LEGISLATIVE DEFINITION OF SPAM FOR NEW ZEALAND

Simon Kellett*

This article discusses the phenomenon of spam with the intention of providing a practical definition of the concept for use in anti-spam legislation. The billions of e-mails that are classified as spam every year affect the majority of the world's e-mail users, and apart from causing annoyance these unwanted communications create significant economic costs. Filtering and downloading spam wastes both time and money, and governments around the world are beginning to react to the problem with legislation to reduce the volume of spam and penalise those who deal in this medium.

The problem is how to define "spam" without punishing legitimate commercial e-mails and other unsolicited e-mails that, while not specifically requested, are not unwanted. The author supports an "opt-in" regime with the defences of consent and conspicuous publication available to prevent undue curtailment of the freedom of expression guaranteed by the New Zealand Bill of Rights Act 1990. This approach is encompassed in draft legislation set out at the end of the article.

I INTRODUCTION

The Internet, and associated technologies such as e-mail, have changed the way New Zealanders communicate. E-mail is an "essential means of communication and exchanging data for most businesses" and a valuable communication medium on a social level.[1] When compared to telephone and postal services, e-mail is faster,[2] more cost effective,[3] and can reach a wider target audience.[4]

---

* Submitted as part of the LLB (Honours) Degree at Victoria University of Wellington.

1 X-tech group *Employee Email Use – Are You Exposed?* (Simpson Grierson, 2002) <http://www.simpsongrierson.co.nz> (last accessed 19 June 2005).

2 Webopedia <http://www.webopedia.com> (last accessed 19 June 2005).

3 It has been estimated that it costs between US$0.000082 and US$0.00030 to send a single e-mail. See IBM Almaden Research Centre <http://www.almaden.ibm.com> (last accessed 19 June 2005). Other research suggests that it costs between US$0.01 and US$0.05 to send one e-mail. Association for Interactive Marketing *Survey on the Commercial Use of E-mail* <http://www.interactivehq.org> (last accessed 19 June 2005). Further research states that it costs only US$0.00032 to obtain an e-mail address from which to send spam. Cerf Vinton and Orson Swindle "Spam: Can It Be Stopped?" (18 June 2002) <www.gip.org> (last accessed 19 June 2005).

1994 saw the development of the first real threat to e-mail – spam.[5] Vint Cerf, the acknowledged "Father of the Internet", succinctly stated the problem caused by spam:[6]

> Spamming is the scourge of electronic mail and newsgroups on the Internet. It can seriously interfere with the operation of public services, to say nothing of the effect it may have on any individual's e-mail mail system. … Spammers are, in effect, taking resources away from users and service suppliers without compensation and without authorisation.

Spam "has grown to become the major plague affecting the digital world".[7] A potential threat to the full use of digital services, spam has been described as a "[s]ignificant and growing problem for users, networks and the Internet as a whole".[8]

Like many other countries New Zealand is looking to legislate against spam.[9] The Associate Minister for Information Technology and Communications, Hon David Cunliffe, recently stated:[10]

> This Government is committed to an anti-spam law. Spam is a huge waste of time and money, over two thirds of all email [sic] is now spam. This undermines the confidence, security and efficiency of New Zealanders on line.

If anti-spam legislation is to be effective, a precise definition of "spam" must be developed. The government policy group currently working on a legislative proposal identified drafting such a definition as a key issue.[11] The definition will affect the way New Zealand businesses and individuals use e-mail, and will have freedom of expression implications.[12]

---

4 Seismic Internet <http://www.seismicinternet.com> (last accessed 19 June 2005).

5 In 1994 Lawrence Canter and Martha Seigel sent an advertisement to almost every active bulletin board on the Internet, causing it to be viewed by millions of Internet users: David Harvey *Internet.law.nz* (LexisNexis, Wellington, 2003) 309.

6 EuroCAUCE <http://www.euro.cauce.org/en/index.html> (last accessed 19 June 2005).

7 International Telecommunication Union "Wave of Optimism as ITU WSIS Meeting on Countering Spam Closes" (9 July 2004) Press Release.

8 International Telecommunication Union "World Summit on the Information Society – Declaration of Principles" (2003) WSIS-03/GENEVA/DOC/4-E para 37.

9 For example, the United States of America, Australia, Japan and the United Kingdom. SpamLaws <http://www.spamlaws.com> (last accessed 19 June 2005).

10 Hon David Cunliffe MP, Associate Minister of Information Technology (17 May 2004) Press Release.

11 Ministry of Economic Development *Legislating Against Spam: Discussion Paper* (Wellington, 2004) 11-14. See also Commission of the European Communities *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee for the Regions on Unsolicited Commercial Communications or 'Spam'* (COM(2004) 28, Brussels, 2004) 8. [*Commission of the European Communities on 'Spam'*].

12 New Zealand Bill of Rights Act 1990, s 14. This section protects freedom of expression.

Legislating against spam raises a number of other issues. Penalties, standards of evidence, the inter-jurisdictional application of laws and the difficulty of tracing offenders are all important considerations for drafters.[13] However, these issues are only relevant when we have identified what spam is, and are beyond the scope of this article.

This article explores potential legislative definitions of spam. First, the necessary background concepts are laid out, then a working definition of spam will be explored, drawing on the opinions of a range of commentators. This definition will be used to help identify the harms caused by and the attributes of spam. Next the goals of anti-spam legislation will be outlined, providing a framework to measure any legislative options. Finally, a range of options will be put forward and critically analysed in relation to the framework. This paper concludes with a model legislative definition of spam.

II TECHNICAL CONCEPTS

As a creature of technology,[14] it is necessary to have a basic understanding of the mechanics of e-mail and the Internet before further analysing the features of spam.[15]

The Internet is the world's largest network,[16] in effect a network of smaller networks.[17] Essentially, the Internet facilitates the transfer of data from one computer to another.[18] Businesses

---

13 See generally Ministry of Economic Development, above n 11, 11-20.

14 The following discussion has been simplified for the purposes of brevity and does not accurately represent the precise workings of e-mail and the Internet. For a more detailed discussion of e-mail, see generally James F Kurose and Kevin W Ross *Computer Networking – A Top Down Approach Featuring the Internet* (Addison-Wesley, Massachusetts, 2001) 106-124.

15 When legislation is adopted in a technologically complex area, there are several difficulties. "First, the nature of the harms that a new technology or social phenomenon poses to the community … are unknown and the subject of speculation. Second, the measures that need to be taken to tackle the punitive harms are equally speculative – therefore, does one assume the worst case scenario and respond accordingly … or does one work with the current state of known harm and only deal with other potential harms when they actually manifest themselves?" Andrew S Butler "Limiting Rights" (2002) 33 VUWLR 537, 558.

16 A network is simply two or more computers connected together. Before the Internet, computer A could only communicate with computer C if both computers were linked directly to each other. Networks (such as the Internet) allow computer A to communicate with computer C via a third party, computer B. SearchNetworking.com <http://searchwebservices.techtarget.com> (last accessed 19 June 2005).

