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]

> 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

---

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.

> 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]

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

---

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.

> 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.

Searching the premises of spam recipients

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

---

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.

> 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 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]

---

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

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

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

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

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.

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:

---

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

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

> …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.