Submission to the Commerce Select Committee on the Unsolicited Electronic Messages Bill

20th March 2006

Submission to the Commerce Select Committee on the Unsolicited Electronic Messages Bill

Introduction

1. This submission is from InternetNZ, the Internet Society of New Zealand (Inc).

2. We are located at Level 9 Exchange Place, 5-7 Willeston St, Wellington (PO Box 11-881, Wellington 6004). The point of contact for this submission is Jordan Carter, Research & Policy Officer, who is contactable by phone on (04) 495 2118 or by e-mail (jordan@internetnz.net.nz).

3. InternetNZ seeks permission to address the Committee orally in support of its submission. Please contact Jordan Carter using the details shown above to arrange this.

4. InternetNZ is a membership-based not-for-profit organization responsible for the administration of the .nz domain name registry. Our mission is to protect and promote the Internet in New Zealand; we advocate the ongoing development of an open and uncaptureable Internet, available to all New Zealanders.

5. InternetNZ has been heavily involved in the campaign against spam since 2003, and has actively contributed to the development of this legislation. Its activities have included:

    i. The organization and hosting of two well-attended seminars on spam – one on the issue generally and a major gathering specifically on legislative options. The second of these was formally opened by the Minister, Hon. David Cunliffe, and was attended by a wide range of representatives from business, industry and government departments.
    ii. The establishment and maintenance of an informational anti-spam website (http://stopspam.net.nz) and the publication of educational resources on the issue.
    iii. Two meetings with Australian government officials to discuss their legislation ("The Australian Spam Act 2003") and their enforcement of the legislation.
    iv. Extensive liaison with peers and stakeholders, in particular the New Zealand Direct Marketing Association (NZDMA, http://www.marketing.org.nz/), the Telecommunications Carriers' Forum (http://www.tcf.org.nz/) and other business and industry bodies.
    v. Service on the board of, and provision of the secretariat for, the Asia-Pacific Coalition Against Unsolicited Commercial E-mail (APCAUCE, http://www.apcauce.org), a major regional anti-spam lobbying and interest group.
    vi. Attendance at two OECD Summits on spam, one in Brussels (Belgium) in early 2004, the other in Busan (Korea) in late 2004.
    vii. Initiating membership of the London Action Plan against spam: the London Action Plan (http://www.londonactionplan.com/) is a major consortium of anti-spam enforcement agencies including the UK Office of Fair Trading and the US Federal Trade Commission.

6. InternetNZ commends the intention behind the Government's Unsolicited Electronic Messages Bill ("the Bill"), and has been heavily involved in the consultations which led to the Bill's development. InternetNZ would like to acknowledge especially the Minister, Hon David Cunliffe, for his personal interest in this issue and for championing the legislation.

7. Aside from one serious reservation we hold concerning the enforcement regime proposed by the Bill, InternetNZ broadly supports the legislation and, if it is appropriately amended, would like to see the Committee recommend it for passage through the House as quickly as possible.

8. In developing this submission, InternetNZ has consulted with its members, with a range of Internet Service Providers and with numerous anti-spam workgroups and firms. We have also met with ACMA (the Australian Communications and Media Authority, the regulator responsible for enforcing the Australian legislation) to discuss the Australian Spam Act's enforcement provisions and their experience arising from them. The views we present here are broadly representative of those held by the industry and by those involved in fighting spam in New Zealand and overseas.

9. This submission is broken into the following sections:

    i. General Policy Position
    ii. Enforcement Regime
    iii. Drafting Issues
    iv. A Brief Conclusion.

10. For ease of consideration, detailed arguments are confined to appendices, which do not need to be read in order to get a sense of our policy position, but which provide key in-depth information in support of the changes proposed in the main body of the submission.

General Policy Position

11. It has become one of the most widely-quoted truisms of the anti-spam community that there are five crucial weapons in the fight against spam:

    i. Technical measures (filtering, blocklists, shared data services and so on)
    ii. Education (making end-users aware of how to handle, avoid and report spam)
    iii. Legislation (to provide a legal framework for handling the worst offenders and to guide the marketplace to the adoption of best practices)
    iv. International co-operation (like the Internet, spam is a borderless phenomenon)
    v. Enforcement (the American experience has shown that it's better to have bad laws well-enforced than good laws badly-enforced)

12. InternetNZ believes strongly that effective legislation is an essential component in the fight against spam, even in countries like New Zealand where there is not a large indigenous spammer population. Solid legislation prevents spammers from seeing New Zealand as a refuge from tougher overseas legislative regimes (the so-called “arbitrage effect”), and simplifies the exchange of information and co-operation with anti-spam agencies in other nations, necessary to curtail the global spread of the problem. It is also in keeping with our long-standing desire to present ourselves as a “good international citizen” by adopting best practice wherever possible.

13. InternetNZ has actively engaged the New Zealand Government and its agencies in the development of the Unsolicited Electronic Messages Bill, and applauds the effort and thought that has gone into the draft version of the legislation. We particularly note important

points of similarity with the Australian Spam Act 2003: given that the Australian Act is internationally regarded as a model of excellence in Anti-Spam legislation, this is an extremely positive outcome.

14. InternetNZ is generally pleased with the definitions and requirements contained in the draft legislation: in particular, the idea of the New Zealand Link, the requirement for opt-in address management regimes, and the restrictions on address harvesting are excellent and represent solid best-practice in the international environment. We are rather less happy with the distinction drawn between commercial (opt-in) and promotional (opt-out) mail, but this does not in itself substantially affect our support for the legislation as a whole.

15. Although we are broadly satisfied with the draft legislation, we were disappointed that in one specific and crucial aspect it falls badly short – that is in the matter and terms of enforcement.

Enforcement Regime

16. The enforcement regime set out in the Bill appears to have been motivated more by a sense of fiscal asceticism than by any desire to produce an effective, workable solution.

17. As drafted, the Bill creates an enforcement agency under the aegis of the Department of Internal Affairs, which is responsible for administering the enforcement sections of the legislation.

18. The only parties able to lay complaints with the enforcement agency are Internet Service Providers or similar businesses – indeed, the enforcement agency is expressly forbidden from accepting complaints from members of the public. Worse, in our eyes, the Bill *obligates* any organization fitting the description of a "Service Provider" to accept complaints from the public.