17 *Malarkey-Taylor Associates Inc v Communications NOW Inc* (1996) 929 F Supp 473, para 6 (D Col); *Bensusan Restaurant Corporation v King* (1996) WL 509, 716 (SDNY) Stein USDJ; *It's In The Cards v Fuschetto* (1995) LEXIS 489, para 3 (CA Wisc) Cane PJ for the Court; *Godfrey v Demon Internet Ltd* [1999] 4 All ER 342, 342 (QB) Morland J.

18 *United States v Morris* (1991) 2 CCH Comp Cas 46, 419 (2d Cir) Newman CJ for the Court.

and private individuals typically access the Internet through an Internet Service Provider (ISP)[19] such as Xtra,[20] or Ihug.[21]

E-mail is simply electronic mail.[22] The European Union has defined e-mail as "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient."[23] E-mail is sent across computer networks (for example the Internet) and is received by an electronic mail box identified by the recipient's unique electronic mail address.[24]

An e-mail is made up of three parts: the header, the subject line (a description of the e-mail seen by the recipient before they open the body of the e-mail) and the body. There may also be any number of attachments (files that are sent to the recipient along with the e-mail).[25] The header in turn contains three parts: [26]

- the address information (where the e-mail is to be delivered);
- the origin information (where the e-mail was sent from); and
- the routing information (the path the e-mail took through the Internet from the origin to the recipient).

---

19 See generally *United States of America v Microsoft Corporation* (2001) 56 F 3d 1448 (DC Cir) Silberman CJ for the Court.

20 Xtramsn <http://www.xtramsn.co.nz> (last accessed 19 June 2005).

21 Ihug <http://www.ihug.co.nz> (last accessed 19 June 2005).

22 *Eidas Software International Inc v Basis International Ltd* (1996) 947 F Supp 41, para 18 (D Ariz) Rosenblatt DJ.

23 EC Directive 58/EC Privacy and Electronic Communications Directive [2002] OJ L201 137, art 2(h).

24 *CompuServe Inc v Patterson* (1996) 39 USPQ 2d 1502, para 6 note 5 (6th Cir) Brown CJ for the Court.

25 See *Public Performance of Musical Works 1996-1998* (1999) 1 CPR (4th) 417 (Copyright Board).

26 Dan Fingerman "Spam Canned Throughout the Land? Summary of the CAN-SPAM Act" (2004) 7 J Internet L 10, 11.

Consider the following diagram:

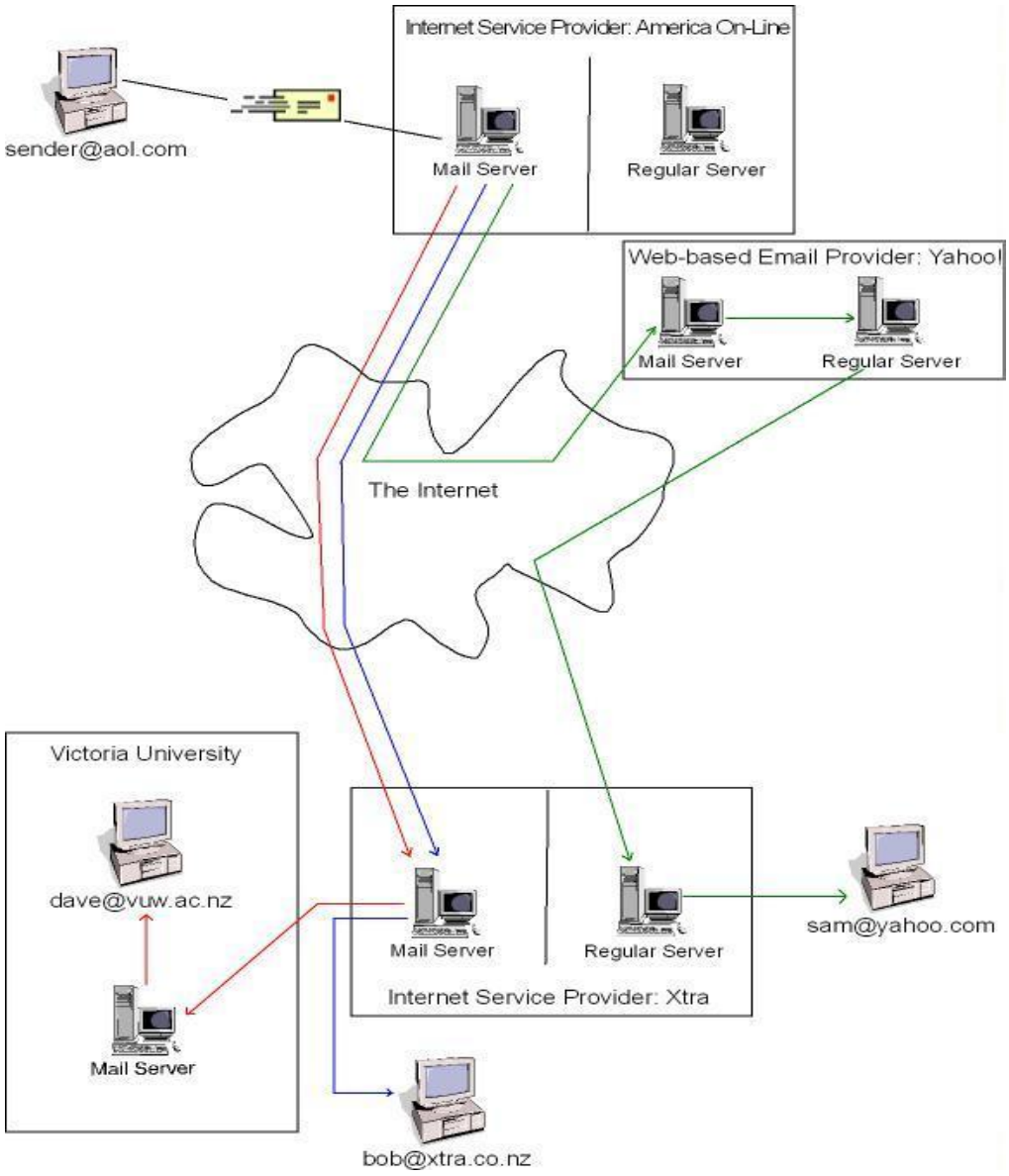

Figure 1 – The Workings of E-mail

Figure 1 represents four individuals who engage in typical e-mail activity. Sender, working within the United States, sends e-mail to three New Zealanders. Dave (who has a work e-mail account), Bob (who has an e-mail account provided by his ISP, Xtra) and Sam (who uses a web-based e-mail account).[27]

E-mail is like any other data and must be downloaded from or uploaded to a network, in this scenario, the Internet. Sender, Bob, Sam and Dave (via Victoria University) all upload and download data to their ISP at a cost.

When Sender sends the e-mail, it is uploaded to America On-Line (AOL). The mail server at AOL (the sender mail server) looks at each recipient address. If the server does not recognise the address (that is, the address is one other than an AOL address), the e-mail is relayed (forwarded) to another mail server. If this second mail server does not recognise the address, the e-mail is relayed to a third mail server. This process continues until the e-mail arrives at a mail server that does recognise the address (the recipient mail server). This intermediate relaying can be thought of as an e-mail reaching the recipient mail server from the sender mail server via the Internet.

