

## **Submissions on Government Discussion Paper Legislating against Spam**

*These comments are made solely in my personal capacity and are not intended nor should they be taken as any view on behalf of the judiciary relating to this subject*

### **1. Introduction**

It is quite clear that spam is a significant problem which has implications for the utilisation of bandwidth together with increasing costs users in a number of different ways.

Spam has become a fact of life. At least 33 percent of my e-mail traffic is spam. I have had to undertake steps to minimise the risk of receiving objectionable or unwanted content by utilising pre-download software solutions.

It is my view that legislation is necessary to deal with certain spam issues. The legislation should be limited to addressing the particular problem and should be no wider than that.

### **2. Definitional and Jurisdictional Issues**

Two important issues are:

- (a) The definition of spam;
- (b) How wide that definition should be so that it does not infringe upon the provisions of s.14 of the New Zealand Bill of Rights Act 1990 which states:

“Everyone has the right to freedom of expression including the freedom to seek, receive and impart information and opinions of any kind in any form.”

Any definition of spam will need to be cast so as to avoid infringement of freedom of expression or interfere with that freedom in the most minimal way.

It is to be noted that legislation will be of limited effect in that it can only be directed towards spam distributors in New Zealand (subject to certain extra-territorial issues which will be referred to later). In the interest of international co-operation it is advisable for legislation to reflect common approaches adopted across jurisdictions to harmonise the legislative approach.

### **3. Existing legal framework**

It is agreed that the Privacy Act 1993 goes some considerable distance towards dealing with the issue of address harvesting without the consent or knowledge of the user. Once again, the Privacy Act is of limited utility in that it is domestic legislation without extra-territorial impact.

#### **3.1 Harassment Act**

Any suggestion that the civil harassment regime under the Harassment Act 1997 potentially covers acts of spamming is without foundation. A detailed consideration of the Harassment Act and online harassment, together with the ingredients of harassment, may be found in Harvey, *internet.law.nz* paragraph 4.7.2 (page 230) and following. It is necessary for there to be a pattern of behaviour directed against a particular person, including doing a specified act to that person on at least two separate occasions within a period of 12 months.

Harassment is divided into civil harassment and criminal harassment. Criminal harassment is that harassment that causes another person to fear for their safety or for the safety of any other person with whom that person is in a family relationship. There is also, pursuant to s.8(1)(b) of the Harassment Act, a form of harassment by proxy.

The specified act defined in s.4 is primarily directed to real world activity although it may cover making contact with the harassed person whether by telephone, correspondence **or in any other way**. The person who is harassed must fear for their safety or the safety of a person with whom they are in a family relationship.

A restraining order may be made for civil harassment if:

- (a) Harassment has been established; and
- (b) The harassing behaviour causes distress or threatens to cause the applicant distress and that behaviour would cause distress or would threaten to cause distress to a reasonable person in the applicant's circumstances and in all the circumstances the degree of distress caused or threatened by that behaviour justifies the making of the order and the making of the order is necessary to protect the applicant from further harassment.

The issue of civil harassment is not covered in the discussion paper and the discussion of harassment that appears seems to be more directed towards criminal sanction. My experience is that spam is rarely threatening and is normally annoying but it would be difficult to establish that in fact it causes distress. Clearly, the Harassment Act does not deal with spam issues and separate legislation is required.

### 3.2 Civil Remedies

The discussion paper fails to address other potential remedies that may be available. The following information is submitted so that, when casting legislation, only areas where existing law is inapplicable may be addressed. Legislation should not create remedies for problems for which there are existing common law or alternative solutions.

### 3.3 Contract

Spammers must have access to the internet that will normally require a contract for ongoing or temporary services of an ISP. Many ISPs insert a standard provision, which is an acknowledgement that spamming is regarded as a fundamental breach allowing the contract to be terminated unilaterally by the ISP at any time. It is suggested by Edwards<sup>1</sup> that where there is

---

<sup>1</sup> Lillian Edwards "Canning the Spam: Is There a Case for Legal Control of Junk Electronic Mail" [www.law.ed.ac.uk/Script/spam.htm](http://www.law.ed.ac.uk/Script/spam.htm) (last accessed 20 December 2002)

no express anti-spam clause it is possible that Courts would be prepared to accept it as a term implied by the common practice of business involving internet access provision.