19. As currently worded, the Bill does not prescribe exact terms and conditions under which ISPs are required to operate: are they required to accept all reports of spam, regardless of origin? Are they required to accept reports only of spam originating within their networks? Are they perhaps required to attempt to distinguish between foreign spam and spam with a New Zealand link? This ambiguity creates uncertainty and expense for ISPs, and we contend in the strongest terms that it is neither desirable nor necessary in the first place.

20. This model of enforcement is effectively the imposition of an unfunded mandate: it requires businesses, for the most part small and operating on narrow margins, to be the primary vehicle in implementing a statute, yet it provides no relief, guidance or support for those businesses – it creates an obligation without incentive.

21. The approach is flawed in several key respects:

    i. It places the burden and cost of enforcement on organizations that are already bearing the brunt of the problem: ISPs already expend considerable portions of their ongoing costs (estimates as high as 15% of operating costs are routinely cited) in mitigating spam via technical means. As one commentator noted, forcing them to handle complaints as well would be *"like requiring victims of crime to pay the costs of prosecuting the offenders"*.

ii. In the total absence of incentives, the majority of ISPs will naturally comply with the letter of the legislation while ignoring its spirit – they will do the minimum necessary to accept complaints, then will silently ignore or discard them. We do not believe they could be criticized for doing this, but feel that it clearly neutralizes most of the Bill's potential effectiveness.
iii. In the unlikely event that ISPs actually choose to comply with the spirit of the Bill, the enforcement regime as proposed would require the creation of hundreds of new helpdesk positions across the country, which, while possibly good for employment statistics, is a manifestly inefficient way of administering a piece of legislation when a small central organization could do the job better and considerably more cheaply.
iv. Crucially, it does not equip the formal enforcement agency with the tools or the information it needs to perform either its domestic enforcement role, nor the international co-operation component of its duty. The Australian experience (see Appendix B) shows clearly that automated processing of spam complaints yields information invaluable for both purposes, and that the absence of this information would immeasurably compromise the agency's ability to function properly. Spam prosecutions, while we expect them to be rare, require considerable quantities of forensic information – information that can only be gathered proactively.

22. We can only assume that such an ineffectual enforcement model must have been chosen through concern of creating a large, expensive bureaucracy to deal with what might be perceived as a relatively minor problem – the old adage of "using a sledgehammer to swat a fly". We do not believe that such fears are either valid or compelling. In Appendix A we show that a small, largely automated enforcement agency could easily handle the workload required to police the Bill in its entirety, and we back this model up with solid, current information from the Australian Enforcement Agency's experience in the first 18 months of overseeing their Act.

23. We cannot stress enough how unsatisfactory the draft enforcement model appears to us. InternetNZ would have considerable trouble supporting the Bill if the enforcement provisions remain as drafted: for the reasons shown above, we feel they are impose unreasonable costs on the industry and will result in the Bill being almost completely ineffective.

24. Instead, we have prepared a detailed proposal (see Appendix A) showing how a small, centralized enforcement agency could be set up to handle the entire burden of enforcement of the Bill. Based largely on automated practices using tools that already exist and are proven, our proposed enforcement authority would have the following key advantages:

i. Low staffing levels (five people in our proposed model)
ii. Setup costs substantially lower than $1m.
iii. Continuous access to current, up-to-date reports on both local and internationally-originated spam appearing in New Zealand.
iv. Sensible use of automation may in fact significantly reduce the existing burden on ISPs by allowing them to "farm" much of their spam complaint load onto the agency's automated systems – a "public good" outcome.
v. Creation of efficient, centralized expertise that can be used to best effect, both in analyzing local spam flows and in liaising with international enforcement agencies.
vi. Its similarity to the Australian model makes inter-agency co-operation easier, and allows the agency to take advantage of the Australian experience.
vii. The ability to enter into MoUs with other jurisdictions to increase the effectiveness of global enforcement efforts (it is worth noting that the Australian enforcement agency,

the ACMA, has sponsored or entered into a number of MoUs in its first 18 months of responsibility for the Australian Spam Act).

25. A key point in understanding our proposed enforcement model is that it provides the public with a means of complaining, but through sensible automation, does not expose actual staff to public interaction. So, the public can feel well-served and empowered without the need to create of any form of excessive bureaucracy.

Drafting Issues

26. Aside from our concerns with the enforcement aspects of the draft legislation, there are a number of smaller drafting issues we feel we should mention, although these do not, for the most part, materially affect our support for the Bill. Rather than weighing down the body of our submission with these points, we have included them separately as Appendix C.

27. As noted in paragraph 14, we are not enthusiastic about the distinction drawn in the draft legislation between Commercial and Promotional e-mail. To our knowledge, no other anti-spam legislation in existence attempts to be simultaneously both Opt-in and Opt-out in nature, and it is our belief that the distinction simply creates ambiguity without actually providing benefits to any party. It seems odd to us that the Bill should be mandating best-practice (opt-in) for commercial entities, while accepting deprecated practice (opt-out) from other entities. Best practice should be the proper and only demand the Bill should make.

28. InternetNZ commissioned a report from Lowndes Jordan and Associates, an Auckland legal firm, on the draft legislation. It raises a number of issues at the drafting level that we believe the Committee would be well-served in considering. A copy of the Lowndes Jordan review is attached to this submission as Appendix D.

Conclusion

29. New Zealand has been slower than most Western nations to adopt anti-spam legislation, but we believe that, with appropriate modification, the proposed bill will represent an excellent outcome and will be able to take its place in the ranks of its global brethren with pride. We congratulate all involved in its creation for producing a draft as good as this.

30. Notwithstanding the excellent overall quality of the draft, InternetNZ urges the Select Committee to agree with our significant concerns about the shape of the proposed enforcement model and to recommend changes in tune with the suggestions we have made.

31. We are pleased to offer our assistance in any form should it be required, and in the event that the modifications outlined in this submission are made to the final form of the Bill, we undertake to use our resources and connections to promote and support it comprehensively when it becomes law.

InternetNZ Submission to the Commerce Select Committee on the Unsolicited Electronic Messages Bill

Appendix A – An Alternative Enforcement Model

Contents

Overview

1. The first draft of the The Unsolicited Electronic Messages Bill 2005 was introduced into the legislative process in July 2005 after extensive discussions with the broader Internet community that began in September 2003. The leadup to the draft involved consultations between Industry, Stakeholders and Government departments, including three significant workshops, moderated and led by InternetNZ.