The e-mail sent to Bob travels via the Internet and is stored at Xtra until Bob decides to retrieve it. Using an e-mail client application (such as Microsoft Outlook Express) Bob will download the e-mail, incurring a cost. Bob does not know what e-mail he has before it is downloaded, and all e-mail must be downloaded.[28]

The e-mail sent to Dave travels via the Internet and Xtra to be stored at the mail server at Victoria University. The University bears the cost of downloading the data from Xtra. Unlike the e-mail sent to Bob, Xtra only have a minimal involvement and do not store the e-mail. Similar to Bob, Dave will use an e-mail client application to download the e-mail from the university's mail server.

The e-mail sent to Sam moves via the Internet to Yahoo! where it is stored until Sam decides to view it. To view an e-mail, Sam downloads an HTML representation of the e-mail – not the actual e-mail itself.[29] Most web-based e-mail systems allow a recipient to view the header information of an e-mail before opening the e-mail body. Thus Sam can decide what e-mail he wishes to view. The HTML representation of the e-mail that Sam does wish to view is downloaded via his ISP. As

---

27 Web-based e-mail services enable you to access your e-mail via your web browser. You log into your e-mail account via the Web to send and retrieve e-mail. EmailAddresses.com "Types of Email Service" <http://www.emailaddresses.com> (last accessed 19 June 2005).

28 Some ISPs also provide access to e-mails via a web-based format (similar to Yahoo!), but this is being ignored.

29 HTML stands for Hypertext Markup Language. An HTML representation of a web-page or e-mail is interpreted by a web-client application (such as Microsoft Internet Explorer) and displayed in a way intelligible to humans.

with the e-mail sent to Dave, the ISP has minimum involvement, but is still essential as a transporter of information. Yahoo! will bear the cost of storing the e-mail on Sam's behalf.

III WORKING DEFINITION

Not all e-mail is actually wanted by the recipient. This unwanted e-mail has been classed as spam.[30] The term "spam"' conjures up images of Nigerian scams,[31] Viagra promotions and other e-mails that breach acceptable social norms in some way. Unfortunately, attaching a precise definition to this societal norm is difficult. Recognising this, some commentators opt for a trivial definition such as "junk e-mail"[32] or "you know it when you see it".[33] The vagueness and imprecision of these descriptions demonstrate the difficulty of defining exactly what spam is.

Despite this difficulty, there have been many attempts to define spam. The ideal definition would deem all e-mails that have no value to the recipient to be spam.[34]

Unfortunately, this ideal is based upon a subjective assessment of "benefit", and would be difficult to implement in practice. Not only would it be hard to disprove that an individual held certain subjective standards by which they judge spam, but it would be almost impossible for senders of e-mail to discern whether their message would be classed as spam or not, and thus whether the e-mail would attract statutory liability or not. The operation of such a subjective definition would severely diminish the effectiveness of e-mail as a communication medium.[35]

---

30 The concept of spam spans more than one medium of communication. Text messages (Short Message Service), facsimile messages and telephone calls may have many of the characteristics of spam. When considering a legislative definition this article will not consider these other communications mediums. There is some commentary suggestions that unsolicited Short Message Service (SMS) messages are not a problem in New Zealand. Interview with Suzie Wigglesworth, Vodafone Marketing Development Manager (Todd Niall, Summer Report, National Radio, 7 January 2004) Transcript provided by Newztel News Agency Ltd.

31 "Claiming to be well-placed Nigerians, con artists offer to transfer millions of dollars into the prospective victim's bank account in exchange for a small fee. Those who respond to the initial offer may receive official-looking documents. Typically, the victim is then asked to provide blank letterhead and his or her bank account numbers, as well as some money to cover transaction and transfer costs and attorney's fees." Federal Trader Commission *FTC Prepared Statement on Spam* (Washington DC, 2003) 5, note 10 [*FTC Prepared Statement on Spam*].

32 Nigel Horrocks (ed) *Netguide for Seniors Premier Issue* (Auckland, 2002) 77.

33 Philip Argy, Vice President, Australian Computer Society (23 October 2003) submission to the Senate Environment, Communications, Information Technology and Arts Committee 18.

34 Wye-Keen Khong "Regulating Spam on the Internet" (15th BILETA Conference: Electronic Datasets and Access to Legal Information, University of Warwick, Coventry, England, 14 April 2000).

35 For example, consider the definition adopted by the *Oxford Concise Dictionary* (10 ed, Oxford University Press, United States, 1999) 1374: "Irrelevant or inappropriate messages sent on the Internet to a large number …of users." This definition suffers from subjective ambiguity. What I consider to be "irrelevant or

In the search for some objective characterisation of spam, many commentators have warned that "not all unsolicited commercial communication is spam (eg direct marketing)."[36] The New Zealand Mission to the European Union decided that spam is generally held to refer to unsolicited, commercial communications sent in bulk by electronic means where the originator has disguised their identity."[37]

The French National Data Processing and Liberties Commission defines spam as: [38]

> The practice of sending unsolicited e-mails, most frequently of a commercial nature, in large numbers and repeatedly to individuals with whom the sender has no previous contact, and whose e-mail address may be found in a public place on the Internet, such as newsgroups, mailing lists, directory or websites.

Concerned about "[b]ulk e-mailing that is clearly inappropriate or unwanted[,] in particular but not exclusively those containing illegal, offensive or deceptive content…",[39] the Australian National Office for the Information Economy defined spam as: [40]

> [U]nsolicited electronic messages, usually transmitted to a large number of recipients. They usually, but not necessarily, have a commercial focus, promoting or selling products or services; and they share one of the following characteristics:
>
> - they are sent in a largely untargeted and indiscriminate manner, often by automated means;
> - they promote illegal or offensive conduct;
> - their purpose is fraudulent or otherwise deceptive;
> - they collect personal information in breach of national privacy principles;

---

inappropriate" may differ considerably to your interpretation. From a practical standpoint, individuals and companies sending e-mail can never be sure if the e-mail will breach the recipient's subjective threshold of spam or not.

36 Mark Talbot, New Zealand Mission to the European Union "OECD Workshop On Spam" (19 February 2004) Letter 2; Business and Industry Advisory Committee to the OECD "Discussion Paper on Spam Presented to the OECD Workshop on Spam" (OECD Workshop on Spam, Brussels, 2-3 February 2004) 1; Directorate for Science, Technology and Industry, Committee on Consumer Policy and Committee for Information, Computer and Communications Policy "OECD Workshop on Spam – Report of the Workshop" (OECD Workshop on Spam, Brussels, 2-3 February 2004) 4.

37 Talbot, above n 36, 2.

38 Commission Nationale de l'Informatique et des Libertés *Report of 14 October 1999* <http://www.cnil.fr> (last accessed 19 June 2005).

39 Australian National Office for the Information Economy *Final Report of the NOIE Review of the Spam Problem and How it can be Countered* (Canberra, 2003) 2.

40 *Commission of the European Communities on 'Spam'*, above n 11, 7.

- they are sent in a manner that disguises the originator, i.e. spoofing and use of third party resources;
- they do not offer a working address which recipients may send messages opting out of receiving further unsolicited messages.

