular computer. The government was cautious not to have a situation where the first contact that person had with an ACA individual was, 'Hello, I have a warrant. I am here to search your premises.' In cases where it is done with consent, the owner or occupier needs to be made aware at commencement that they have the opportunity of not providing consent and furthermore that consent can be withdrawn at any stage during the search.[44]

1.38 NOIE argued that it could see the potential for game playing, and that having to prove the precise owner of the belongings could complicate and slow down search procedures. [45] Given that evidence of spamming can be quickly destroyed or deleted, the Bills have included a solution whilst still maintaining an ethical code of conduct for inspectors.

---

42 Submission No. 14, NOIE, p. 16.

43 Submission No. 14, NOIE, p. 16.

44 Mr Barton of NOIE*, Proof Committee Hansard*, p. 31.

45 Mr Barton, *Proof Committee Hansard*, p. 32.

Searching the premises of spam recipients

1.39 Concern was also raised of the possibility of a recipient of spam having their premises searched.

> While it may be considered unlikely that inspectors would search the homes of recipients of spam, it is essential that the law specifically not allow that to occur without the consent of the relevant individual, e.g. the owner of the computer, email or "thing", as applicable, to be searched.[46]

1.40 The same principles apply to a recipient of spam, an inspector would require either consent from the owner or occupier of the premises, or a warrant obtained from a magistrate to search premises or seize property. NOIE explained in its submission why this would be an unlikely event:

> The only way the ACA would be aware of a recipient of spam would be if the recipient complained to the ACA about receiving spam, or if the ACA had logs or other evidence showing the person as a recipient of spam. In the first instance, the recipient is likely to welcome the ACA's investigation, and in the latter case, the ACA would not need to seek additional evidence.[47]

Passwords and encryption codes: search and seizure of computer systems

1.41 The Bills allow for a person who is "reasonably suspected of being involved in a breach" to supply their encryption keys and/or passwords to their computers. Those who do not supply this information can be penalised with six months imprisonment. Electronic Frontiers Australia (EFA) had strong reservations that an individual could be unreasonably subject to this penalty:

> A person who is merely suspected of having been "involved in" sending one single unsolicited commercial electronic message could be the subject of an order and imprisoned for six months if they decline, or are unable, to provide the required information or assistance.[48]

1.42 EFA was also concerned that a person who has genuinely forgotten a code (especially in the pressure of the moment during a search) would be charged with this penalty and unable to prove that they had genuinely forgotten:

> The prospect of users of encryption being jailed despite having genuinely lost their private keys is a major and quite legitimate concern. Any legislation containing such provisions should, at the very least, provide an

---

46 Submission No. 5, EFA, p. 8.

47 Submission No. 14, NOIE, p. 17.

48 Submission No. 5, EFA, p. 9.

> indication as to how those served with assistance orders requiring plain text or encryption keys can successfully prove that they cannot comply with the order.[49]

1.43 The Committee notes this evidence without having had clear guidance from the government representatives of their view. Given the extent of prior consultation, the Committee assumes that the matters raised have already received due consideration.

Conclusions and recommendation

1.44 Email has revolutionised international communications over the past few years. Spam has grown to be its cancer. It is an issue of international significance and Australia is not alone in seeking to address within its jurisdictional limits the problems it creates, and the Committee was pleased to learn that Australia is taking a significant leadership role in an OECD project which is seeking to identify mechanisms for greater international collaboration.[50]

1.45 The purpose of this package of legislation is to seek to do something about this growing problem of unsolicited and usually unwelcome messages received against the wishes, and at a cost to, the recipient. The parallel with traditional junk mail ends at that point – the recipient of normal junk mail bears no direct cost and they can choose to throw it away with minimal effort. The recipient of electronic messaging has no such choice.

1.46 The Committee notes that the Government is acknowledged to have consulted widely on the problem before bringing forward this legislation. The National Office for the Information Economy issued its report entitled *Spam: Final report of the NOIE review of the spam problem and how it can be countered* in April 2003. That report was a comprehensive and informative contribution to the state of public knowledge about the spam problem. The Committee also notes that many submitters expressed their appreciation of the Government's efforts at consultation before bringing forth this package of legislation.

1.47 It is unsurprising that not everyone agrees with the approach adopted by the Government. The Committee notes advice from NOIE's Mr Besgrove that his organisation has studied overseas experience – specifically in relation to the problems of defining the term 'bulk emails' – and has found them all to be problematic in some way.[51] He argued that critics of the Bills should be aware of those background elements.

---

49 Submission No. 5, EFA, p. 10.

50 Mr Besgrove of NOIE, *Proof Committee Hansard*, p. 3.

51 Mr Besgrove of NOIE, *Proof Committee Hansard*, p. 30.

1.48 The Committee believes that the legislation is an important first step towards addressing the spam problem. As noted above, NOIE has indicated that the legislation is one part of the Government's multilayered approach to spam, and that, while an important component, is only one part of a broader strategy. The Committee fully endorses this approach, in particular the proposed 12-month educational program. As Mr Robert Edwards from ADMA noted:

> …legislation itself is not going to solve the issue, and it would be wrong for Australian citizens to think that when this legislation is enacted their in-box is going to be miraculously empty one day. That is clearly not going to happen. But this legislation is one of a basket of things that, put together, may actually play a role in helping to alleviate the problem.[52]

1.49 It may well be that there are elements in the legislation that, without the benefit of perfect foresight, are found with experience to need correction. This is almost inevitable with any ground-breaking legislation. The Committee notes that the Government has recognised this possibility and has included in the Spam Bill a provision for a review after two years. Given the rapid rate of change in telecommunications in the modern era, the Committee strongly endorses that proposal.