In the US, many ISP contracts have in place a system of rising penalties for repeated spamming that may be imposed instead of termination of the contract. The problem arises in the New Zealand and UK common law jurisdiction that such clauses may amount to penalty rather than true damages clauses and may be struck down.<sup>2</sup>

### 3.4 Tort Remedies Overseas

The tort of trespass has been used in the US in *Earthlink Networks v Cyber Promotions*. In this case it was established that intentional damage was done to the moveable property of the service provider,<sup>3</sup> and the ISP achieved a US\$2 million settlement against a spammer.<sup>4</sup>

In *CompuServe Inc v Cyberpromotions Inc*<sup>5</sup> the defendants sent unsolicited email advertisements to hundreds of thousands of internet users, many of whom were subscribers to the plaintiffs' service. The plaintiffs advised the defendants to stop, advising them that they were prohibited from using the plaintiffs' equipment to store and send unsolicited email. The Court held that electronic signals generated and sent by a computer were sufficiently tangible to support a trespass claim<sup>6</sup> and that, as a result of this conduct, the value of the equipment used by CompuServe was diminished.

In *America Online Inc v IMS*<sup>7</sup> it was alleged that the defendant sent 60 million unauthorised bulk emails through the plaintiff's system and continued to do so after being asked to stop. AOL had to spend time setting up systems to counteract the defendant's activities, and this had resulted in complaints from 50,000 AOL subscribers. The Court referred to *CompuServe v Cyberpromotions* and observed that although there was no physical damage, there was a reduction in value of the plaintiff's equipment, together with an injury to its business goodwill and the value of its possessory interest in its network.

A similar situation provided the factual background in *America Online Inc v Prime Data Systems*.<sup>8</sup> The matter proceeded on an undefended basis because the defendants failed to appear at the hearing. The Court referred to the decision in *AOL v IMS* as authority for the proposition that the defendants' acts constituted trespass to chattels without any further analysis.

---

<sup>2</sup> *Dunlop Pneumatic Tyre Co v New Garage and Motor Co* [1915] AC 79.

<sup>3</sup> BC 167502 (Cal Super Ct Law County, 30 March 1998).

<sup>4</sup> See also *AOL Inc v IMS* (1998) US Dist Lexis 17437; *CompuServe Inc v Cyber Promotions* 962 F Supp 1015; US Dist LEXIS 1997 in which CompuServe server's performance was so degraded that email took three days to deliver which normally would have taken minutes. The damage caused by electronic signals could be sufficiently tangible to found the tort. Damage caused to the plaintiff's property did not need to be permanent so long as it had resulted in actual impairment of its quality and value. CompuServe had not given any permission to any use at all that the spammers made of internet access.

<sup>5</sup> 962 F Supp 1015; US Dist LEXIS 1997.

<sup>6</sup> Citing in support *Thrifty-Tel Inc v Bezenek*, 46 Cal App 4th 1559, 1567 (1996); *State v McGraw* 480 NE 2d 552, 554 (Ind 1985) where it was posited that a hacker's unauthorised access to a computer was more in the nature of a trespass than a criminal conversion.

<sup>7</sup> 24 F Supp 2d 548; US Dist LEXIS 17437.

<sup>8</sup> 1998 US Dist LEXIS 20226.

The Canadian case of *Ontario Inc and Codes Communications Inc v NEXX Online Inc*<sup>9</sup> involved a different factual scenario in terms of the nature of the relationship between plaintiff and defendant. In this case the ISP was the defendant. The plaintiff was a commercial business and a subscriber to the defendant's services. In subscribing, the plaintiff agreed that it would abide by generally-accepted "netiquette". To complicate matters the defendant had an agreement with a company named Exodus Communications Inc who provided internet services to the defendants. It was a specific condition of the agreement between Nexx and Exodus that Nexx was prohibited from allowing its customers to send unsolicited advertising or "spam". The plaintiff used its account with Nexx to send spam and was warned to stop. It failed to do so and even retained a third party to send bulk email on its behalf. Some of this material, which was sent randomly, reached Nexx customers. Nexx cancelled the plaintiff's account. The plaintiff brought proceedings for relief, requiring the defendant to reactivate the account.

