

InternetNZ's reaction to the MED discussion paper on Spam

InternetNZ, the Internet Society of New Zealand, representing Internet users and providers, seeks to promote and protect the Internet in New Zealand.

This is a formal submission to the NZ Government in response to the discussion paper "Legislating against spam" published by the IT and Telecommunications Policy Group of the Resources and Network Branch of the Ministry of Economic Development.

1: Do you consider spam to be an important issue? Has it significantly affected you in any way?

Yes. In all honesty, it's hard to see that any elaboration is required to support this monosyllabic response, but some simple statistics might be apposite: more than 64% of all e-mail crossing the Internet is now spam (*source: Brightmail*) and the EU Directorate prepared a report last year estimating that the annual global cost of dealing with spam was in excess of 12 billion Euros. E-mail developers are now reporting that more than 90% of the connections made to mail servers are spurious in one form or another, and even if effective filtering reduces the overall quantity of spam reaching the end user, this is merely a movement of the burden, not a solution to the problem.

Spam has markedly decreased the reliability of e-mail (through false-positive spam detection and anti-spam measures that misfire), and has introduced significant extra expenditure of time by all users of e-mail, at more or less any level. Its significance cannot be disputed and should not be underestimated.

2: Do you think legislation has a role to play alongside other complementary measures?

Emphatically yes. Six years of incessant spam levels spiraling upwards out of control have shown that technical solutions on their own cannot fix the problem. InternetNZ believes strongly that legislation provides both a proper moral underpinning for dealing with spam (the law being the social vehicle by which particular behaviours are formally classified as unacceptable), and a means of dealing with the most serious offenders. It is our view that effective, properly-enforced legislation is one of the four key pillars of a workable anti-spam solution, the others being education, industry self-regulation, and the development of technical counter-measures.

It is also very important that New Zealand puts in place legislative measures alongside those of other countries so that spammers do not engage in "regulatory arbitrage" by moving from countries where their actions would be subject to sanction, to New Zealand where they would not.

3: Do you consider existing legal protections in this area sufficient?

No – in support of this, consider the case in 2003 of Shane Atkinson, a spammer discovered pushing “Penile enlargement pills” from his base in Christchurch. Although he was clearly breaching a number of existing laws (including fraudulent or misleading advertising and peddling an unlicensed remedy) formal complaints by InternetNZ to the Commerce Commission and Medsafe (a section of the Ministry of Health) led to a flurry of finger-pointing and buck-passing. No action was ever taken against Mr Atkinson, and we have received reports that suggest he may still be operating, albeit in a less conspicuous manner.

4: Do you believe that stand-alone anti-spam legislation is preferable to reliance on the Harassment Act?

InternetNZ believes that the Harassment act is unlikely to be a viable way of handling spam, because the formal definition of harassment involves a deliberate repeated behaviour directed against a particular person. Spam, being inherently indiscriminate, is unlikely to be considered “harassment” using the definitions in the Act.

The adoption of formal stand-alone anti-spam legislation allows the problem to be defined clearly and accurately: it also allows resources to be properly targeted to address the specific issue, rather than being lost in a swirl of more general priorities.

5: What message mediums should be caught by the legislation?

InternetNZ believes that spam is an electronic-age problem, and that legislation should therefore be limited to electronic media. One of the primary differences between spam and other types of unwanted promotional material (such as postal deliveries), is that with spam, it is the recipient who typically bears the cost of delivery. We believe that this could form part of the determination of which types of media should be covered by legislation. Given the rate of change prevalent in the electronic frontier these days, we also believe it would be appropriate to cast the wording of the act to allow particular electronic media to be specified by order in council as required.

6: Do the messages caught by the legislation have to be sent/conveyed to many recipients, and if so, how many?