1.50 The Committee recommends:

> That the Spam Bill 2003 and the Spam (Consequential Amendments) Bill 2003 be agreed to without amendment.

Alan Eggleston
Chairman

52 Mr Edwards of ADMA, *Proof Committee Hansard*, p. 17.

Senate Environment, Communications, Information Technology and the Arts Legislation Committee

LABOR MINORITY REPORT

Inquiry into the Spam Bill 2003 and the Spam (Consequential Amendments) Bill 2003

Introduction

1. The *Spam Bill 2003* (Spam Bill) and the *Spam (Consequential Amendments) Bill 2003* (SCA Bill) create a new regime regulating the sending of commercial electronic messages – including emails and mobile phone short message services (SMS) – to, from, and within Australia.

2. The Spam Bill operates to prohibit the sending of unsolicited commercial electronic messages (commonly referred to as "spam"), and includes a series of remedies including civil penalties, injunctions, and enforceable undertakings.

3. The SCA Bill contains a series of amendments to the *Telecommunications Act 1997* and the *Australian Communications Authority Act 1997* which allow the Australian Communications Authority (ACA) to investigate breaches of the scheme.

4. Labor shares public concern over the rising incidence of spam and understands the necessity for undertaking this inquiry in such a short time-frame (three weeks). Labor notes that despite this short time-frame, the Committee eventually received 19 submissions, and thanks respondents for contributing to a constructive and necessary process.

5. Spam is widely acknowledged as having a significant negative impact on the Internet and email worldwide. The National Office for the Information Economy (NOIE) gave evidence to the Committee that "spam now constitutes over 50% of all the worldwide email", adding that it is "seriously degrading the functionality of the Internet."[1]

6. It is widely accepted that the regime proposed in these Bills alone will not result in a noticeable reduction in spam levels, and that the Government must take other steps. The general objectives of this Bill are seen as an essential element of a broader campaign against spam including international co-operation, business and consumer education, and work with industry. Generally, the Bills received widespread support from respondents to this Inquiry.

7. However, Labor believes that these Bills can be improved, and the Committee heard evidence from many submitters suggesting how this could be achieved. In addition to several minor concerns raised before the Committee, the main issues included:

- Concern about the provisions in the SCA Bill that empower the Australian Communications Authority (ACA) to enter premises for the purpose of the search and seizure of articles contained within, relating to alleged spam activity;
- The possible application of the regime to unsolicited commercial emails not usually considered to be "spam";
- The nature and operation of the exemptions contained in Schedule 1 of the Spam Bill; and
- Concern about the operation of the "conspicuous publication" rule contained in Schedule 2 of the Spam Bill in determining consent.

---

[1] Mr Keith Besgrove, *Proof Committee Hansard*, Senate Environment, Communication, Information Technology and the Arts Legislation Committee, 23 Oct. 2003, p. 2.

8. Following Labor's consideration of the Bills, and as a result of examining the submissions and evidence presented in the inquiry, Labor has determined several specific recommendations on how these Bills can be improved and the proposed scheme strengthened.

Search and Seizure Provisions

9. Several respondents, including Electronic Frontiers Australia, Inc. (EFA), the Australian Consumers' Association, the Australian Privacy Federation (APF), the Australian Computer Society (ACS), and to a limited extent, the Internet Society of Australia (ISOC-AU), raised concerns with search and seizure provisions in the SCA Bill. In two instances the Bill amends the Telecommunications Act to allow ACA inspectors to enter and search a property to investigate breaches of the Spam Bill without obtaining a warrant. First, under the amended section 542 of the Telecommunications Act, inspectors would be able to enter and search premises, including computer files and email accounts, with only the consent of the owner or an occupier of the physical premises in which the computer is located. Second, under the new section 457A inspectors would need the consent of the occupier. Labor is concerned that the owner or the occupier might not be the owner of the computer system or possessions being investigated.

10. Labor heard evidence that, because of the wording of the legislation, recipients of spam who were not suspected of breaching the spam regime could also have their computer searched and seized. Combined with the point above, Labor is concerned that recipients of spam could have their computer seized without their consent, or without a warrant being obtained, for example through the consent of their landlord.

11. NOIE has defended the operation of the amended section 542, stating that "[t]he search and seizure provisions relating to breaches of the Spam Bill are unaltered from the search and seizure provisions currently in the Telecommunications Act".