2. In general, the reaction to the draft legislation within the Internet community has been broadly favourable: the definitions of "unsolicited electronic messages", the penalties for offending and the scope of the legislation are largely in accord with the consensus developed within the industry during the consultation process. Only the issue of the Enforcement Agency and its mandate as defined by the draft legislation has generated controversy, but that controversy has been significant and widespread.

3. Subsequent to the release of the draft legislation, InternetNZ invited interested parties within the Internet industry and the regulatory domain to a one day workshop in September, where the issue of the enforcement model under The Bill was reviewed.

4. This document summarizes the reasons why the proposed enforcement model is unlikely to be effective, and the conclusions and recommendations of the workshop, which lead to a suggested alternative enforcement more likely to be welcomed by the industry.

The enforcement model outlined in the draft legislation

5. The draft legislation tasks a specific agency, the Department of Internal Affairs, with the policing and enforcement of the bill. The enforcement agency's mandate allows it to accept complaints about non-compliant messages only from Internet Service Providers (ISPs), specifically excluding the public from the process. The bill's intention is evidently that the

public, as end-users, should make complaints to their ISP, who will determine whether or not the matter should be referred to the enforcement agency for action.

Problems with the draft model

6. A major difficulty with the model proposed in the draft legislation is that it places the majority of the burden of handling complains about non-compliant messages on ISPs, who are already significantly burdened by the phenomenon through having to provide technical measures for reduction and mitigation. Preventing the public from complaining to the enforcement agency will inevitably result in a significant increase in complaints made to ISPs, often about material over which the ISP has no control: in effect, the ISP becomes a free filtering service for the enforcement agency, dealing with the vast bulk of complaints without redress or compensation. In our view, this is akin to requiring the victim of a crime to pay the expenses involved in prosecuting the offender – it is, in simple terms, unfair.

7. An equally serious problem with the draft model is that it creates a formal enforcement agency that will not have access to most of the information it needs to fulfil its duties. The forensic process of tracking and prosecuting a spammer requires access to significant quantities of data in order to map the flow and volume of the spam involved. In the draft model, the information the agency gets is likely to be degraded and its volume substantially reduced as it passes through the ISP's own complaints process – if it is passed on at all. This would damage the agency's ability to analyse New Zealand spam flows, and would make its potential contribution to regional and global anti-spam efforts less valuable.

An alternative model

8. We believe that the enforcement model proposed in the draft legislation represents a reaction based on misunderstandings of the core problems surrounding Unsolicited Electronic Messages. In particular, it presumes a much higher reporting level than is actually likely to exist, and out of fear of creating an over-large bureaucracy to deal with that reporting level, it attempts to shunt the up-front burden to other organizations that will not need direct funding.

9. In fact, because of the “village” nature of the New Zealand Internet community, the number of clearly-identifiable breaches of the act is likely to be extremely small. The real issue is differentiating those cases involving a *New Zealand Link* (in terms of The Bill) from generic “spam”, which typically will not fall within the ambit of the act.

10. During the September workshop considering the enforcement problem, we concluded that the application of suitably-constructed centralized software automation to the problem would remove the reporting burden almost entirely. In this model, the public can report (indeed, are even *encouraged* to report) any spam they feel might have a New Zealand Link to a well-known service address (either a web site or possibly an e-mail address). The service address, rather than being a regular mailbox, will actually be a software process that scans the messages it receives for evidence suggesting a New Zealand Link. While the submitter of the suspect message would probably receive an automated response from the software process, the actual human involvement within the enforcement agency would be

limited to handling only those messages where the software process detects the possibility of a New Zealand Link and escalates it for action.

11. When the software detects a suspect message, it passes it on to an operative within the enforcement agency. The operative may decide to use any of a wide range of already-extant forensic software tools to trace the New Zealand Link within the message: if a link is found, the operative can take any of a range of actions, from contacting and liaising with a host ISP through to initiating actions under the Act in extreme cases.

12. Broad analysis of spam within the New Zealand Internet community suggests that the total number of spam messages with an identifiable New Zealand Link probably constitutes an amount less than one percent of the total volume of Unsolicited Electronic Messaging received during any period. We believe that this low volume, combined with a well-developed automated software scanning service, should result in levels of suspect messages that could easily be handled by as few as one or two operatives.

13. The InternetNZ workshop considered a number of possible structural models, including making the front-line agency a completely separate organization run by a board composed of industry and government figures, operating it as a sub-unit of a larger body, such as the Department of Internal Affairs, or even setting up a completely separate organization that acts as a "filtering layer", escalating any actionable matters to the formal enforcement agency.

14. The workshop considered the split-layer approaches and decided that, while they might free the formal enforcement agency to handle only matters requiring direct judicial input, such as prosecutions (which we would expect to be very rare), the loss of shared resources and information flow gained by homing the agency within a larger parent outweighed any possible benefits they might have. The workshop's eventual conclusion was that the agency would be best and most efficiently run as a sub-unit of an existing agency.

15. When considering basic resourcing requirements, the general feeling of the workshop was that the front line agency need only consist of five staff:

    i. A Manager, responsible for the overall running of the unit
    ii. An Investigator to handle interviews, evidence assessment and case preparation for any prosecutions under The Bill.
    iii. A Technical Lead, knowledgeable about the mechanics of spam, who could develop technical strategies, analyze the reports generated by the automated spam processing software, and liaise with international enforcement agencies.
    iv. A Systems Administrator, to maintain the servers on which the automated spam processing software runs, and to manage network and systems issues within the agency.
    v. An Administrative Assistant to handle data input and collation from the online reporting systems and to handle general administrative tasks in the office.

16. In situations where roles can be shared with the parent department (for instance, where management is assigned as a secondary role to an existing manager), these levels could be reduced even further. Similarly, we considered that the comparatively low levels of actual enforcement activity that are likely to be required make it quite possible that the roles of manager and investigator could be combined.

17. The automated spam processing software that is the hub of this process could be either an existing, proven package, such as SpamMatters (http://www.spammatters.com), the

product used by the ACMA in Australia, or else a custom-developed local solution. The workshop considered that this item was the most difficult to cost, and the figures shown below should only be considered estimates.