This is the crux of the difference between the UCE Camp (Unsolicited Commercial E-mail) and the UBE Camp (Unsolicited Bulk E-mail). It is InternetNZ’s belief that attempting to define legislation based on specific numbers of messages would create ambiguities (for instance, if two messages are identical except for the recipient’s address, would they be deemed “the same”?) and difficulties in establishing a burden of proof. We contend that the real issue in spam is neither the quantity nor the content, but rather the issue of whether or not consent has been given by the recipient to receive the message. While it will clearly be necessary to add a layer of

definition above the issue of consent, we do not believe that basing a definition of spam on specific numbers of messages will produce effective legislation.

At the recent spam legislative issues workshop, there was overwhelming support by participants for focusing on consent instead of quantity.

InternetNZ also believes that the quantity of spam sent should be a key factor in determining what action is taken by an enforcement agency (warning vs prosecution for example), but that setting a legislative level would be unhelpful. Instead, it may be preferable to indicate a series of guidelines but leave the question of actual enforcement levels to the discretion to the agency itself.

7: Should the messages caught by the legislation be of a commercial/promotional nature only, or should other types of message be caught?

The process of defining exactly what “spam” is has proven notoriously elusive (see *Harris: Spam White Paper* for elaboration on this). Since it is clearly nonsensical to create a definition of spam based solely on the fact that a message is unsolicited, some “higher level” of definition has to be applied to solidify the exact intent of the legislation. There are arguments for using wider definitions than “commercial/promotional”, but at a practical level, we note that if all spam currently matching such a definition were removed from circulation, there would be very little spam left over. We therefore suggest that the idea of “unsolicited messages of a commercial/promotional nature” represents a good starting point for legislation, and that once again it may be appropriate to consider leaving room for more specific definitions to be determined by order in council.

7b: Should there be exceptions, and if so, what should be exempted?

According to Andrew Maurer, from NOIE, the issue of exemptions and exclusions was a major stumbling point during the framing of the Australian legislation.

This issue was discussed vigorously at the spam legislative options workshop and there was no support for having exemptions for charities or political parties/MPs.

We note that a focus on commercial/promotional is likely to exclude many messages from such groups anyway.

8: Should the legislation extend to coverage of acts done overseas?

Yes. It is InternetNZ’s belief that anti-spam legislation will only become genuinely effective when a significant level of international co-operation is possible. Because geographical details are largely immaterial where the Internet is concerned, a spammer’s activities may span several jurisdictions. Assuming that some form of international treaty is a likely long-term outcome of anti-spam activities, having

legislation that covers acts committed outside New Zealand will likely prove worthwhile in the future.

We note however that international co-operation may be hampered by the introduction of the Telecommunications Information Privacy Code Amendment 3, which will remove an exception currently provided in the code. That exception essentially allows personal information, disclosure of which would otherwise be prohibited under the Privacy Act, to be released to assist in prosecution of overseas telecommunications laws. If the exception is removed as currently seems to be proposed, whichever New Zealand authority is charged with policing the new legislation will be unable to share personal information about the spammer or his/her targets with fellow overseas enforcement agencies. This may both make it difficult to enhance co-operation and may also make it more difficult to bring a prosecution against a New Zealand spammer since the collection of evidence may be impeded.

Therefore, either legislatively or by a further amendment to the code by the Privacy Commissioner, the exception for overseas telecommunications laws should be re-introduced.

9: Should all parties involved in the act of spamming, such as the vendor sponsoring the spamming, be covered by the legislation?

The primary targets of legislation should be the vendor and anyone undertaking the explicit task of distributing spam on his behalf. We believe that it should not be a defense for a vendor to claim that he did not realize that his agent would be using spam as a means of disseminating the vendor's material unless they can prove that they instructed said distributors not to spam and did not reward them for spamming: it should be the vendor's obligation to ensure that ethical and legal means are being employed on his behalf, just as it would be in any other area of his business endeavours.

9b: Should there be express exceptions, such as for Telecommunications Companies and ISPs?