12. However some respondents argued that when applied to breaches of the spam legislation these existing provisions were far more intrusive. Electronic Frontiers Australia noted that ACA inspectors' current powers:

> "relate to investigating whether there are illegal telephones installed in commercial or residential premises and whether there is illegal telecommunications cabling installed … Even if an inspector did believe that there were illegal telephones installed in a house, they would not need to go through a person's computer and email messages to find out what the problem was—to find out whether the person was breaching the law".[2]

13. The Australian Consumers' Association also pointed out that:

> "In the radio communications hardware environment there may be urgency in stopping the operation of illegal equipment, since there can be danger to life or health. Spam has many hazards, but direct threat to health or life is not one of them."[3]

14. The Coalition Against Unsolicited Bulk Email, Australia (CAUBE.AU) also raised the point that landlords are not commonly granted the right to give consent to enter a tenant's house, adding "if the provisions [in the SCA BILL] were interpreted to grant such a right there would be a substantial abridgement of the rights of the occupier."[4]

15. The APF noted that the legislation uses a sledgehammer to crack a nut, arguing that it "imposes an uncertain and potentially onerous and intrusive regime on all Internet users in Australia to deal with a problem that is in terms of Australian origin Spam, only originating from a very small number of users."[5] In

---

[2] Ms Irene Graham, *Proof Committee Hansard*, Senate Environment, Communication, Information Technology and the Arts Legislation Committee, 23 Oct. 2003, p. 5.

[3] Australian Consumers' Association, *Submission No. 6*, p. 3.

[4] Coalition Against Unsolicited Bulk Email, Australia, *Submission No. 7*, p. 10.

[5] Australian Privacy Foundation, *Submission No. 10*, p. 1.

relation to the search and seizure provisions of the legislation, Labor agrees with the sentiments in this statement. The intrusion into an individual's privacy caused by these provisions outweigh the impact the Spam Bills will have on the intrusion of spam emails, especially given the Government's own acknowledgement that this legislation will "not result in an immediate or dramatic reduction of the spam problem."[6]

16. Labor shares the concerns expressed in relation to the search and seizure provisions in the SCA Bill and recommends that search and seizure operations on private premises without a warrant are amended so that consent must be obtained from the individual whose property will be subject to such operations in the first instance. The Bill currently provides for a warrant to be obtained if consent is not given and Labor supports this action where an individual refuses consent.

17. Labor also recommends that the SCA Bill is amended to prevent search and seizure operations on the premises of spam recipients. The Committee heard evidence that this power would never be utilised by the ACA. If this is the case, Labor sees no reason for it to be included in the legislation as it represents an unacceptable intrusion on the privacy of the victims of spam. Labor notes that there is nothing in this Bill that would prevent victims of spam voluntarily assisting the ACA in its enquiries.

18. A related concern is the operation of the proposed Telecommunications Act section 547J, which would require any individual "reasonably suspected of having been involved in [a breach of the Spam Bill]" to disclose decryption keys and access codes. Failure to do so would result in a criminal penalty. The EFA, the Australian Consumers' Association, and the APF hold the view that this provision is unacceptable in its current form because the resulting criminal penalty is far harsher than the pecuniary penalties provided for under the Spam Bill and therefore "disproportionate". Labor concurs with these opinions and recommends that the application of section 547J is not subject to a test of strict liability and is tightened in its scope to affect a smaller class of people.

---

[6] *Spam Bill 2003 Explanatory Memorandum*, p. 1.

Recommendations:

- The amendment of provisions in the *Spam (Consequential Amendments) Bill 2003* relating to search and seizure operations on private premises without a warrant so that consent must be obtained from the individual whose property will be subject to such operations;
- The amendment of the *Spam (Consequential Amendments) Bill 2003* to prevent search and seizure operations on the premises of spam recipients;
- The amendment of the proposed section 547J of the *Telecommunications Act 1997* to remove the existing strict liability test and to tighten its scope to affect a smaller class of people, and that its operation is not subject to a test of strict liability.

Application of regime to single commercial emails

19. Several respondents to the Inquiry, including Mr Athol Yates, the EFA, the Australian Consumers' Association, the APF, and the ACS, noted that as currently drafted the Spam Bill prohibits some single unsolicited commercial electronic messages sent by individuals or organisations that genuinely believe that the intended recipient would want to receive it. The implication is that the Bill prohibits some emails currently not widely regarded as being "spam".

20. According to NOIE the drafting of the Bill to include single emails is intended to prevent the circumvention of various definitions of "bulk" email. NOIE also notes that "[t]he legislation provides the ACA a measure of discretion in enforcement to ensure that the response is proportional to the breach. In cases where a single unsolicited electronic message is sent, then a formal warning would generally be sufficient to cause a change in the contravening behaviour."[7]

21. The ACS proposes an amendment in paragraph 14 of their submission which would ensure that a single unsolicited commercial email, when distributed by a sender with a bona fide held view that the addressees would have an interest in

[7] National Office for the Information Economy, *Submission No. 14*, p. 14.

receiving them, would not be subject to penalties[8]. Labor recommends that the Bill is amended to reflect this.

Recommendation:

- The amendment of the *Spam Bill 2003* to include a mechanism where single messages distributed by a sender with a bona fide held view that the addressees would have an interest in receiving them, would not incur a penalty. As an example, Labor notes the amendment in paragraph 14 of the ACS submission.

