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