Finally, a European Commission report found that "spam" is generally understood to mean the repeated mass mailing of unsolicited commercial messages by a sender who disguises or forges his identity."[41]

It is clear that the current definitions of spam are founded upon either the content (illegal, pornographic), the nature of sending (unsolicited, no prior relationship, indiscriminate) or the harms caused by spam. Considering these different approaches, it is possible to discern three similar yet distinct definitions of spam:

(1) Unsolicited commercial e-mail. Some commentators include the qualifier "usually commercial" which adds further uncertainly to the definition;[42]

(2) unsolicited commercial (typically) bulk e-mail; and[43]

(3) unsolicited bulk e-mail.[44]

---

41 Commission of the European Communities *Unsolicited Commercial Communications and Data Protection – Summary of Findings* (2001) 14 <http://europa.eu.int/index_en.htm> (last accessed 19 June 2005).

42 *1267623 Ontario Inc v NEXX On-Line Inc* [1999] ACWSJ 621737, para 2 (Ont SC) Wilson J; Claudia Ray and Johanna Schmitt "Stopping Spam: Federal and International Initiatives" (2003) 7 J Internet L 1, 1; Preston Gralla *How the Internet Works, Millennium Edition* (Que, Indianapolis, 1999) 100; Interview with Nick Bolton, Anti-Spam Software Developer (Todd Niall, Summer Report, National Radio, 7 January 2004) Transcript provided by Newztel News Agency Ltd; Rebecca Porter "Smothered in Spam" (2004) 40 Trial 50, 50; Mark Morris and Troy L Booher "A Case for National E-mail Regulation: State UCE Statutes Have Infirmities" (2003) 70 Def Couns J 355, 355; Rene Ryman "The Adverse Impact of Anti-Spam Companies" (2003) 20 Computer & Internet Law 15, 15; Charles H Kennedy and Christine E Lyon "The CAN-SPAM Act of 2003: A New Regime for Email Advertising" (2004) 21 Computer & Internet Law 1, 2; Erkki Liikanen, European Commission Enterprise and Information Society Commission "Opening Remarks at the OECD Workshop on Spam" (OECD Workshop on Spam, Brussels, 2-3 February 2004); Trans Atlantic Consumer Dialogue *Consumer Attitudes Regarding Unsolicited Commercial Email (Spam)* (INTERNET-29-04, London, 2004) 1.

43 *America Online v LCGM Inc* (1998) 46 F Supp 2d 444, 446 (D Va) Lee USDJ; *FTC Prepared Statement on Spam*, above n 31, 2; *Commission of the European Communities on 'Spam'*, above n 11, 8.

44 *Maxnet Holdings Inc v Maxnet Inc* [2000] US Dist Lexis 7524, para I (ED Penn) Hutton J; Rebecca Porter, above n 42, 50; Sophie Dawson "Green Eggs and SPAM – Regulation of Unsolicited Email in Australia" (2001) 44 NSWSCL <http://www.nswscl.org.au> (last accessed 19 June 2005); Paul Hoffman, Internet Mail Consortium *Unsolicited Bulk Email: Definitions and Problems* (5 October 1997) <http://www.imc.org/ube-def.html> (last accessed 19 June 2005); Spamhaus *The Definition of Spam* <http://www.spamhaus.org> (last accessed 19 June 2005); Coalition Against Unsolicited Bulk Email, Australia *Submission for the Inquiry into the Spam Bill 2003 by the ECITA Legislation Committee* (submission to ECITA Legislation Committee,

Another spam definition, "[d]eceptive unsolicited email messages",[45] has not received such widespread support. Although some 66 per cent of spam contains some deceptive element, spammers can work around this definition by sending truthful e-mail. [46]

An effective definition of spam will target a range of factors such as illegal content, deceptive header information, indiscriminate sending as well as being commercial or bulk in nature. Furthermore, spam is invariably unsolicited.[47]

Consequentially, this paper suggests a working definition of spam as:[48]

unsolicited e-mail that is either:

(a) sent to many recipients; or

(b) has content which is illegal, fraudulent or commercial in nature.

This definition is consistent with the perception of the New Zealand business community,[49] and Internet users generally.[50]

IV HARMS

The case for anti-spam legislation is strengthened if it can be shown that spam causes serious harm. Further, the effectiveness of a legislative definition can be tested by reference to the extent to which it focuses on those harms.

2003) 12; but see Australian National Office for the Information Economy *The Spam Problem and how it can be Countered: An Interim Report by NOIE* (Canberra, 2003) 8 which defines spam as "unsolicited bulk electronic messages …. They are usually – but not necessarily – commercial in nature i.e. they generally promote or sell products or services."

45 "Microsoft Files 15 Lawsuits Against Spammers in the US and UK" (2003) 20 Computer & Internet Law 28, 28.

46 Federal Trade Commission "FTC Measures False Claims Inherent in Random Spam" (29 April 2003) Press Release. Around 40 per cent of those messages contained some indication of falsity in the message body. Thirty-three per cent of those messages had false 'from' information while a further 22 per cent had false 'subject' lines.

47 Stop Spam "Understanding Spam" <http://www.stopspam.net.nz> (last accessed 19 June 2005); Survey data collected by author. Here, 100 per cent of survey respondents felt that "unsolicited" was an essential defining characteristic of spam.

48 Another good working definition of spam is found in David Harris "Drowning in Sewage" 6 <http://www.internetnz.net.nz> (last accessed 19 June 2005).

49 Survey data collected by author (Wellington, 2004).

50 Gartner Consulting "ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition" (California, 1999) 6. In response to the question "what is spam?" 74 per cent of respondents said it was unsolicited bulk e-mail, while 72 per cent of respondents said it was unsolicited commercial e-mail (respondents could choose more than one category for what they considered to be spam).

Some harms caused by spam are self-evident (such as a breach of privacy), while others are only brought into sharp focus when one considers the huge volume of spam being sent.

In the middle of 2001, spam accounted for just eight per cent of all e-mail traffic; spam now constitutes 63 per cent of all e-mail sent around the world.[51] In New Zealand, 60 per cent of the e-mail traveling through the ISP TelstraClear is spam.[52] New Zealand companies find that spam accounts for between 20 and 60 per cent of all e-mail received, the average amount being 35.92 per cent.[53]

Underlying these percentages are the huge volumes of e-mail being sent. In the year ending 31 January 2003 Brightmail,[54] one of the world's leading e-mail companies, filtered 145 billion e-mail messages. Eighty billion of these were subsequently classed as spam.[55] Currently, there are 31 billion e-mails sent daily,[56] 63 per cent of which are spam. Considering that there are only 888 million individuals with Internet access,[57] using just under an estimated 1200 million mailboxes, these numbers demonstrate that spam is a large scale problem affecting many individuals.[58]

The harms, or costs of spam can be broken down into financial and social costs, and harm to the Internet as a communication medium. The following section will precisely detail those harms.

A Financial Costs

There are a range of financial costs imposed on the Internet community by spam.

1 Internet costs

When communicating by telephone, text message (SMS) or post, the sender must incur a unit cost for each communication before that communication can reach the recipient. For e-mail, the financial burden of sending one is the same as the burden for sending one million. Essentially the

---

51 Ministry of Economic Development, above n 11, 5.

52 Interview with Paul Brislen, Writer, Computer World On-line (Todd Niall, Summer Report, National Radio, 7 January 2004) Transcript provided by Newztel News Agency Ltd.