Schedule 1 Exemptions – "designated commercial electronic messages"

22. Labor concurs with the Explanatory Memorandum when it states that the reason for exempting "designated commercial electronic messages" from organisations listed in Schedule 1 Clause 3 is to avoid any:

> "unintended restriction on government to citizen, or government to business communication, nor any restriction on religious or political speech."[9]

23. However, it is unclear why the Government has chosen to apply this reasoning in an inconsistent fashion. Clearly an arbitrary decision has been made to protect the free speech of some classes of political, religious and charitable organisations, and not others. NOIE has stated that:

> "Religious organisations and charities commonly reach beyond their congregations or membership to deal with broader elements of society that have no ongoing relationship with their organisation. The beneficial nature

---

[8] Australian Computer Society, *Submission No. 13*, p. 2.

[9] *Spam Bill 2003 Explanatory Memorandum*, p. 107.

> of the activities of these sectors has lead to their exemption from the prohibition on sending of unsolicited commercial electronic messages, in order to ensure there are no unexpected or untoward impacts on the sector."[10]

24. Labor agrees with this statement but believes that Schedule 1, Clause 3 should be expanded to include trade unions, and other not-for-profit political lobby groups, such as the Australian Council of Social Service, Amnesty International, or AusFlag. Labor does not agree that the exemptions applying to "designated commercial electronic messages" listed in Schedule 1 of the Spam Bill should be scaled back or removed, as argued by some respondents.

25. It is unclear whether charitable organisations which also engage in political lobbying would be covered by this exemption. Currently these types of organisations are unfairly disadvantaged by the measure. This point was raised in the submission from the Australian Council of Trade Unions which said:

> "Unions should be able to send out mass e-mails to members, supporters and to other groups and individuals participating in our democratic society so long as an effective opt-out system is provided and maintained.
>
> "The ACTU submits that unions should be exempted on the same basis as other non-profit community groups. If this is not done, it will be difficult to explain other than as reflecting the Government's ideological bias against unions."[11]

26. The argument that prohibiting unsolicited *commercial* emails from Clause 3 organisations would not pose any restriction on these forms of communication is noted, however, Labor is concerned that there may be instances where religious or political speech might overlap with some commercial activity. For example,

---

[10] National Office for the Information Economy, *Submission No. 14*, p. 11.

[11] Australian Council of Trade Unions, *Submission No. 19*, p. 2.

where a charity combines a non-commercial message with a request relating to a fund-raising activity.

27. In contrast, Labor notes the claim by NOIE that "very few messages currently sent have been identified as falling squarely within the scope of these exemptions."[12] For example, witnesses before the Committee only raised "a couple of isolated cases in which charities have spammed."[13] In this context these exemptions, if applied consistently across all not-for-profit political groups, are an appropriate way to protect free political and religious expression.

28. Labor recommends that the exemption outlined in Clause 3 of Schedule 1 should be applied consistently, and therefore expanded to include Trade Unions and not-for-profit political lobby groups.

29. Labor also supports the insertion of a provision to require a functional unsubscribe facility to be placed in "designated commercial electronic messages", to enable recipients to "opt-out". Labor notes that National Privacy Principles are still applicable.

30. Labor recommends the removal of provisions of the Spam Bill exempting senders of "designated commercial electronic messages" from including a functional unsubscribe facility in such messages.

Recommendations:

- The amendment of the exemption outlined in Schedule 1, Clause 3, so that the exemptions are applied consistently, and expanded to include Trade Unions and not-for-profit political lobby groups.
- The amendment of the *Spam Bill 2003* to remove provisions that exempt

[12] National Office for the Information Economy, *Submission No. 14*, p. 9.

[13] Mr Troy Rollo, *Proof Committee Hansard*, Senate Environment, Communication, Information Technology and the Arts Legislation Committee, 23 Oct. 2003, p. 27.

senders of "designated commercial electronic messages" from including a functional unsubscribe facility in such messages.

"Conspicuous Publication"

31. EFA, the Australian Consumers' Association, and CAUBE.AU raised concerns with the "conspicuous publication" exception to the rule in Schedule 2, Clause 4, that consent to receiving commercial electronic messages may not be inferred from the mere fact that an electronic address has been published.

32. EFA described this exception as "seriously flawed" and, along with the Australian Consumers' Association, recommended that the inference should be reversed so that consent may only be inferred from conspicuous publication when a statement to this end accompanies the publication.[14]

33. The exception allows consent to be inferred if a work-related email address has been "conspicuously published" (on the Internet, or in an offline form, such as on a business card), the electronic message is work or business related, and the publication is not accompanied by a statement indicating an objection to being sent unsolicited commercial email.

34. NOIE has pointed out that a person who wished to receive only a certain class of message could modify this statement to suit themselves. For example: "no spam – but offers to sell antique jam tins always welcome"[15]. Given the existing hurdles accompanying this exception, Labor considers this to be appropriate.

---

[14] Electronic Frontiers Australia, Inc., *Submission No. 5*, pp 19-21; and Australian Consumers' Association, *Submission No. 6*, pp 2-3.

[15] National Office for the Information Economy, *Submission No. 14*, p. 7.