InternetNZ believes strongly that those who simply provide bandwidth and are not aware of the exact nature of the content passing through their channels should be specifically excluded from liability under the legislation. We do believe, however, that this exemption should not extend to ISPs or Telecommunications providers who knowingly offer their services to spammers (that is, so-called "spam-friendly ISPs").

InternetNZ notes that almost all New Zealand Internet Providers do not allow spamming, and it is incredibly rare for there to be a major spam attack through a local Internet provider. InternetNZ will encourage ISPs to retain anti spam clauses in their acceptable use policies as a good example of industry self regulation.

10: Should New Zealand adopt an opt-in, double opt-in or opt-out approach in legislating against spam?

InternetNZ believes emphatically that only an opt-in model is suitable for anti-spam legislation, and that mandating opt-in would not create unreasonable compliance difficulties for existing operations. Double opt-in, while generally regarded as a “best practice” in the industry, cannot, we believe, be legislated as a primary requirement because its demands are too onerous for many existing operations. We are convinced that opt-out is totally unsuitable as a basis for legislation because it creates too great a burden for the recipient, who is obliged to opt-out any time he receives unwanted material. To illustrate what we mean by this, consider the case of an individual receiving in excess of 500 spam messages a day: estimating that it can take a minute to opt out of each message, an opt-out regime could require a person to spend eight hours a day doing nothing but opting out.

It is worth emphasizing that many of the difficulties of defining spam are greatly ameliorated by adopting opt-in as the basis for legislation: since true spam is by definition unsolicited, adopting an opt-in model immediately makes all true spam illegal. We contend that the problems created by opt-in (namely, defining express consent and the nature of pre-existing business relationships) are considerably less severe and intractable than the problems created by an opt-out model, where the burdens are borne entirely by the innocent end-user.

11: In an opt-in environment, what should amount to express consent, and what actions and/or relationships should amount to inferred consent to the sending of a “commercial” electronic message?

A number of standard conventions exist for express consent on the Internet – the most common is a checkbox on any page where an e-mail address is requested: if the checkbox is checked when the form is submitted, then the user has given express consent. Problems arise over the intended scope of that consent (see below), and the issue of whether or not the checkbox should be pre-checked is quite contentious.

Conventions notwithstanding, the issue of consent is likely to be the most difficult part of any effective anti-spam legislation, as much because of human nature and forgetfulness as anything else: even with existing opt-in mailing lists, people often forget that they have subscribed to a list and later complain when they receive mail from it.

We believe that the key to having legislation that will provide a workable solution is to use wording that emphasizes two key points:

- That the sender should have “reasonable grounds” for believing that a recipient has given consent: this prevents a sender for being liable in the event that someone “spoofs” another person’s e-mail address during a subscription, and covers a number of other “human weakness” situations where a sender might actually be blameless, despite the recipient’s perceptions.
- That the sender must provide a working, clearly visible means of opting out of future mailings, even where the recipient has given explicit consent. This normally

takes the form of a clickable link in the message, or perhaps also an automated mailing address to which the recipient can send a message. At a minimum the opt out mechanism should be accessible through the same medium as the message itself.

If “reasonable grounds” and “opt-out on request” are both stated clearly in the legislation, we believe that many of the more vexing issues of express and inferred consent can be reduced to more manageable issues of good faith and common sense. A sender who claims “reasonable grounds” as a defense, but against whom there is a disproportionate number of complaints can be reasonably assumed to be pushing or fracturing the limits of the law, so the mechanism becomes self-regulated.

12: How should the scope of any opt-in assent be framed?

Express or inferred consent should be for one specific purpose only. It should not be possible for a sender to sell a list of addresses to another sender claiming that the recipients have all given assent unless the possibility of that action was clearly and unambiguously stated when the assent was given. Finer gradations of scope (for instance, whether giving assent to receive information about one type of product from a vendor should be construed as assent to receive information about other products from the same vendor) are more complex. We do, however, believe that some of the complexity may be adequately covered by the Privacy Act, and its key principle that information should be used only for the purpose it was given.