The Judge considered the terms of the contract and considered the meaning of "netiquette". He referred to a popular publication that listed six reasons why spam advertising was considered unacceptable behaviour on the internet. Evidence of complaints from Nexx customers was also available. The complaints were described as often intense and to the point of outrage, which the Judge took as an indication that unsolicited bulk email was not an acceptable internet practice. The Judge considered the US authorities, particularly relying on *CompuServe Inc v Cyberpromotions*.<sup>10</sup> The Judge concluded:<sup>11</sup>

[A]fter reviewing the principles that emerge in the American case law, the excerpts from the literature provided, and the reaction of individual internet users that unless a service provider specifically allows in the contract for unsolicited commercial bulk e-mail to be distributed, it appears clear that sending out unsolicited bulk email for commercial advertising purposes is contrary to the emerging principles of "Netiquette".

This conclusion is further reinforced by the admission by the plaintiff that they are unable to find another service provider which will permit bulk e-mail advertising through a third party.

The case was one based in contract, but the significance lies in the recognition of the unacceptability of unsolicited bulk advertising on the internet. The reference to the US decisions lent weight to the Judge's conclusion that the actions of the plaintiff did not constitute netiquette and he refused the relief sought.

### 3.4.1 Tort Remedies in New Zealand

It is debatable whether trespass to chattels could provide grounds in New Zealand for proceedings against spammers. The developing importance of the internet as a forum for communication, education and commerce may well lead a Court to determine a policy issue regarding the extension of the law of trespass into cyberspatial activity. The US authorities in this area are not so influenced by constitutional issues as to seriously diminish their persuasive authority.

---

<sup>9</sup> 1999 ACWSJ LEXIS 48853.

<sup>10</sup> 962 F Supp 1015; US Dist LEXIS 1997.

<sup>11</sup> Para 35.

### 3.5 Trademark infringement

Claims for trademark infringement or passing off may arise where well known brands are “spoofed”<sup>12</sup> within the main text of the messages sent by spammers, or where a well-known ISP name is given as part of a fake or “spoofed” reply-to address.<sup>13</sup> In the latter situation recipients may be confused into believing messages were sent out with the complicity of the spoofed ISP when they were not, thus trademark was infringed. In the US in the case of *AOL v Prime Data Systems*<sup>14</sup> spammers sent out 130 million junk emails all of which gave the reply to address as from the domain AOL.com. The Court found there was wilful trademark infringement and awarded \$400,000.00 damages. This demonstrates that attempts to use an ISP’s name as a jumping off spot will not be tolerated.<sup>15</sup>

### 3.5 Possible Criminal Remedies

Edwards<sup>16</sup> suggests that in the UK the Computer Misuse Act 1990, although introduced primarily to deal with computer hacking, has been used to deal with spam. In an informally reported case, an ISP had its system brought down by an overload of spam and what effectively amounted to a denial of service attack.

In New Zealand, the provisions of section 250(2)(b)(i) and (ii) of the Crimes Act (criminalising reckless or intentional access of a computer system to cause a denial of service or to cause the system to fail) may well provide a remedy in this area.

It is also possible that it an offence of disturbing use of a telephone under the Telecommunications Act<sup>17</sup> has been committed but that may only be utilised where a telephone connection is the means of accessing the internet. In these days of wireless and broadband, the use of voice connections for large scale internet operations is diminishing

## 4. Legislative issues

Although it is tempting to suggest that annoyances such as telemarketing and junk mail in the mail box could be dealt with under an all embracing spam legislation, to do that would be to overreact to a particular problem that arises from network computer technology. In my view, the legislation should be directed towards messaging systems such as e-mail, SMS using mobile phones, faxes and other electronic messaging systems.