35. CAUBE.AU also expressed reservations about the exception, based on the absence of any time limit to which the exception can apply. Its submission stated that:

> "A person who has had their email address conspicuously published at one time should not be subject to being bombarded with spam for an eternity as a result of data sharing arrangements."[16]

36. In relation to the "conspicuous publication" exception, Labor recommends that Clause 4 of Schedule 2 is amended to add a freshness requirement for consent inferred by conspicuous publication.

Recommendation:

- The amendment of Schedule 2 Clause 4 of the *Spam Bill 2003* to add a freshness requirement for consent inferred by "conspicuous publication".

Conclusion

37. Labor believes that the growth of spam acts as a disincentive for citizens to use email, and therefore the Internet. This is a cause of grave concern, not least because so many essential government, business and community services are now online and use email to communicate. Email is the ubiquitous "killer application" of the Internet, and given that the cost of spam is borne by the recipient, spam is an unacceptable and unfair abuse of the medium. That is why Labor believes that the Government has a responsibility to act. Labor is pleased that the Government has

[16] Coalition Against Unsolicited Bulk Email, Australia, *Submission No. 7*, p. 12.

finally and belatedly responded to Labor's call for a legislative response to the increasing incidence of spam.

38. Labor supports the general aims of these Bills. Based on a close examination of the concerns raised during the course of this Inquiry, Labor has identified important areas where these Bills can be improved.

39. Labor recognises that there may be unforseen problems which have not come to light through this Inquiry. However Labor believes that Australians need a legislative response to spam. After waiting over 18 months for the Government to take action this worsening problem must be addressed.

40. Labor's recommendations address the weakest aspects of these Bills, and hopes that the Government will constructively consider amendments arising from them.

41. Labor notes the scheduled review of these Bills, as required by section 46 of the Spam Bill, will provide an opportunity to further improve the application and operation of the anti-spam regime.

42. Labor recognises that these Bills are only one part of an appropriate response to the rising incidence of spam, and recommends that the Government proceed with a concerted public education campaign involving consumer groups and industry to further assist internet users to protect themselves against the costly, frustrating and damaging effects of spam.

43. Summary of Recommendations:

- The amendment of provisions in the *Spam (Consequential Amendments) Bill 2003* relating to search and seizure operations on private premises without a warrant so that consent must be obtained from the individual whose property will be subject to such operations;
- The amendment of the *Spam (Consequential Amendments) Bill 2003* to prevent search and seizure operations on the premises of spam recipients;
- The amendment the proposed section 547J of the *Telecommunications Act 1997* to remove the existing strict liability test and to tighten its scope to affect a smaller class of people, and that its operation is not subject to a test of strict liability;
- The amendment of the *Spam Bill 2003* to include a mechanism where single messages distributed by a sender with a bona fide held view that the addressees would have an interest in receiving them, would not incur a penalty. As an example, Labor notes the amendment in paragraph 14 of the ACS submission;

- The amendment of the exemption outlined in Schedule 1, Clause 3, so that the exemptions are applied consistently, and expanded to include Trade Unions and not-for-profit political lobby groups.
- The amendment of the *Spam Bill 2003* to remove provisions that exempt senders of "designated commercial electronic messages" from including a functional unsubscribe facility in such messages;
- The amendment of Schedule 2 Clause 4 of the *Spam Bill 2003* to add a freshness requirement for consent inferred by "conspicuous publication"; and
- That the Government considers the non-legislative recommendations made by respondents to this Inquiry when implementing its broader approach to spam.

Senator Kate Lundy

Australian Labor Party

Australian Democrats Minority Report

Senate Environment, Communication, Information Technology and the Arts Legislation Committee

Spam Bill 2003

Introduction

The Australian Democrats support the broad intent of the Spam Bill 2003.

We have long been aware of the increasing cost and time consuming impact to business and the broader community resulting from spam, and its potential to cause offence to its recipients. Indeed we have been vocal advocates for the need for a range of legislative and cooperative measures to respond to the volumes of unsolicited email traffic causing enormous expense to end-users, and traffic congestion to electronic networks worldwide.

We welcome this Bill as an attempt to respond to these issues. We believe Australian business and individuals should not to be forced to pay for unsolicited materials particularly those that are offensive, misleading and inaccurate. We commend the intention to introduce a broad requirement for recipient consent, and options for opting out altogether. We acknowledge that a range of civil sanctions should accompany these measures in order to make the 'destructive and intrusive practices followed by spammers less desirable'[1].

Indeed the Australian Democrats find there is much to commend in this Bill, yet there are also a number of flaws in the drafting of the Bill that detract from its efficacy, and further, have the potential to seriously impinge on the rights of individuals. Even enthusiastic supporters of the Bill have recommended a range of changes, many of which are reflected in this report.

We acknowledge the view of the Committee Chair that the Spam Bill 2003 is groundbreaking legislation and, that without the benefit of perfect foresight, it may require some future refining to make it fully functional[2]. To this extent we welcome the provision for review following two years of operation.