13: Should there be a requirement for commercial electronic messages to accurately identify the sender of the message? If so, what constitutes accurate identification?

We believe this is a crucial issue. One of the primary distinguishing factors between “true spam” and genuine commercial mailings is the fact that true spam almost never accurately identifies the sender, therefore having this as a requirement will provide a major “catch point” for trapping true spam. We maintain that accurate identification need be nothing more than a valid “friendly name” in the address field, accompanied by a functioning e-mail address that is legitimately usable by the sender. By “valid friendly name”, we mean that the name appearing in the “From” column of the recipient’s mail client should reasonably represent the true identity of the person or entity sending the message. We do not believe that it is necessary to require physical addresses in electronic media.

14: Should there be a requirement for commercial electronic messages to include a statement to the effect that the recipient may use an electronic address set out in the message to send an “unsubscribe” message to the sender, and to ensure (require) that such electronic addresses be functional?

Yes. Any true, legitimate commercial/promotional message must include an opt-out link. (see our comments to section 11, above). We also believe that any such opt-out mechanism **must** be usable at no charge to the recipient (other than incidental or

unrelated costs, such as the normal cost of using the Internet via the recipient's connection to his or her ISP). If it were possible for senders to levy a charge for processing an unsubscribe request, we are sure that there are those who would exploit that loophole as a way of making money. Note that, as discussed in section 11 above, an unsubscribe mechanism need not only be an e-mail address, but can be a website link (which is often quicker and easier to use).

15: Should there be a requirement that commercial electronic messages provide accurate header and subject information?

We feel that "accurate header information" may end up being unacceptably ambiguous, especially since many users do not have full control over all the mail transit servers between them and the recipient (so, if a server not under the control of the sender added an inaccurate header to the message while it was in transit, would the sender be liable for this?). We do, however, feel that it should be a requirement that the subject line of the message should accurately reflect the content of the message: you should never find yourself in the position of opening a message whose subject is "You forgot your umbrella", only to find that it is an advertisement for Viagra. InternetNZ believes that more appropriate wording for this requirement is that "the header and subject information should not be misleading or deceptive" (in line with existing concepts that are well understood under the Fair Trading Act 1986).

It was highlighted during the spam legislative options workshop, that sometimes a header may be altered for what most would accept as a legitimate reason. The example given was an ISP warning its customers of a virus attack, and changing the time on the e-mails so they will appear in people's inboxes (and hopefully be read) prior to the virus infected messages.

16: Should there be a requirement for the labeling of advertising or adult messages?

In an opt-out environment, labeling of advertising messages may be useful, but we believe it achieves nothing in an opt-in environment. There may, however, be a case for requiring the labeling of adult messages even in an opt-in environment: our rationale for this is that in many households, a mailbox may be shared between several users, potentially including children; adult labeling may simplify the process of protecting children from messages that have been legitimately sent but are inappropriate for some recipients.

17: Should anti-spam legislation include rules against the supply, acquisition and use of address-harvesting software and harvested address lists in connection with the unlawful sending of electronic messages?

Yes – we believe that as worded, this paragraph nicely summarizes the situations where address-harvesting tools should be restricted or outlawed. We believe that address harvesting software may have perfectly legitimate uses, but in conjunction with the sending of spam, its use should always be proscribed.

18: Who should be able to bring an action against the spammer?

InternetNZ believes the Crown and legitimate ISPs should be able to initiate action under the legislation, but the potential of vexatious litigation is too great to consider allowing the public to take action. We believe that the public should be able to petition the Crown's designated agent to take action, and equally that if enough of an ISP's customers complain about spam, then the ISP may well consider initiating an action as well: this should be enough to allow reasonable enforcement latitude. The rationale for allowing ISPs to take action is so they can claim damages (payable to them) for costs incurred by spam from a particular organization or individual.

There is however concern from some ISPs that a provision which allows them to sue, may result in pressure from customers to take potentially costly legal action. We recommend specific consultation be undertaken with ISPs to see if they wish to have the right to initiate legal action.