53 Survey data collected by author (Wellington, 2004).

54 Symantec Brightmail <http://www.brightmail.com> (last accessed 19 June 2005).

55 Symantec Brightmail "The State of Spam Impact & Solutions" (California, 2003) 1 <http://www.brightmail.com> (last accessed 19 June 2005).

56 Spam Filter Review "E-mail Statistics 2004" <http://www.spamfilterreview.com> (last accessed 19 June 2005).

57 Internet World Stats "Usage and Population Statistics"<www.internetworldstats.com> (last accessed 19 June 2005).

58 CNN.com "Email Mailboxes to Increase to 1.2 Billion Worldwide by 2005" <http://www.cnn.com> (last accessed 19 June 2005).

financial burdens are shifted from the sender to the recipient (and intermediate carrier). Consider figure 1.[59]

Notice that all our e-mail recipients are at some stage reliant on an ISP to have the e-mail delivered to them. When data is downloaded from an ISP, either in the form of e-mail or an HTML page, a cost to the recipient is incurred. Users are charged for either the volume of data downloaded, or the amount of time spent connected to the Internet.[60] Assume that the e-mail sent by Sender was 100 kilobytes (KB).

Bob pays for his Internet on the basis of time connected. Given that he *must* download all e-mail sent to him, Bob will be charged for the time taken to download 100KB of data. Interestingly, as a consumer, Bob can expect to receive, and be charged for, 2200 spam e-mails a year.[61]

Compare this to Sam and Dave who are charged on the amount of data downloaded. Both will have to pay the price of downloading 100KB of data.[62] In this situation, Sam is in the better position. Using a web-based e-mail account, he can view the header information of the e-mail before downloading it. He may decide an e-mail is spam and delete it.

Furthermore, Bob or Dave may pay a fixed or flat rate for their Internet connection and are charged the same rate regardless of the amount of data sent and received. In this scenario, there are no Internet costs for the recipients.

Whenever an ISP transfers data to and from the Internet, they incur a cost as well. This is because an ISP pays for bandwidth, or the volume of data sent or received from the Internet.[63] Therefore, Xtra will incur costs when it receives data from the Internet in order to pass that onto their customers. It has been estimated that it costs an ISP US$2.50 per 1000 e-mails sent.[64] This cost becomes substantial when we consider how many millions of e-mails an ISP must deal with.

Contrast these costs to those incurred by the spammer. Sender must initially upload the e-mail to the AOL mail server. Thus, Sender will incur a charge for either the time taken to upload 100KB or simply pay for 100KB of data to be uploaded. However, this is where the costs for Sender end.

---

59 See Part II Technical Concepts.

60 TelstraClear "Internet Access" <http://www.telstraclear.co.nz> (last accessed 19 June 2005).

61 Don Passenger, Jeff Kikkey "Un-Canned Spam" (2003) 82 Mich Bar J 36, 36.

62 In this scenario the company Dave works for will have to pay, rather than Dave himself.

63 Office of Information Technology "Glossary of Terminology" <www.oit.ohio-state.edu> (last accessed 19 June 2005).

64 *America Online Inc v National Health Care Discount Inc* (2001) 174 F Supp 2d 890, 899 (ND Iowa) Zoss MJ.

Once the e-mail is in the mail server, the server then sends a copy of that e-mail to the recipients. This will incur three times 100KB of data transfer costs to AOL.

The cost for Sender does not change whether the e-mail is addressed to three or three million recipients.[65] A similar situation occurs when using a web-based e-mail service.[66] In the worst case scenario, the spammer can use a variety of hacking techniques to completely avoid being charged at all.

2 Maintenance costs

On top of the actual Internet costs are the underlying costs of maintaining e-mail systems. There are three types of maintenance costs that affect the Internet community.

First are data storage costs. An ISP or web-based e-mail host will store all their customers' e-mails before the customers retrieve them. If there are more e-mails to store (due to the amount of spam) then data storage facilities will have to be upgraded.

Second is filtering. Filtering is the process of scanning an e-mail and determining whether it is spam. If the e-mail is spam, it may be deleted before the recipient receives it, or it may be tagged as spam indicating that a recipient may safely delete it.

Consider figure 2. The e-mail destined for Dave could be filtered at Victoria University's e-mail server, or by his e-mail client program. The e-mail destined for Bob could be filtered by the e-mail server at Xtra, or by his e-mail client program. Only the mail server at Yahoo! can filter Sam's e-mail. The costs of filtering are fourfold. Initially, the filter must be purchased and large commercial filters can be very expensive.[67] Then the filter must be updated or trained to keep up to date with new spamming techniques. This takes time and may incur additional costs to purchase upgrades.[68] Thirdly, the process of filtering e-mail requires processing power. It may be necessary to purchase faster computers to deal with the demands of filtering.[69] Finally, filters may accidentally identify a legitimate e-mail as spam. The recipient may never receive the e-mail, potentially meaning business or social opportunities will be lost.

---

65 Ray Everett-Church *Prepared Statement for the United States House of Representatives Subcommittee on Telecommunications, Trade and Consumer Protection* (submission to United States House of Representatives Subcommittee on Telecommunications, Trade and Consumer Protection, 1999) 2.

66 Ray Everett-Church, above n 65, 2.

67 Survey data collected by author (Wellington, 2004); see for example Symantec Brightmail "Pricing" <http://www.brightmail.com> (last accessed 19 June 2005). However, free filters are also available, for example MailWasher <http://www.mailwasher.net/> (last accessed 19 June 2005).

68 Survey data collected by author (Wellington, 2004).

69 Survey data collected by author (Wellington 2004). One respondent purchased three new servers in 2004 to cope with the added processing demands of spam.

Third are the costs of fielding customer complaints. ISPs spend valuable staff resources responding to complaints about, and troubleshooting problems arising from, spam.

3 Productivity losses

Spam has escalated beyond the nuisance stage to become a harmful impediment to productivity.[70] This problem often stems from misleading subject lines and false sender details, which force the recipient to view the message body before it can be identified as spam. From a business perspective, it may cost employers anywhere from Australian$1 per spam received,[71] to between UK£326[72] and US$1000[73] per employee per annum.[74] There will also be a cost for any organisation trying to deal with spam. For example, the United States Federal Trade Commission receives 120,000 spam related complaints daily.[75]

A survey of 1000 consumers conducted by InsightExpress suggests that 65 per cent spent more than 10 minutes each day dealing with spam, and 24 per cent reported dealing with it for more than 20 minutes per day.[76] In New Zealand, it may take employees anywhere from 1 to 20 minutes per day to deal with spam.[77]

4 Reputation loss

A spammer may modify the "from" header information in an e-mail to make it appear as if the e-mail is from some other sender. As a result, the reputation of a business can be ruined if it appears that they are sending spam. There will be a potential community backlash at the (perceived)

---

70 Jonathan Bick "Spam-Related Class Actions are on the Horizon" (2003) 172 NJLJ 29, 29.

71 Surf Control "Anti-Spam Prevalence Study" (2002) 1 <http://surfcontrol.com> (last accessed 19 June 2005).

72 Star "Spam and Porn Cost UK Business £3.2 Billion Every Year" <http://www.star.net.uk/star/home.stml> (last accessed 19 June 2005).