The test that is suggested in the paper that the legislation should cover communications the cost burden for which fall upon the recipient rather than the sender is a proper one.

<sup>12</sup> “Spoofing” is the illegitimate use on the internet of an address, identity, IP number or other form of identifier.

<sup>13</sup> Lillian Edwards “Canning the Spam: Is There a Case for Legal Control of Junk Electronic Mail” [www.law.ed.ac.uk/Script/spam.htm](http://www.law.ed.ac.uk/Script/spam.htm) (last accessed 20 December 2002), p 5.

<sup>14</sup> VA No.97015–1652-A12 10 98.

<sup>15</sup> *Hotmail Corp v van\$ Money Pie Inc* 47 US PQ 2d 1020 (ND CAL 1998) 1998 3 BNA ECLR 586; see also *AOL v IMS* (1998) US Dist Lexis 17437; see also *Yahoo Inc v Worldwide Network Marketing* (1999) 4 BNA ECLR 384.

<sup>16</sup> Lillian Edwards “Canning the Spam: Is There a Case for Legal Control of Junk Electronic Mail” [www.law.ed.ac.uk/Script/spam.htm](http://www.law.ed.ac.uk/Script/spam.htm) (last accessed 20 December 2002).

<sup>17</sup> Telecommunications Act 1987, s 8(2) which reads:

[(2) Every person commits an offence against this Act who—

(a) Uses, or causes or suffers to be used, any telephone station for the purpose of disturbing, annoying, or irritating any person, *whether by calling up without speech or by wantonly or maliciously transmitting communications or sounds, with the intention of offending the recipient*; or

(b) In using a telecommunications device, knowingly gives any fictitious order, instruction, or message.

The definition should be future-proofed as far as possible and the "cost to recipient" test should be the guideline for new messaging technologies to which the legislation could apply.

The scope of the legislation should be directed towards commercial or promotional messages and, in my view, the Australian definition is most satisfactory together with the exclusions that legislation incorporates.

Earlier in this submission, I suggested that any legislation would apply only domestically, subject to specific extraterritorial implications. Once again, the Australian legislation provides a guideline. There should be extraterritorial effect extending the legislation to acts, omissions, matters and things outside New Zealand and applies to commercial electronic messages that have a New Zealand link, including messages sent from overseas to New Zealand e-mail account holders. This certainly would cover the New Zealander who arranges for spam to be directed by an overseas entity.

A numerical test provides some difficulties in determining whether or not a message is spam. This is resolved by addressing the commercial and promotional nature of the message which should be the principal test.

Necessarily, there should be express exemptions or safe-harbour provisions for telecommunications organisations and for Internet service providers. Internet service providers occupy much the same role in the Internet as the Post Office does in the hard copy mails environment. Internet service providers are those who transmit the message but have no control over its content.

#### **4.1 The consent issue**

New Zealand should adopt an opt-in approach in the manner similar to Australia. It is noted that the only country that has an opt-out approach is the United States. There are a number of constitutional reasons why this is the case. Notwithstanding the provisions of s.14 of the New Zealand Bill of Rights Act (which is one of the reasons why I have suggested a limitation of spam to commercial or promotional messages) an opt-in approach would harmonise our legislation with that of Australia and also with that proposed by the European Union.

#### **4.2 Address Harvesting**

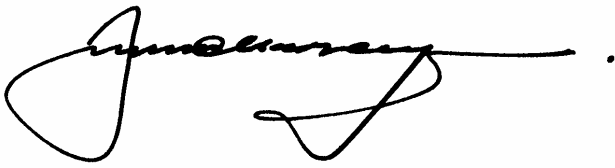
The Legislation should provide protection against the collection, transfer and use of electronic address information. It is unnecessary to include rules against the supply and acquisition of address harvesting software. The legislation should be directed towards the act of address harvesting utilising such software. It may well be that address harvesting software has other significant lawful uses. To ban software on the basis that it can be used for address harvesting is unnecessary, extends the scope of the legislation beyond the evil that it attempts to address and could interfere with commercial activity and the development of commercial utilities. The prohibition should be against the act of address harvesting utilising the software rather than putting an all-out ban on the software itself.