19: What agency should have the enforcement role under the legislation?

The primary candidates for this role amongst existing agencies would appear to be the Department of Internal Affairs or the Commerce Commission, but whichever agency is designated, we urge that:

- It be given explicitly targeted resourcing through its purchase agreement with the Minister, to ensure that enforcement actually occurs. The whole process of establishing anti-spam legislation is completely without purpose if the agency tasked with enforcing it does not do so.
- It be specifically tasked and resourced to initiate actions against spammers who are only in breach of the anti-spam act. We believe that given a choice between pursuing someone who has committed fraud or another criminal act, and someone who has simply breached the anti-spam act in the process of selling an otherwise legitimate product, most agencies will instinctively favour the criminal act. In an environment where resourcing or manpower is tight, this may result in action never actually being taken against spammers unless specific direction and resourcing is targeted towards that task.

InternetNZ has considered the merits of half a dozen existing agencies, and believes the Department of Internal Affairs or the Commerce Commission are the best fits. We do not take a strong stance on promoting one particular agency for taking on the enforcement role, but we note the Department of Internal Affairs already engages in a large degree of international co-operation in pursuit of traders in objectionable material under the Films, Videos and Publications Classification Act. Whilst spam does not necessarily contain such content, it can on occasion, and is also likely to lead to similar exchanges in its own right. Therefore, there would seem to be some synergy to be obtained in having Internal Affairs funded and tasked with this additional responsibility. This would take advantage of the international links with other enforcement agencies that they have already established and also recognize that there may be some overlap between the two regimes in terms of enforcement.

A suggestion was made at the spam legislative options workshop, that consideration be given to setting up an industry agency (similar to the Advertising Standards Authority) funded by the Crown to handle the investigations, education, codes of practice and warnings under any Act, with an existing crown agency receiving and deciding upon any occasional recommendations for prosecutions or search warrants.

InternetNZ believes this idea has some merit, and is worthy of further consideration. The two main benefits would appear to be greater acceptability by stakeholders, especially legitimate businesses concerned with potentially heavy handed enforcement, and arguably better value for money as industry expertise would be more easily available.

InternetNZ plans to consult with other industry groups about the pros and cons of such an approach. If there is widespread support, we will investigate specific models to be put to the Government for consideration. Groups which could be part of any industry agency include the Direct Marketing Association, Business NZ, Retailers Federation, InternetNZ, Telecommunication Carriers Forum, and the Consumer's Institute

20: What should be the available penalties and remedies for breaches of anti-spam legislation, and what should be the maximum fine or pecuniary penalty?

We note that the Australian legislation specifies a fine of up to AU\$220,000 per day, to a maximum of AU\$1.1 million – these figures may provide a guideline for the type of penalties that could be applied here. Whatever penalties are chosen, however, must act as a disincentive to spam, remembering that spam can be quite lucrative. A maximum fine of NZ\$250,000 is unlikely to be significantly effective if a spammer can accrue NZ\$500,000 from a spam run. For this reason, there may be a value in having a provision for escalating fines for repeat offending.

The United States legislation allows for penalties up to twice the value of any proceeds from spamming. This approach has merit as ultimately any penalties must be potentially larger than profits from spamming activity, otherwise it will not be an effective deterrent.

21: Should contraventions give rise to criminal or civil penalties?

We believe that civil penalties, with their somewhat lower burden of proof, are probably adequate for dealing with spam. In the event that a spam was also fraudulent, there are existing acts that could be used to apply criminal sanctions in particularly egregious cases.

22: Should the responsible enforcement agency be given the ability to obtain search warrants conferring powers of entry, search and seizure?

Yes. It is our belief that a significant portion of the value of anti-spam legislation in a country like New Zealand will arise from the extent to which it can facilitate international co-operation with other enforcement agencies. For this reason, we

believe it is important that the enforcement agency be given the powers necessary to enable such co-operation.