---

[1] Mr Keith Besgrove, Chief General Manager, Regulation and Analysis, NOIE, *Proof Committee Hansard,* p.2

[2] Senator Alan Eggleston, Chair, Senate Environment, Communications, Information Technology and the Arts Legislation Committee, *Draft Report,* p.52

Having said this, we also believe that where there are clearly identified loopholes already evident, as there are in this Bill, it is incumbent upon the legislator to ensure the Bill is as watertight as it can be from the outset.

The Australian Democrats share the following concerns with many of those who submitted to the inquiry:

1. Definition and Scope of 'Unsolicited' Email;
2. Powers relating to search and seizure;
3. Offence provisions relating to assistance
4. Range of exempt organisations;
5. Opt out Methods; and
6. Compensation for Costs and Damages.

These concerns are discussed in more detail in the pages that follow, and are preliminary in nature. We reserve the right to further develop and/or alter the views contained herein.

Recommendations

Recommendation 1: That the Bill be amended to require the sender of unsolicited electronic messages is able to demonstrate a genuine belief that the addressee is likely to have an interest in the content of a given message.

Recommendation 2: That the Bill be amended to prohibit unsolicited bulk email regardless of whether it is of a commercial or non-commercial nature.

Recommendation 3: That the Bill be amended to require inspectors to obtain a warrant for search or seizure of property, in the absence of securing permission from the owner of the hardware to be searched or seized.

Recommendation 4: That the Bill be amended to require that search or seizure warrants expressly indicate what items or types of files may be searched or seized.

Recommendation 5: That the Bill be amended to ensure that inability to provide information or assistance is not grounds for an offence, and that this provision is only applied to those deliberately obstructive in the provision of reasonable access.

Recommendation 6: That the Bill be amended to prevent government bodies, political parties, religious organisations and charities being exempted from its provisions.

Recommendation 7: That the Bill be amended to ensure all unsolicited electronic messages be required to contain an opt out clause.

Recommendation 8: That the Bill be amended to ensure that any method chosen by a recipient of a commercial electronic message is accepted as a means of communicating that person's desire to opt out of future communication.

Recommendation 9: That the Bill be amended to ensure receipt of spam is grounds upon which the recipient may seek damages and costs from the sender.

Recommendation 10: That the Bill be amended to ensure consideration for damage compensation gives regard to whether the owner was consulted, able to give appropriate warning or guidance on the operation of the equipment, and whether they were required to do so by law.

Definition and Scope of Unsolicited Email

A number of submissions raised questions about definitional ambiguity in the Bill and whether spam only related to bulk or single messages.

In its evidence to the Committee, the Australian Computer Society Inc, submitted that a definition of 'unsolicited' should be included in the Bill, to provide a greater degree of clarity in relation to issues of consent.

It was ACS Inc's view that it is not so much the relationship between an email sender and recipient that determines issues of consent, but rather the content of each individual message. Consequently, APS has argued for inclusion of a definition of 'unsolicited' that requires the sender to demonstrate a genuine belief that the recipient is likely to have an interest in the content of the email.

> "At the moment the onus of proof is on the sender to prove (a) that the recipient gave consent or (b) that the person did not know that the message had an Australian link or (c) that the message was sent by mistake. The onus of all of those things is supposed to be cast on the sender. We suggest that it is quite reasonable to also cast on the sender the onus of proving that they held a genuine belief that the addressee is likely to have had an interest in the content."[3]

This view was also supported in evidence by the Coalition Against Unsolicited Bulk Email, Australia (CAUBE).[4]

We are of the view that consideration given to the likely interest of a recipient in the content of an unsolicited message, and a requirement to be able to demonstrate how this conclusion is reached is an appropriate mechanism. It will not only assist to reduce unsolicited traffic, but will also require greater accountability, clarifying issues of consent, and place limits on allowable messages that arise from 'existing relationships'.

The Spam Bill 2003 in its current form prohibits the sending of unsolicited electronic messages of a commercial nature. The Australian Democrats believe the scope of the Bill should be expanded to also include unsolicited email of a non-commercial nature.

---

[3] Mr Philip Argy, Vice President and Chairman, Economic, Legal and Social Implications Committee, Australian Computer Society Inc, *Proof Committee Hansard,* p.14

[4] Mr Troy Rollo, Chair, Coalition Against Unsolicited Bulk Email, Australia (CAUBE), *Proof Committee Hansard,* p.22

We are of the view that a bill seeking to limit and protect against unsolicited bulk email should not distinguish between the commercial or non-commercial nature of that email, and that all unsolicited email should be prohibited.

Recommendation 1: That the Bill be amended to require the sender of unsolicited electronic messages is able to demonstrate a genuine belief that the addressee is likely to have an interest in the content of a given message.

Recommendation 2: That the Bill be amended to prohibit unsolicited bulk email regardless of whether it is of a commercial or non-commercial nature.

Powers Relating to Search and Seizure

Many submissions raised concerns about the powers extended to Australian Communication Authority inspectors in being able to enter premises, and search and seize property. These concerns related specifically to the failure of the Bill in any instances to require inspectors to present search warrants, a failure to determine limits on the extent to which searches may be conducted, issues in relation to who might consent to search and seizure, and arising out of all of these issues, a range of significant privacy concerns.