73 Erado "White Paper on Spam" <http://www.erado.com> (last accessed 19 June 2005).

74 See also Confederation of Danish Industries and ITEK "Antispam – A Guide from the Conference of Danish Industries and ITEK" (2004) 3 <http://www.itek.di.dk> (last accessed 19 June 2005) which estimates the cost to employers at DKK 33.74 per worker per day.

75 Jonathan Krim "FTC Files Suit Against Sender of Porn 'Spam'" (18 April 2003) *Washington Post* Washington DC E1; "Federal Anti-Spam Law Guts Tough State Remedies" (23 December 2003) *USA Today* Virginia A14.

76 OECD Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy *Background Paper for the OECD Workshop on Spam* (DSTI/ICCC/(2003)10/REV1, Brussels, 2003) 12 [*OECD Background Paper*]; Robyn Greenspan and Brian Morrissey *Spam Expected to Outnumber Non-Spam* <http://www.clickz.com> (last accessed 19 June 2005).

77 Survey data collected by author (Wellington, 2004).

sender,[78] increasing maintenance costs while the company responds to complaints. The company may be "blacklisted" (a list of individuals/groups who spam) by recipients, meaning that future (legitimate) e-mails sent by the company may be blocked by filters under the assumption that those e-mails are spam. Essentially, once a company has been labeled as a spammer, it is extremely difficult to remove that taint.[79]

5 Total costs

Aggregated, these costs are substantial. Some believe that the international community loses £25 million per year.[80] Companies in the United States put the figure much higher, calculating that they alone lost US$10 billion in 2003. US$4 billion of productivity was lost, and US$6 billion in network upgrades, increased personnel costs and unrecoverable data.[81] For the consumer, it is estimated that fighting spam adds another US$2 to each user's monthly Internet bill,[82] as costs to ISPs are generally passed on to the consumer.[83]

B Social Costs

Apart from being very annoying,[84] spam creates other social harms. Spam often contains fraudulent or deceptive material.[85] Consumers may be enticed to engage in "get rich quick schemes" or to purchase faulty (or non-existent) goods or services. Eighteen per cent of spam carries pornography,[86] and may be accessible by minors. Some spam may carry computer viruses.[87] These viruses could destroy critical data on a computer network, or allow third parties to "hijack" a computer and use the resources of that computer for their own purposes.[88] Privacy concerns are

---

78 Ellen Neuborne "Unleashing the Monster of E-Mail Marketing" (15 May 2000) <http://www.businessweek.com> (last accessed 19 June 2005).

79 EmailAddresses.com "The Cost of Spam" <http://www.emailaddresses.com> (last accessed 19 June 2005).

80 UN News Centre "Un Meeting Outlines Steps to Curb Problem of Spam Email" (21 July 2004) <http://www.un.org/apps/news> (last accessed 19 June 2005).

81 Senate Report No 108-102 (2003) WL 21680759 7.

82 Senate Report, above n 81, 6.

83 *OECD Background Paper*, above n 76, 12.

84 In a recent survey, 96 per cent of respondents said they hated spam or that spam annoyed them. Trans Atlantic Consumer Dialogue, above n 42, 2.

85 *FTC Prepared Statement on Spam*, above n 31, 2.

86 Symantec Brightmail "The State of Spam Impact & Solutions" (California, 2003) 3 <http://www.brightmail.com> (last accessed 19 June 2005).

87 Adam Gifford "US War on Spam May Put NZ at Risk" (19 March 2004) *The New Zealand Herald* Auckland.

88 David Harris, above n 48, para 3.2.6.

raised by the fact that a recipient of e-mail can frequently see the e-mail addresses of all the other recipients. Additionally, private e-mail addresses are often collected without a recipient's consent.

C Threat to Internet

As a result of the potential social and economic harms, people feel genuine aggravation against spam – the public is hostile to junk e-mail.[89] This is having a spin off effect against the Internet and the value of e-mail itself.[90]

1 Internet communication

There is a concern that spam may stifle other Internet communications.[91] Evidence suggests that some users avoid Internet forums and other activities where they need to give their e-mail address, for fear that their address will be picked up by a spammer. This has a chilling effect on the use of the web and discussion forums.[92] One half of all e-mail users are already more distrustful of e-mail, while one quarter of users use e-mail less because of spam.[93] Other commentators fear that the threat of spam completely turns people away from using e-mail or the Internet.[94]

2 Internet commerce

At the recent OECD Workshop on spam, there was concern that consumer trust and confidence have been adversely impacted by spam.[95] As "[c]onsumer trust is key for the growth and success of e-commerce",[96] the threat of spam ruining the necessary consumer confidence is serious.[97] One survey suggests that 52 per cent of respondents shop online less or not at all because they are

---

89 Robert C Beasley "Practically Speaking" (2004) 24 Licensing Journal 26, 26.

90 CAUBE.AU "The Problem" <http://www.caube.org.au> (last accessed 19 June 2005).

91 CAUBE.AU, above n 90.

92 Dan Fingerman, above n 26, 13. Further research indicates that 100 per cent of e-mail addresses posted on chat rooms received spam, as did 86 per cent of addresses posted to newsgroups or on web-pages: *FTC Prepared Statement on Spam*, above n 31, 6.

93 Jane Black "Needed: A Beefier CAN-SPAM Bill; Recipients of Unwanted Email Should Have the Right to Sue, and Law Enforcement Needs More Muscle to Put These Pests Out of Business." (30 October 2003) *Business Week Online* <http://www.businessweek.com> (last accessed 19 June 2005).

94 Australia Labor Party *Inquiry into the Spam Bill 2003 and the Spam (Consequential Amendments) Bill 2003* (Senate Printing Unit, Canberra) para 37; Gartner Consulting "ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition" (California, 1999) 9.

95 *OECD Background Paper*, above n 76, 4.

96 *OECD Background Paper*, above n 76, 4.

97 *FTC Prepared Statement on Spam*, above n 31, 3; Erkki Liikanen, above n 42. A survey concluded that 25 per cent of interviewees used e-mail less because of spam. *Commission of the European Communities on 'Spam'*, above n 11, 8 note 11; *OECD Background Paper*, above n 76, 4.

worried about spam.[98] This is consistent with the theory that spam is choking commerce on the Internet.[99]

3 Infrastructure

Finally "a serious Internet infrastructure problem flows from the sheer volume of spam that is now being sent."[100] Spam can be used to disrupt communications networks through denial of service attacks,[101] and small ISPs may be overwhelmed by the volume of traffic.[102]

D Analysis of Harm

Clearly there is a wide range of harm caused by spam. Some harm, like the financial burden, is content-neutral. In fact, even bona fide e-mail incurs these harms. The only difference is that when the recipient has an interest in the e-mail, they are content to bear the cost of that receipt. Other harms, like pornography or false advertising, are content specific.

In deciding what attributes are most relevant to a legislative definition, it is necessary to decide what harms are linked to what attributes, thereby ensuring the legislation targets the harm. The following table demonstrates this relationship:[103]

---

98 Trans Atlantic Consumer Dialogue, above n 42, 2.

99 Australian Direct Marketing Association "Submission on the Spam Bill 2003 and Spam (Consequential Amendments) Bill 2003" to the Senate Environment, Communications, Information Technology and the Arts Legislation Committee (2003) 1.

100 *FTC Prepared Statement on Spam*, above n 31, 2.