Example cost estimates

18. The InternetNZ-sponsored workshop spent some time considering the possible costs associated with setting up and running an enforcement agency using the guidelines in section (4). This was done primarily as a brainstorming exercise – naturally, we do not presume to tell other organizations how they should structure themselves. Nonetheless, the process was useful for identifying the likely levels of resource and staff such an organization might require.

19. Using the idea of an standalone sub-unit of the Department of Internal Affairs as a basis, the workshop concluded that the following costings might allow the realization of a practical and functional agency:

Staffing - $390,000 p.a.

- One manager, $110,000pa
- One investigator, $90,000pa
- One lead technical staff member, $80,000pa
- One system administrator, $65,000pa
- One administrative staff member $45,000pa

Overheads - $195,000 p.a.

- Calculated as 50% of staff costs
- Covers office space, stationery, general running costs
- Assumes high-speed network services

Computer equipment - $60,000 first year.

- Covers servers and staff PCs $30,000 p.a after

Spam analysis and tracking software $80,000 first year

- Rough estimate of cost only $40,000 p.a after

Publications - $75,000 first year

- For educational and informational purposes $40,000 p.a. after

Travel - $60,000 p.a.

- International for conferences etc - $25,000;
- Domestic for education etc, $35,000

TOTAL EXPECTED COSTS:	**First Year:**	**$860,000**
	Ongoing Cost:	**$755,000**

20. Note that there is an expectation that any actual prosecutions would be handled by the Legal Division of the DIA. Similarly, HR costs and services would be provided by the parent department.

InternetNZ Submission to the Commerce Select Committee on the Unsolicited Electronic Messages Bill

Appendix B – The Australian Experience

Introduction

1. In September 2005, when the draft form of the New Zealand Unsolicited Electronic Messages Bill was released, the InternetNZ Anti-Spam Task Force ("ATF") decided, as part of its submission strategy, to seek permission to visit the Australian Communications and Media Authority ("ACMA") – the enforcement agency for the Australian Spam Act – and discover their experiences in the first year of operating under the legislation. In December, the InternetNZ Office sought permission from the Minister of Communications, David Cunliffe, to approach the ACMA. That permission was granted in February 2006, and communicated to the ACMA, who kindly agreed to see a representative team. On February 13th, David Harris, David Farrar and Jordan Carter flew to Melbourne to meet with the ACMA.

The ACMA

2. The ACMA is the Australian government body tasked with watching over the telecommunications and media industries, and with enforcing various Australian Acts of Parliament, including the Spam Act 2003. Their Anti-Spam enforcement operation is based in Melbourne, on the 44th floor of the Melbourne Tower in central Melbourne.

Staff

3. The ACMA has allocated a total of seven-and-a-half staff to handle the enforcement of the Anti-Spam Act:

    i. Two front-line staffers handle input from the public and maintain the CRM system (see below) – one acts as supervisor for this part of the operation.
    ii. A technical specialist based in Canberra (as part of the High Technology Crime Squad) acts as a general liaison with Police and the "Intelligence Community", and is training as an Investigator;
    iii. One full-time and one contracted part-time technical staff look after the operational aspects of the programme;
    iv. One full time position develops educational materials, policy capacity and communications support for the unit (split between two part time staff) and
    v. Chris Duffy is the unit's Senior Investigator and, currently acts as Operations Manager.

4. The Anti-Spam unit does not have an on-board legal team, relying instead on the ACMA legal division for legal support when required. ACMA also provides standard HR and corporate functions.

Methodology

5. The ACMA accepts input on spam in two primary ways. The first is via a web form which the complainant must complete manually: the resulting information is entered directly into an off-the-shelf Customer Relationship Management (CRM) system, where it is evaluated by the two front-line staff. In its first eighteen months of operation, the CRM system has logged 8,000 reports. An interesting tactic used by the ACMA is to refer complaints received via the CRM system to both the complainant *and* the alleged offender. According to Mr Duffy, this has resulted in nearly an 80% response rate from alleged offenders, allowing many cases to be resolved amicably without further effort.

6. The second input involves an automated submission plugin designed for Microsoft Outlook. Using this plugin, the user can submit any spam he or she receives directly to the ACMA's automated spam processing system, SpamMatters, simply by selecting the message and clicking a button. The plugin ensures that the offending message is properly-packaged and submits it to the ACMA's spam reporting address, reportingspam@acma.gov.au. Estimates from the ACMA suggest that approximately 500,000 alleged spam messages have been reported using the plugin or forwarded to the reporting address in the first eighteen months of operation. Amusingly enough, the spam reporting address itself is now also receiving a significant amount of direct spam.

7. It is worth noting that the ACMA has an active policy of minimizing its direct interaction with complainants: anyone phoning the offices of the ACMA to try and complain about spam is instructed to use either the web form or the reporting address. When we asked Mr Duffy how many phone calls the office was actually fielding, he passed it off as inconsequential, saying "not a lot of people phone in".

SpamMatters

8. At the core of the ACMA's enforcement process is an Australian-developed package called SpamMatters, which is an automated spam processor and analyser. SpamMatters takes all the spam that is thrust at it, and examines it for patterns, similarities and programmed conditions. Just as the proposed New Zealand legislation defines a "New Zealand Link", the Australian Act has an "Australian Link", and SpamMatters has been tuned to search for such links.

9. Although Mr Duffy was not specific about the exact outputs generated by SpamMatters, it is clear that this is very close to the type of automation we have envisaged for use in our proposed enforcement model; the software escalates any cases of clear Australian Linkage it encounters, and is able to generate a wide range of reports. SpamMatters is a third-party product available for license (its author gave a presentation at the OECD meeting in Busan in 2004).

Outcomes in the first eighteen months of operation

10. The ACMA's presentation to the Australian Parliament as part of the mandatory review of the Spam Act (currently underway) contains the following key statistics:

Activity	Number of actions taken
Businesses warned to comply with the Act	More than 350 (warning letter sent)
Formal warnings under section 41	8
Fines and infringement notices issued	5
Enforceable undertakings	3
Search warrants	5
ACMA demands for formal interview	5
Prosecutions	1

11. Some aspects of these statistics were not explained, but the 350 warnings in the first row refers to automatically-generated warnings produced by the CRM system, and manually taken up with potential offenders on an informal basis, while the "Formal warnings" represents escalated complaints.