In evidence given at the Committee hearing by Ms Irene Graham, Executive Officer, Electronic Frontiers Australia Inc:

> "We feel that the provision of search powers that are without a warrant – and that also refer to the owner or occupier consenting – potentially opens the law to being used in a very intrusive manner… We feel that the legislation needs to be changed to ensure that it cannot be misused."[5]

Ms Graham went on to argue that, in the view of the EFA, searches should not be permitted at any time without an authorising warrant. By comparison, the Australian Computer Society Inc opted for a slightly less restrictive regime in which search and seizure warrants be required unless the hardware owner themselves consented to that search.[6]

---

[5] Ms Irene Graham, Executive Officer, Electronic Frontiers Australia Inc, *Proof Committee Hansard,* p. 5.

[6] Mr Philip Argy, Vice President and Chairman, Economic, Legal and Social Implications Committee, Australian Computer Society Inc, *Proof Committee Hansard,* p.13

In answer to a Question on Notice, the Mr Besgrove of the NOIE acknowledged the desirability of an owner's consent, and that in it's absence, there was a very real possibility that evidence would be rendered inadmissible in a court of law. Mr Besgrove went on to state:

> "It is consequently highly likely that in the absence of consent from the owner of the account or computer, the ACA would as a matter of practice, seek a warrant to enter and search premises."[7]

Given this likelihood, and the fact that such a scenario would both alert a suspect, and provide time to remove or destroy evidence, it would appear to make sense that an ordinary course of action would be to secure a warrant from the outset – to ensure access and admissibility of evidence and to maximise the element of surprise.

The EFA submission expressed concern about the range of material stored on a computer, particularly stored emails from any number of sources, which in turn had a range of privacy implications for those people in no way associated with the alleged spam breach.[8]

Consequently, the Australian Democrats are of the view that the issuing of any search warrant should also indicate the specific information that may be collected in the course of that search.

The Internet Society of Australia (ISOC-AU) raised concerns in their submission about the monitoring power provisions within the Spam (Consequential Amendments) Bill 2003. Specifically their concerns related to powers that would allow the search or seizure of any "thing" reasonably suspected to contain evidence about a breach of the Spam Act.[9] The wording of these provisions fails to specify what that "thing" may be, and conceivably could allow for the seizure or search of any computer on which an email deemed to be spam resides.

While the NOIE regard it as unlikely that a spam recipient would be at risk of search and seizure[10], the Australian Democrats concur with the views of Electronic Frontiers Australia who stated:

> "While it may be considered unlikely that inspectors would search the homes of recipients of spam, it is essential that the law specifically not allow that to occur without the consent of the relevant individual."[11]

---

[7] Mr Keith Besgrove, Chief General Manager, Regulation and Analysis, NOIE, *Answer to Question on Notice, 27th October 2003*

[8] Ms Irene Graham, Executive Officer, Electronic Frontiers Australia Inc, *Proof Committee Hansard,* p. 5.

[9] Submission No. 11, Internet Society of Australia (ISOC-AU), p.1.

[10] Submission No. 14, NOIE, p.17.

Recommendation 3: That the Bill be amended to require inspectors to obtain a warrant for search or seizure of property, in the absence of securing permission from the owner of the hardware to be searched or seized.

Recommendation 4: That the Bill be amended to require that search or seizure warrants expressly indicate what items or types of files may be searched or seized.

Offence Provisions Relating to Assistance

The Spam (Consequential Amendment) Bill as it currently stands, establishes as an offence a failure to provide information or assistance that is reasonable or necessary. The Australian Democrats share the view expressed by a number of submissions that these provisions may extend to a failure to provide a password or encryption key. We do not support this provision particularly as it currently applies not only to owners, but also to occupiers.

We maintain that due to the nature and variety of information stored on computers today, strong security is the norm, or it should be. Few company employees or in the instance of a private dwelling, few housemates, could be expected to know the full details of password, encryption and privacy systems for machines they do not own. Few people for example, would know that there are separate passwords for the BIOS, the Administrator account, and possibly, for each individual user. Each of these permissions can be prescriptive, limited in their nature, and only allow certain users access to some areas and not to others. The Bill as it currently stands, assumes that any computer operator (or flatmate) would have access to these pieces of information, and therefore, the capacity to bypass security and encryption devices.

This concern was shared by Ms Graham of Electronic Frontiers Australia, who stated in hearing:

> "The problem with the provisions… is that they pay no attention to the fact that a person may have legitimately lost… an encryption key and may be unable to provide the sought assistance. The penalties do not give a person any way to prove it. You have a situation where… if a person has forgotten a password they can be thrown in jail, in theory, for six months."[12]

---

[11] Submission No. 5, Electronic Frontiers Australia, p.8.

[12] Ms Irene Graham, Executive Officer, Electronic Frontiers Australia Inc, *Proof Committee Hansard,* p.7.

Recommendation 5: That the Bill be amended to ensure that inability to provide information or assistance is not grounds for an offence, and that this provision is only applied to those deliberately obstructive in the provision of reasonable access.

Range of Exempt Organisations

The Australian Democrats are of the view that government bodies, political parties, religious organisations and charities should not be authorised to send designated commercial electronic messages, thus exempting them from provisions contained within the Bill.