101 "Conduct directed towards a website or email recipient which has the objective of making it impossible for legitimate users of the website [sic] or email address to use the facility. This might take the form of using software to generate a very large number of requests for pages off the website, or sending a very large number of emails – mailbombing." SiteMaster-Internet.co.uk <http://www.sitemaster-internet.co.uk> (last accessed 19 June 2005).

102 *OECD Background Paper*, above n 76, 12.

103 This table was developed on the assumption that the recipient did not want the e-mail.

Attribute		Harm										
		Internet Charges	Maintenance	Productivity	Reputation	Privacy	Deceptive Material	Pornography	Viruses	Lose Consumer Confidence	People Stop Using Forums	Threats to Internet Infrastructure
Message Body Content Neutral Factors	Sent in bulk	Yes	Yes	Yes	No	Yes	No	No	No	No	No	Yes
	Overall volume of e-mail	Yes	Yes	Yes	No	No	No	No	No	No	No	Yes
	Unsolicited	Yes	No	Yes	No	No	No	No	No	Yes	No	No
	Sent by automated means / indiscriminately	Yes (bounced emails)	No	No	No	No	No	No	No	No	No	No
	Repetitive	No	No	No	No	No	No	No	No	No	No	No
	Unstoppable	No	No	No	No	No	No	No	No	Yes	No	No
	Deception of origin	No	Yes	No	Yes	No	No	No	No	Yes	No	No
	Deceptive "subject line"	Yes	No	Yes	No	No	No	No	No	No	No	No
	Opt-out mechanism does not work	Yes	Yes	Yes	No	No	No	No	No	Yes	No	No
	E-mail address collected without consent	No	No	No	No	No	No	No	No	Yes	Yes	No
Message Body Content Specific	Commercial	No	No	No	No	No	Yes	No	No	Yes	No	No
	Fraudulent / illegal / objectionable content	No	No	No	No	No	Yes	Yes	Yes	No	No	No

Interestingly, the "commercial" attribute has little to no relevance to any of the harms. The volume of e-mail sent – particularly in terms of financial cost – causes the greatest harm.

V LEGISLATION

Building upon the previous discussion of spam, this paper will now identify problem areas for legislators, and suggest a piece of model legislation. The legislative experiences of Australia,[104] the United States,[105] and the United Kingdom,[106] have demonstrated that legislation must:

---

104 Spam Act 2003 (Cth) [the Spam Act].

105 Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003 Pub L No 108-187 117 Stat 2699 (2003) [CAN-SPAM Act].

(1) Be effective, in that it targets the harms caused by spam;

(2) be clear, to reduce uncertainty which leads to compliance costs and the risk that individuals will refrain from e-mail communication out of fear that they may be caught by the legislation; and

(3) place the minimum possible intrusion on the freedom of expression.

In New Zealand, the Bill of Rights Act 1990 (BORA) protects anything that is written or said,[107] regardless of the nature of the particular communication or the context in which it occurs.[108] When deciding whether a legislative limitation on e-mail communications (which clearly gain the protection of the BORA)[109] is "demonstrably justified in a free and democratic society",[110] the *Moonen* test will be applied:[111]

(1) identification of the importance and significance of the objective of the legislation;

(2) reasonable proportionality between the objective and the limit;

(3) rational connection between the limit and the objective; and

(4) as little interference with the right as possible.

Generally, if the problem being addressed is significant, the limitations introduced can be greater and still be proportional to that goal.[112]

---

106 The Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK).

107 New Zealand Bill of Rights Act 1990, s 14. This section protects freedom of expression.

108 Paul Rishworth and others *The New Zealand Bill of Rights* (Oxford University Press, Melbourne, 2003) 311. See also *Ballantyne, Davidson and McIntyre v Canada* (1994) 1 IHRR 145, 156 (UNHRC).

109 See generally Matthew D Farrington *Change Begets Change: Internet Technology and Free Speech* (LLM Research Paper, Victoria University of Wellington, 2002). Interestingly, the characteristics of the Internet (limitless range of subject matter; innovation and the ability for all Internet users to be active producers of information; the ability to build upon what is already there; internet speech is participatory and interactive; the Internet allows new communities, cultures and sub-cultures to develop, opening forums for all types of speech) may actually exemplify the underlying proposition of free speech: Jack M Balkin "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society" (2004) 79 NYUL Rev 1.

110 New Zealand Bill of Rights Act 1990, s 5.

111 *Moonen v Film and Literature Board of Review* [2000] 2 NZLR 9 (CA), 16-17 Tipping J for the Court. This is clearly a restatement of the test in *R v Oakes* [1986] 1 SCR 103, 138-9 (SCC) Dickinson CJ. See generally Rishworth and others, above n 108, 168-216 for an excellent discussion on rights limitations.

112 Rishworth and others, above n 108, 177.

VI WHAT E-MAIL SHOULD BE COVERED?

Legislators must first decide what types of e-mail fall, prima facie, within the legislative scope.

A Unsolicited E-mail

The one universally accepted characteristic of spam is that it is unsolicited.[113] In other words, the recipient has not consented to receive the e-mail. If an individual does consent to receive an e-mail, they also voluntarily shoulder any financial and social harms caused by that receipt. Therefore, legislators must decide if the recipient's consent must be obtained before an e-mail can be sent to them (an opt-in regime) or if e-mail may be sent to an individual until they expressly revoke their consent to receive further e-mail (an opt-out regime).

1 Opt-out regime

This approach provides the best protection for freedom of expression and direct marketing,[114] because the restriction on sending e-mail only applies where the recipient has expressly removed their consent. Provided an opt-out (revocation of consent) request has not been received, individuals or businesses can confidently send e-mail to whomever they wish. This adds certainty to the application of the legislation. Further, the introduction of a national do-not-e-mail registry makes the opt-out approach more effective.[115] In the United States, such a registry was found to be consistent with the protection of freedom of expression.[116] For these reasons, an opt-out regime has been adopted in several countries.[117]

Ironically, an opt-out regime actually legalises spam rather than banning it.[118] This is because any e-mail sender, including spammers, has a "free shot" at every mailbox. Additionally, spammers can work around opt-out requests by starting multiple companies. An opt-out request only applies to the e-mail sender (a company) meaning the other companies are free to continue spamming you.

---

113 See Part III Working Definition.

114 Fingerman, above n 26, 14.

115 A centralised list of individuals who do not want to receive unsolicited communications, generally maintained by government or a regulatory body such as a Direct Marketing Association. Individuals may have the option of deciding what types of communications they do not want to receive, as well as refusing all unsolicited communications generally.

116 A do-not-call telephone register was found to be consistent with the United States Constitution's first amendment: *Mainstream Marketing v Federal Trade Commission* (2003) US App LEXIS 20366 (10th Cir); "Tenth Circuit Upholds Do-Not-Call Registry" (2004) 21 Computer & Internet Law 33, 33.

117 See generally CAN-SPAM Act, above n 106; The Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK); The Law on Regulation of Transmission of Specified Electronic Mail 2002 (Japan); Act on Information Network and Protection 2001 (Korea); Government Decree Nr 17/1999 (II 5) on Distance Selling (Hungary).