12. According to Mr Duffy, the "Search warrants" column refers only to domestic search warrants – to date, no International requests for searches under the Australian Act have been received.

13. The prosecution referred to in the last column was still *sub judice* at the time of the meeting, and was expected to be resolved in March. Although Mr Duffy was not able to provide any on-the-record information about the prosecution itself, he did indicate that the costs of taking the prosecution were significant – he estimated a figure of around AU$500,000.

InternetNZ Submission to the Commerce Select Committee on the Unsolicited Electronic Messages Bill

Appendix C – Detailed amendments to the Bill in line with improving the enforcement model

Clause 4

To amend the definition of "promotional electronic message by omitting in paragraph (b) the words "primary purpose" and substituting the words "purpose or one of the purposes"

Clause 6

To omit from paragraph (a) the words "primary purpose" and substitute the words "purpose or one of the purposes"

To omit from paragraph (a)(ii) the words "a financial advantage or gain from another person" and substitute the expression "ownership or possession of, or control over, any property, or any privilege, service, pecuniary advantage, benefit, or valuable consideration"

To omit paragraph (b)(vii)

Clause 10

To omit from subclause (3) the number "5" and substitute the number "3"

Clause 12

To insert in subclause (1) the following paragraph after paragraph (b)

(ba) The unsubscribe facility must not incur a cost to message recipients if they use the facility to unsubscribe.

Clause 23

To insert in paragraph (a) the following subparagraph after subparagraph (ii)

(i) make a complaint to the enforcement department:

Clause 24

To insert in subclause (1) after the expression “section 23(a)(i)” the words “if the complaint involves breaches of the Act by one of their customers”

Clause 25

To omit from paragraph (a) the words “but must not consider” and substitute the words “and may consider”

To insert in paragraph (b) after the words “service provider” the words “or any other person”

InternetNZ Submission to the Commerce Select Committee on the Unsolicited Electronic Messages Bill

Appendix D – Legal opinion from Lowndes Jordan

23 August 2005

Keith Davidson
Internet Society of New Zealand, Inc
Level 9
5-7 Willeston Street
WELLINGTON

Email: exe.dir@internetnz.net.nz ***By Email***

Dear Keith

UNSOLICITED ELECTRONIC MESSAGES BILL 2005

1. You have asked us to review and provide you with our comments on the Unsolicited Electronic Messages Bill (**Bill**) that was tabled in Parliament on 28 July 2005, to assist Internet Society of New Zealand Incorporated (**InternetNZ**) with its preparation of a submission to the Select Committee charged with considering the Bill once the Bill has had its first reading.

2. Based on our understanding of InternetNZ's views on spam and the need for legislation of some form to address its dissemination, we have not addressed in this letter the desirability of legislation in this area per se. Instead, we have focussed our analysis on whether the provisions of the Bill as drafted are likely to be an appropriate and effective means of achieving the Bill's stated purposes.

3. This letter is necessarily a report by exception and focuses primarily on areas of the Bill that could be improved. We have assumed that InternetNZ will otherwise generally support the passage of the Bill.

Overview of the Bill

4. **Bill derived from Australian Act:** The provisions of the Bill are clearly derived to a significant extent from the Australian Spam Act 2003 (**Australian Act**), and the form of the Bill will not be a great surprise to anyone who has read that Act and followed the consultation and other documents released by the Ministry of Economic Development during the policy process leading up to the Bill's drafting and introduction to Parliament.

5. **Key differences from the Australian Act:** The key differences between the Bill and the Australian Act are as follows:

5.1 **Scope of the Bill:** The Bill seeks to regulate two distinct classes of electronic message: *commercial electronic messages* (regulated on an *opt-in* basis) and *promotional electronic messages* (regulated on an *opt-out* basis), while the Australian Act deals only with the former category of messages.

5.2 **Responsibility for enforcement:** While the Bill creates a role for a government enforcement agency (to be carried out by the Department of Internal Affairs), the Bill differs from the Australian Act by placing considerable emphasis on telecommunications service providers (primarily Internet Service Providers (**ISPs**)) receiving, and taking action in response to, customer complaints.

6. **Broad overview:** Briefly, the Bill:

6.1 prohibits any person from sending, or causing to be sent, an unsolicited commercial electronic message with a New Zealand link (clause **9**) – see the discussion at paragraphs **10** to **12** below;

6.2 prohibits any person from sending, or causing to be sent, a promotional electronic message that has a New Zealand link to any person who has opted out of receiving messages from that sender (clause **10**) – see the discussion at paragraphs **13** to **15** below;

6.3 requires all commercial electronic messages and promotional electronic messages that have a New Zealand link to include accurate sender information identifying the person who authorised the sending of the message, how the recipient of the message can readily contact that person and any other information specified in regulations (clause **11**) – see the discussion at paragraph **10.4.1** below;

6.4 requires all commercial electronic messages and promotional electronic messages to contain a functional unsubscribe facility (clause **12**) - see the discussion at paragraphs **19** and **20**;

6.5 prohibits the supply, offer to supply, acquisition or use of address-harvesting software, a right to use address-harvesting software, a harvested-address list or a right to use a harvested-address list (clauses **15**, **16** and **17**) – see the discussion at paragraph **21** below;

6.6 provides that a *civil liability event* occurs where certain provisions of the Bill are breached, entitling:

6.6.1 affected persons and any person who suffers loss or damage as a result of a civil liability event to:

(a) make a complaint to the relevant service provider (only a service provider is entitled to complain to the enforcement department);

(b) seek an injunction from the High Court;

(c) or make an application to the High Court for compensation or to join any Court action initiated by the enforcement department;

6.6.2 a service provider to:

(a) make a complaint to the enforcement department;

(b) seek an injunction from the High Court;

(c) or make an application to the High Court for compensation or to join any Court action initiated by the enforcement department;

6.6.3 the enforcement department to:

(a) issue a formal warning;

(b) issue a contravention notice (bearing a proposed fine of $200);

(c) accept an enforceable undertaking;

(d) seek an injunction from the High Court;

(e) make an application to the High Court for a pecuniary penalty of up to $200,000 for an individual and $500,000 for an organisation in relation to the sending of a commercial electronic message, and $50,000 in relation to a promotional electronic message; and

(f) apply for a search warrant and exercise the powers of search and seizure granted by the warrant (clause **23**) – see the discussion at these enforcement provisions at paragraphs **22** and **23** below.