This is a view supported by many of the respondents to the Committee Inquiry, and was strongly reinforced in the submission from the Australian Privacy Foundation when they noted:

> "The Bill fails to identify the true scope of the problem, and fails to look ahead. What most people find objectionable, and a growing nuisance, are unsolicited communications from any source and with any content. "Commercial communications" are only one subset of Spam – most people, in our view, find uninvited charitable appeals and solicitations, political communications, and even public service announcements and notices equally annoying."[13]

In response to a question from a Committee member about the extent to which unsolicited approaches from charities, and religious and political organisations were commonly accepted, Electronic Frontiers Australia responded by stating:

> "EFA would strongly disagree with that. I do not want to get direct marketing or messages about goods and services from charities or religious organisations or government bodies either. If I want to communicate with them, I will tick a box on a form."[14]

Recommendation 6: That the Bill be amended to prevent government bodies, political parties, religious organisations and charities being exempted from its provisions.

---

[13] Submission No. 10, Australian Privacy Foundation, p.1.

[14] Ms Irene Graham, Executive Officer, Electronic Frontiers Australia Inc, *Proof Committee Hansard,* p.8.

Opt out Methods

The Australian Democrats fully support the requirement for commercial electronic messages to contain a functional unsubscribe facility. We do not accept however that there should be circumstances or organisations exempted from providing such a clause.

Additionally, we concur with the submission from the Australian Computer Society, that any request to be removed from a mailing list, communicated in any mode, shall be respected.[15] The Australian Democrats do not believe there is any need for a prescribed form of opting out.

Recommendation 7: That the Bill be amended to ensure all unsolicited electronic messages be required to contain an opt out clause.

Recommendation 8: That the Bill be amended to ensure that any method chosen by a recipient of a commercial electronic message is accepted as a means of communicating that person's desire to opt out of future communication.

Compensation for Costs and Damages

A substantial driver behind the development of the Spam Bill 2003 was the cost incurred to business and private individuals contending with large volumes of unwanted data.

The Australian Democrats share the view expressed by ACS are of the view that where a person or company has incurred any expense arising from the receipt of unsolicited spam, they should be entitled to seek redress for expenses through the court system.[16]

With regard to damages and data loss caused as a consequence of search and seizure, the Bill currently provides that compensation will be partly determined on the basis of whether the owner, or the owner's employees and agents, provided appropriate warning and guidance on the operation of the equipment.

---

[15] Submission No. 13, Australian Computer Society, p.2.

[16] Submission No. 13, Australian Computer Society, p.2.

The same principle that leads to our concern regarding possible imprisonment for failure to provide a password or encryption key, applies in this case. The Australian Democrats are of the view that any damage arising from an assumption that anyone other than the owner will have full knowledge of all security safeguards, and consequently the impact of any attempts to tamper with these, is an unsafe one. Consequently, we believe that any damage or data loss occurring as a result of search and seizure that occurs without a warrant, or direct consultation with the owner, should be fully compensated.

Recommendation 9: That the Bill be amended to ensure receipt of spam is grounds upon which the recipient may seek damages and costs from the sender.

Recommendation 10: That the Bill be amended to ensure consideration for damage compensation gives regard to whether the owner was consulted, able to give appropriate warning or guidance on the operation of the equipment, and whether they were required to do so by law.

Senator Brian Grieg

Australian Democrats

Appendix 1

Submitters

1	Mr Colin Hunt
2	Mr Howard F Lowndes
3	Professional Way Pty Ltd.
4	Australian Direct Marketing Association (ADMA)
5	Electronic Frontiers Australia Inc. (EFA)
6	Australian Consumer's Association
7	Coalition Against Unsolicited Bulk Email, Australia (CAUBE.AU)
8	Microsoft Australia
9	Captain Susan L. Smith
10	Australian Privacy Foundation
11	Internet Society of Australia (ISOC-AU)
12	Mr Rowan Rafferty
13	Australian Computer Society Inc.
14	National Office for the Information Economy (NOIE)
14a	National Office for the Information Economy (NOIE)
15	Mr Dan Svantesson
16	Ms Sharon Grierson MP
17	Mr Andrew Calvin
18	Infobase Systems Pty Limited
19	Australian Council of Trade Unions (ACTU)

Appendix 2

Witnesses at Public Hearing

Thursday, 23 October 2003

National Office for the Information Economy (NOIE)

Mr Keith Besgrove, Chief General Manager – Regulation and Analysis

Mr Lindsay Barton, Manager – Online Policy

Department of Communications, Information Technology and the Arts (DCITA)

Ms Kirsten Miller, Legal Group

Electronic Frontiers Australia Inc. (EFA)

Ms Irene Graham, Executive Director

Australian Computer Society (ACS)

Mr Philip Argy, Vice President

Australian Direct Marketing Association (ADMA)

Ms Jodie Sangster, Legal and Regulatory Affairs Manager

Mr Robert Edwards, Chief Executive Officer

Coalition Against Unsolicited Bulk Email Australia (CAUBE.AU)

Mr Troy Rollo, Chair