#### **4.3 Evidential Issues**

Given difficulties of proof, the need for forensic analysis as an adjunct of that, difficulties of detection, there is a need for search warrants and for specialist analysis of computers to obtain evidence. It is quite clear that enforcement is beyond the private citizen and should be in the hands of the Government Agency. Regrettably, the Commerce Commission has proven to be

less than aggressive in its enforcement actions in comparison with the AAAC in Australia. Furthermore, any agency that is tasked with enforcement should be prepared to be aggressive and should be funded accordingly.

Penalties should be in line with those provided under the Fair Trading Act 1986 and there should be both civil and criminal consequences. The responsible enforcement agency must be given the ability to obtain search warrants and to conduct forensic analysis on target computers. Questions of proof in the digital environment are extremely difficult and complex. Indeed, it may well be that some form of interception warrant in the nature of that provided by the Crimes Act, Part 11A and recent amendments to Summary Proceedings Act relating to tracking devices could well be of assistance in the detection of offending.

A handwritten signature in black ink, appearing to read 'D.J. Harvey', with a long horizontal flourish extending to the right.

**D.J. Harvey**  
**15 June 2004**

## Legislating against SPAM

### Questions from discussion paper

1. Do you consider spam to be an important issue? Has it significantly affected you in any way?	Yes - about 33% of my e-mail is spam
2. Do you think legislation has a role to play alongside other complementary measures?	Yes
3. Do you consider existing privacy protections in this area are sufficient?	Privacy protections are not applicable
4. Do you agree that stand-alone anti-spam legislation is preferable to reliance on the Harassment Act?	The Harassment Act is not applicable
5. What message media should be caught by the legislation (e.g. email, short message services using mobile phones, Internet instant messaging, faxes, telephones (telemarketing), physical mail delivery)?	All media should be caught subject to the provisions of the New Zealand Bill of Rights Act 1990
6. Do the messages caught by the legislation have to be sent/conveyed to many recipients, and if so, how many?	Rather than a "numerical" test, a commercial nature test should be applied
7. Should the messages caught by the legislation be of a commercial advertising and promotional nature only or should other types of messages be caught? Should there be exceptions and if so what should be exempted?	Yes
8. Should the legislation extend to coverage of acts done overseas? If so, what acts should be covered?	Yes - in a manner similar to the Australian legislation
9. Should all parties involved in the act of spamming, such as the vendor sponsoring the spamming, be covered by the legislation? Should there be express exceptions such as for telecommunications companies and ISPs?	There should be safe harbour for ISPs and Telecommunications companies as long as there is an absence of knowledge that spam is being forwarded. Sponsoring spam should be prohibited
10. Should New Zealand adopt and opt-in, double opt-in or opt-out	Double opt-in

approach in legislating against spam? Why?	
11. If an opt-in or double opt-in approach was to be adopted, 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?	Consent should not be inferred but must be express, clear and unequivocal
12. How should the scope of any opt-in or double opt-in assent be framed?	See above
13. Should there be a requirement for commercial electronic messages to accurately identify the sender of the message? If so, what constitutes accurate identification (e.g. name and physical address, name and email address)?	Yes
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 that such electronic address is functional?	Yes
15. Should there be a requirement that commercial electronic messages provide accurate header and subject information?	Yes
16. Should there be requirement for labelling of advertising or adult messages?	Yes
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?	No - there should be a prohibition against the <u>utilisation</u> of data harvesting software in that some software may have alternative and legitimate purposes
18. Who should be able to bring an action against an alleged spammer?	Commerce Commission - properly funded
19. What agency should have the enforcement role under the	Commerce Commission - properly funded

legislation?	
20. What should the available penalties and remedies for breaches of anti-spam legislation and what should be the maximum fine or pecuniary penalty?	In line with the penalties under the Fair Trading Act
21. Should contraventions give rise to criminal or civil penalties?	Both
22. Should the responsible enforcement agency be given the ability to obtain search warrants conferring powers of entry, search and seizure?	Yes
<b>Any other general comments</b>	As per my paper