7. It will be clear from the summary above that the definition of key terms such as *commercial electronic message* and *promotional electronic message* are critical to the efficacy of the Bill's provisions.

Detailed comments

8. **Scope of the Bill:** The type of spam regulated by the Bill is, naturally, a central issue. While the Australian Act only prohibits unsolicited *commercial* electronic messages, the submissions received by the Ministry of Economic Development evidenced widespread support in New Zealand for legislation applying to unsolicited marketing and promotional messages irrespective of their nature.

9. The Bill represents something of a half-way house by restricting the distribution of both commercial and non-commercial messages. However, it regulates the two categories differently in terms of what constitutes consent to receipt of an electronic message and the severity of the pecuniary penalties that may be imposed for sending an electronic message in breach of the Bill's provisions. The Cabinet papers relating to the Bill record concerns that applying an *opt-in* procedure to all types of unsolicited messages would:

9.1 raise difficulties in terms of rights of freedom of speech;

9.2 create legal liability issues for the use of email as a general form of communication; and

9.3 impose widespread compliance costs on email users.

10. **Definition of *commercial electronic message*:** We have attached as a schedule to this letter a

complete copy of the Bill and it is important to pay particular attention to this definition given that it is central to the Bill's operation. Broadly however, a *commercial electronic message* is defined in clause **6** as an electronic message that has, as its primary purpose, the marketing or promotion of goods or services (as defined in the Fair Trading Act 1986), land or an interest in land, a business or investment opportunity, or assisting or enabling a person to dishonestly obtain a financial advantage or gain from another person. We have identified the following issues with the definition as currently worded:

10.1 Under the Bill a message is only a commercial electronic message if its *primary purpose* is the marketing or promotion of the various matters listed above. The obligation to establish the primary purpose of a message may make enforcing the prohibition on sending such messages in clause **9** of the Bill more difficult than its Australian counterpart (section **6** of the Australian Act requires only that the purpose, *or one of the purposes* of a message is the marketing or promotion of the various matters listed above). Further, whilst it is clear from the wording of the Australian Act that its test is *objective*, this is not clear in the New Zealand wording. What this means is that it may be possible for a defendant to avoid liability in two ways:

10.1.1 First, the defendant might raise a defence by objectively showing that the primary purpose was not commercial (in the senses set out in the Bill) (e.g., by showing that as a percentage of total content the commercial aspects were not significant); and

10.1.2 Secondly, since liability will need to be proved, the defendant might argue that it is for the enforcement body to prove, subjectively, that the defendant's primary purpose or intention was commercial. To do so, the enforcement body would need to adduce evidence of some sort of knowing intent or at least recklessness, which might be difficult.

10.2 In our view therefore, the wording should be changed to make it clear that the test is objective (i.e., what would a reasonable person consider was the purpose of the message). We assume that the *primary purpose* test was introduced for policy reasons, however, in our view, even if the test is objective, this will provide a significant means by which a spammer might avoid liability. One can imagine a spammer crafting the message in such a way as to make it very difficult to show that it was primarily commercial.

10.3 Clause **6(a)(ii)** of the Bill provides that a commercial electronic message includes a message that has as its primary purpose, assisting or enabling a person to obtain a financial advantage or gain from another person. The words *financial advantage or gain* are relatively narrow in comparison to dishonesty offences in the Crimes Act which refer to an intention to obtain *ownership or possession of, or control over, any property, or any privilege, service, pecuniary advantage, benefit, or valuable consideration* (see for example section **240** of the Crimes Act 1961 "obtaining by deception or causing loss by deception"). Accordingly, there may be situations where spam falls outside the definition of commercial electronic message because the person responsible for sending the message is seeking to dishonestly obtain some type of non-financial gain or advantage or to cause a loss. Acts such as unauthorised access to a computer system are now serious criminal offences under Part X of the Crimes Act 1961 and that Act already creates a number of offences relating to fraud and dishonesty, but we see no reason why the same definitions could not be used.

10.4 Clause **6** also excludes a number of types of electronic messages from the definition of commercial electronic message. The following exclusions merit comment:

10.4.1 Clause **6(b)(vii)** excludes from the definition of electronic commercial messages any message that provides information about goods or services offered or supplied by a government body or a court or tribunal. If such messages do not fall within the definition of promotional electronic messages (see paragraph **13** below) because they do not market or promote the organisation's aims or ideals, then those electronic messages will not be governed by the provisions of the Bill at all. While it is unlikely that New Zealand government bodies account for much (if any) of the current volume of spam distribution (although the current election campaign may belie that), it is difficult to see any reason for excluding government bodies from the Bill's requirements to include accurate sender information and a functional unsubscribe facility in electronic messages. (It should be noted that it appears that Australian government bodies are also so exempted under the Australian Act (see section **18(1)(b)**).

10.4.2 Clauses **6(b)(iii)**, **(iv)** and **(v)** exclude from the definition electronic commercial messages containing certain types of information. The drafting of the exceptions is not sufficiently precise and leaves room for an argument that, for example, the reference to warranty information in clause **6(b)(iii)** allows spam regarding additional or future warranty protection, rather than messages regarding an existing warranty. The types of relationship listed in clause **6(b)(iv)** should be qualified by the word *existing* (to remove any room for argument that spam regarding potential ongoing membership offers is permitted), and messages containing the types of information described in clause **6(b)(v)** should be limited to situations where the person sending the email is in some way connected to the employment relationship (unsolicited advertising messages from an employment lawyer may be directly related to the recipient's current employment relationship, while still constituting what most people would consider to be spam).

11. **Prohibition on sending *commercial electronic messages*:** Clause **9** contains a brief prohibition on the sending of unsolicited commercial electronic messages that have a New Zealand link. The term *New Zealand link* is broadly defined in clause **4(2)** and largely follows the equivalent term in the Australian Act (see section **7** of that Act). Clause **4(2)(f)**, however, goes further than the Australian Act and provides that there is a New Zealand link where a message is sent to an electronic address that ends with ".nz" or begins with an international access code directly followed by "64".

12. **Consent to receiving *commercial electronic messages*:**

12.1 A commercial electronic message is unsolicited if the recipient has not consented to receiving the message. *Consented to receiving* is further defined in clause **4** to:

12.1.1 include express consent; or

12.1.2 consent that can reasonably be inferred from the conduct and the business and other relationships of the persons concerned, or any other circumstances specified in regulations.

12.2 Consent is deemed to be given where:

12.2.1 an electronic address is conspicuously published by a person in a business or official capacity and the publication of an address is not accompanied by a statement to the effect that the relevant electronic address-holder does not want to receive unsolicited electronic messages at that address; and

12.2.2 the message sent to that address is relevant to the business, role, functions, or duties of the person in a business or official capacity.

12.3 The Bill's provisions dealing with consent again largely follow the provisions of the Australian Act (see Schedule **2** of that Act). While the provision for inferred consent is a sensible relaxation of a strict *opt-in* rule, providing for deemed consent to receipt of commercial electronic messages where an address is prominently displayed is potentially problematic, in that a presumption that unsolicited commercial messages are permitted in certain situations is contrary to the general purpose of the Bill. The Bill attempts to restrict this blanket consent by requiring that the message may only be sent if it is *relevant to the business, role, functions or duties of the person in a business or official capacity*. So, for example, a spammer could not take a recipient's address from a business website and then send them personal health related messages. However, whether a spammer could send to a lawyer's website email address messages promoting legal text books will depend on how the Courts interpret the *relevance* test. Of course the other way of avoiding the implication of inferred consent is to explicitly state that such messages are not to be sent (the electronic equivalent of a *no junk mail* notice on a letterbox).

13. **Definition of *promotional electronic messages*:** A promotional electronic message is defined in clause **4** as an electronic message that is not a commercial electronic message and has, as its primary purpose, the marketing or promotion of an organisation's aims or ideals. Again, there are the problems with the primary purpose/objective-subjective wording that we identified with respect to commercial electronic messages above. Also, the definition appears flawed in that it is limited to messages promoting an *organisation's* aims or ideals. Non-commercial spam promoting an individual's aims or ideals would not fall within this definition and, accordingly, would not be regulated by the provisions of the Bill. This should be changed. Finally, as with any definition, unless one endeavours exhaustive cover (which is often impossible and creates inflexibility in terms of future developments), the definition will be open to different interpretations. A topical example of this is to take some of the current messages issued by Government departments. These of course fall outside the definition of commercial electronic message by virtue of the exception in clause **6(b)(vii)**. Whether they also fall outside the definition of promotional electronic message may well depend on one's perception of the extent to which the message simply conveys information rather than promotes ideals. As has been found with election hoardings and advertising, this is often a very fine line.

14. **Prohibition on sending promotional electronic messages:** Clause **10** prohibits the sending of a promotional electronic message to a person who has opted out of receiving messages from the sender. The clause requires that a person must first receive at least one message from a sender and then send, deliver or give to the sender a message to the effect that he or she does not want to receive, at that address, any further promotional electronic messages from or authorised by the sender.

15. ***Opt-out* procedure:** The use of an *opt-out* procedure in relation to promotional electronic

messages set out in clause **10** will give rise to the same issues that are inherent in any *opt-out* procedure, including that:

15.1 a sender has one *free hit* at any email address;

15.2 a reply email to give an *opt-out* notice may or may not hit a valid address;

15.3 sending an *opt-out* notice will confirm to the sender that the spammed address is valid; and

15.4 allowing some unsolicited electronic messages to be sent (albeit subject to an *opt-out* procedure) creates a "legitimate" purpose for address-harvesting software that, in practice, is likely to make the enforcement of the prohibitions in the Bill more difficult (see the discussion of the address-harvesting provisions at paragraph **21** below).

16. Arguably having an *opt-out* procedure for promotional electronic messages undermines much of the benefit that might have been obtained by regulating promotional electronic messages under the Bill. While there are fewer non-commercial messages and, accordingly such messages are less of a drain on resources and recipients' time, receiving an unsolicited non-commercial electronic message is arguably just as objectionable in and of itself as receiving an unsolicited commercial message. We suspect however that any attempt to further restrict promotional messages will not be successful given the policy balance which appears to have been drawn and the fact that the Australian Act does not regulate them at all.

17. Another significant limitation on the effectiveness of the *opt-out* provisions is that clause **12(2)** of the Bill provides that the *opt-out* provisions do not apply to the extent to which they are inconsistent with the terms of a contract, arrangement, or understanding between the sender and recipient, effectively enabling "contracting out" of the *opt-out* provisions.

18. A minor point to note is that an *opt-out* message generally takes effect at the end of a period of 5 working days from the day on which the message was sent (depending on the method of sending the *opt-out* notice) (clause **10(3)**). The period appears to have been taken from clause **6** of Schedule **2** of the Australian Act, which deals with the withdrawal of a consent previously given under the opt-in provisions. Arguably a shorter period is appropriate for an *opt-out* notice than for the withdrawal of a consent.

19. **Functional unsubscribe facility:** Clause **12** of the Bill prohibits the sending of either a *commercial electronic message* or a *promotional electronic message* without including a functional unsubscribe facility that the recipient may use to instruct the person who is authorised that message to be sent that the recipient does not want to receive further messages from the sender at that address.

20. Clause **12** of the Bill is based on clause **18** of the Australian Act, but omits the requirement in the Australian provision that messages include *a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message.* Instead, clause **12** remains silent on the form of the unsubscribe facility (although the form of any unsubscribe facility may be prescribed by regulation). It would be unsatisfactory if (for example) an 0900 number could constitute a *functional unsubscribe facility*, forcing recipients of spam to go to the expense of utilising such a facility in order to unsubscribe.

21. **Address-harvesting:**

21.1 The Bill contains prohibitions on the supply, offer to supply, acquisition or use of

address-harvesting software, a right to use address-harvesting software, a harvested-address list or a right to use a harvested-address list (clauses **15**, **16** and **17**). However, none of those clauses apply to a person who had no reason to suspect that the customer or another person, intended to use the address-harvested software or harvested-address list, in connection with the sending of unsolicited electronic messages in breach of clauses **9** and **10** of the Bill.

21.2 The term *address-harvesting software* is defined broadly in clause **4** as software that is capable of, or marketed for use for, searching the Internet for electronic addresses and collecting, compiling, capturing or otherwise harvesting those electronic addresses. In contrast, the Australian Act applies more narrowly to software *specifically designed or marketed for* address-harvesting. The focus on the capability of software in the clause **4** definition is likely to capture a range of innocuous software, such as Internet search engines that, while having a legitimate use, could also be said to capable of searching the Internet for electronic addresses and compiling those addresses. Notwithstanding the proposed defence discussed at paragraph **21.4** below, the more narrowly focused Australian provision appears to be a better option for this reason.

21.3 By allowing certain unsolicited messages to be sent (e.g. *promotional electronic messages* and messages sent by government bodies), the Bill permits legitimate uses for address-harvesting software and, accordingly, makes it easier for a person to rely on the defence that they had no reason to suspect that the software would be used for an improper purpose.

21.4 The address-harvesting restrictions apply only where both parties to an offer, or supply, or the person using the address-harvesting software or harvested-address list, are either an individual who is physically present in New Zealand or an organisation carrying on business or activities in New Zealand at the relevant time (clause **14(1)**). A defence is provided for a supplier who did not know, or could not with reasonable diligence have ascertained that the customer was in New Zealand (clause **15(3)**). These restrictions appear to have the odd result that the Bill will not be contravened by, for example, the sale of harvested-address lists to overseas entities, even if the addresses are New Zealand addresses.

22. Enforcement:

22.1 A fundamental issuein the Bill is that only service providers may make a complaint to the enforcement body. Individual recipients may only make a complaint to their service provider or apply to the High Court for the various remedies described above. Naturally, the cost of an application to the High Court will almost always be uneconomic for an individual recipient of spam so granting that right seems somewhat unrealistic. The policy rationale set out in the Cabinet papers for involving service providers in the enforcement of the Bill's provisions is both that the government is reluctant to bear the cost of enforcement and that service providers have access to technological measures to assist them and an incentive to reduce spam volume. Given that a spammer will almost always impact on multiple people in New Zealand at the same time, we consider that there are legitimate public interest arguments that would support enforcement being resourced out of the consolidated fund rather than by individuals.

22.2 Further, even though the implication is that service providers are expected to be at the forefront of enforcement activity, from a user's perspective, there is no right given to

force the service provider to do anything and nor is there any explicit obligation on the service provider to take action in relation to a complaint. Clause **24** provides only that a service provider must *consider* a complaint and have regard to any relevant, generally accepted industry code that applies to the service provider.

22.3 The level of the pecuniary penalties that may be awarded by the High Court on the application of the enforcement department are substantial: up to $200,000 for an individual and $500,000 for an organisation in relation to the sending of a *commercial electronic message*, and $50,000 in relation to a *promotional electronic message*. However, in practice the efficacy of the pecuniary penalties as a deterrent will depend on the resources and willingness of the enforcement agency to take proceedings through the High Court.

22.4 The Cabinet paper dealing with enforcement issues provides that $200 is proposed as the fine that will be payable on the issue of a contravention notice, which appears to be too insignificant an amount to act as any sort of deterrent. Under clause **28(2)**, contravention notices may only be delivered or posted, requiring that the physical location of the offender is known. More significantly, where a penalty is paid under a contravention notice, *any liability* of the person for the alleged civil liability events to which the contravention notice relates is discharged (clause **32**). The provision appears not to be limited to liability arising under the Bill and could result in recipients of an unsolicited messages being left without recourse against a spammer, even though the recipients have suffered damage or loss as a result of unsolicited electronic messages, simply because the spammer had paid a $200 fine.

22.5 The workability of any enforcement regime will be critical to the effectiveness of the Bill, and we have serious reservations regarding the practicality of placing the burden of enforcement on service providers in the manner proposed in the Bill. We note that the Australian Act establishes a government regulatory agency as the primary enforcement body, and consider that the creation of a small, well-funded government agency along the lines of that created by the Australian Act would provide a much more effective enforcement regime.

23. Extra-territoriality

23.1 The Bill purports to have extraterritorial application. It follows the Australian Act in stating that the prohibitions under clauses **9** and **10** the Bill apply to electronic messages with a New Zealand link. The extent to which the Bill purports to have territorial effect is, however, more limited than the Australian Act. Clause **8** of the Bill provides that the Bill only applies to conduct outside New Zealand if that conduct is engaged in by a relevant person (compare section **14** of the Australian Act). *Relevant person* means an individual who is resident in New Zealand or an organisation that carries on business or activities in New Zealand. Presumably the narrow extraterritorial application has been chosen because of the considerable practical difficulties inherent in endeavouring to take any enforcement action in relation to a person not physically present in New Zealand.

23.2 Whether the narrow extraterritorial scope of the Bill will have any effect in practice at the present time is doubtful, as the Bill's primary sanction is the imposition of pecuniary penalties. Generally, the courts of one jurisdiction will not enforce a foreign judgement if to do so would involve enforcing the payment of taxes or a fine or other penalty

imposed by the foreign jurisdiction.[1]

23.3 However, the narrow extraterritorial scope of the Bill will limit the ability to take action, or to seek assistance from another country, in relation to spam sent by persons who are not resident in New Zealand. It also precludes the ability to take advantage of any future developments in relation to the enforcement of judgments. For example, a joint Australia/New Zealand working group, established to review trans-Tasman co-operation in court proceedings has recently recommended that certain criminal fines under a specified list of statutes should be enforceable in the other country.[2] Arguably, the extra-territorial scope of the Act should be broadened (there does not appear to be any real disadvantage to doing so) and the Bill should be included in the list of statutes in any legislation enabling fines to be enforced in Australia.

Yours faithfully
LOWNDES JORDAN

Rick Shera / Greg France
Partner / Solicitor

[1] For example, judgments where taxes or other charges of a like nature or in respect of a fine or other penalty are payable are not enforceable under New Zealand's Reciprocal Enforcement of Judgments Act 1934.

[2] A copy of the report is available at http://www.justice.govt.nz/pubs/reports/2005/trans-tasman-court-proceedings-and regulatory-enforcement/part1.html#101