118 Fingerman, above n 26, 10; Kennedy and Lyon, above n 42, 1.

This problem would be circumvented by a national do-not-e-mail list, but these lists have been declared unsustainable by the United States Federal Trade Commission.[119] Additionally, such a list has no impact on spammers working from other jurisdictions. Worse still, such a list could be stolen by spammers and used as a source of e-mail addresses.

The opt-out approach completely ignores the burden spam places on productivity. The time spent sending an opt-out request would take longer than simply deleting the e-mail. Therefore, the harm of spam is not specifically targeted. It is also confusing for consumers who have been told that responding to spam merely confirms that your address is "live", thus inviting even more spam.[120]

2 Opt-in

The general public prefer an opt-in approach,[121] because it gives better protection to consumers.[122] This is because people only receive those e-mails that they consent to receive. However, the limit on freedom of expression (no e-mail may be sent without the recipient's consent) is far too wide and the opt-in approach must be tailored to ensure consistency with the BORA. This can be achieved by further limiting the application of the legislation (for example, to only illegal or commercial speech) or providing a range of legislative defences for sending unsolicited e-mail.

3 Mixed approach

The United Kingdom has adopted a mixed approach.[123] E-mail (for direct marketing purposes) sent to natural persons works on an opt-in basis, while that same e-mail sent to a legal person is sent on a opt-out basis.[124] This approach fails to recognise that "spam is a problem not only for personal e-mail accounts, but for corporate accounts."[125] Spammers are free to spam businesses with impunity,[126] causing financial and social harms. Additionally, legitimate e-mail senders are faced with the difficult (and potentially costly) question of whether they are sending an e-mail to a legal or

---

119 Federal Trade Commission *National Do Not Email Registry A Report to Congress* (Washington DC, 2004) i.

120 Stop Spam "Golden Rule No. 2: Never Reply to Spam" <www.stopspam.org.nz> (last accessed 19 June 2005).

121 Eighty-one per cent of respondents in the poll said that opt-in was the way to go. Trans Atlantic Consumer Dialogue, above n 45, 1; Survey data collected by author (Wellington, 2004). But note that New Zealand marketers demonstrated a comparative bias towards an opt-out approach when compared to the rest of the business community.

122 Talbot, above n 36, 6.

123 As found in The Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK) in implementing EC Directive 58/EC Privacy and Electronic Communications Directive [2002] OJ L201/37.

124 The Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK) cl 22 (1) and (2).

125 *OECD Background Paper*, above n 76, 3.

126 *OECD Background Paper*, above n 76, 38.

natural person – something that is not always clear from the e-mail address itself.[127] A uniform approach would add certainty to the legislation.

Therefore, an opt-in approach is the most effective, provided it can be tailored to promote BORA consistency.

B Bulk

An e-mail is sent in "bulk" when it is sent to many recipients. Consistency with the BORA can be achieved by applying an opt-out regime to unsolicited bulk e-mail. As discussed above, spam is generally sent in bulk, which in turn adds to the harm caused by the sheer volume of e-mail sent.[128] Therefore, there is a rational connection between the limitation and government desire to eliminate spam. Unfortunately, a definition of "bulk" that is effective against spammers but does not affect legitimate e-mail communications is difficult to find.

Defining "bulk" in terms of the number of recipients an e-mail is sent to is problematic. If a very small number is attached to the notion of bulk, such that any unsolicited e-mail sent to two or more recipients attracts liability,[129] a vast range of e-mail (both spam and legitimate) would be captured. This lacks the necessary rational connection between the limitation and the harm. If a much larger number of recipients was used, for example 1000, spammers could easily avoid liability by sending each e-mail to 999 recipients.

In response to this technique, "bulk" could be defined as any particular e-mail sent to (for example) 1000 different recipients on a single day. Spammers will respond by sending 999 people the original e-mail, and subsequent groups of 999 people slightly modified versions of the e-mail. Adding the qualifier "particular e-mail or *materially similar e-mail*" could stop this practice. In deciding whether two e-mails are materially similar, the courts could look at the purpose of the e-mail. If two e-mails both advertise the same herbal medication (albeit with different text) they are materially similar. Unfortunately a "materially similar" approach still carries some latent uncertainty. Further, spammers could circumvent the legislation altogether by sending out e-mail that advertises different products.

A final option is to limit the total amount of e-mail any one person can send per day. This approach requires a number small enough to cripple spammers, but large enough to ensure that legitimate e-mail senders are not caught. Consider a figure of 2000. Spammers, who usually send significantly more e-mails per day would be severely affected. However, it is not unreasonable to assume that some individuals or companies actually send 2000 unsolicited e-mails each day, that

---

127 *Commission of the European Communities on 'Spam'*, above n 11, 9.

128 See Part IV Harms.

129 Survey data collected by author (Wellington, 2004).

are nonetheless legitimate.[130] The amount of e-mail sent by individuals may increase as more uses are found for the communication medium. On the other hand, setting the threshold at 2000 means every individual has the right to send 1999 unsolicited e-mails each day – resulting in a potential 4.3 billion e-mails sent per day, all completely legally.[131]

Therefore, "bulk" e-mail should not be used as the basis for legislation because of the difficulties inherent in its definition.

C Commercial

Another option for achieving BORA consistency would be to apply an opt-in regime to unsolicited commercial e-mail. Two reasons add legitimacy to this option. First, although pure commercial speech is covered by the BORA,[132] such speech receives less protection.[133] This means that limits may be imposed on commercial speech that could not be imposed on political or religious speech.[134] A similar situation exists in the United States, although the constitutionality of anti-spam legislation is yet to be tested.[135]

Secondly, most commentators agree that people send spam for financial gain.[136] "As long as the profit motive remains, so will the problem."[137] The economic viability of spamming is clearly evidenced in that people continue to purchase goods and services from spam.[138] This financial

---

130 These e-mails may include internal company communications, offers of work, information about current business transactions and other content that should not be affected by anti-spam legislation.

131 New Zealand has a population of four million, and an Internet penetration rate of 55 per cent. Internet World Stats "Top 20 Countries with Highest Internet Penetration Rate" <www.internetworldstats.com> (last accessed 19 June 2005). This means that 2.2 million natural persons can send 1999 unsolicited e-mails each day. This figure would increase when the e-mail sent by legal persons is factored in.

132 New Zealand Bill of Rights Act 1990, s 14.

133 See *Hosking v Runting* [2004] 1 NZLR 1, para 258 (CA) Tipping J.

134 *Virginia State Board of Pharmacy v Virginia Citizens Consumer Council* (1976) 425 US 748, 772 Blackmun J for the Court; See generally Rishworth and others, above n 108, 331-332.

135 *CompuServe Inc v Cyber Promotions Inc* (1997) 93 F Supp 1015, 1026 (SD Ohio) Graham DCJ; and *Cyber Promotions Inc v America Online Inc* (1996) 948 F Supp 436, 451 (ED Pa) Weiner J both dealt with the issue of spam, but involved private companies and thus did not require a First Amendment inquiry.

136 Interview with Nick Bolton, above n 42.

137 Harris, above n 48, 10. See also Elizabeth A Alongi "Has the US Canned Spam?" (2004) 46 Arizona L Rev 263, 274.

138 Seven per cent of e-mail users have ordered from unsolicited commercial e-mail, while 33 per cent have clicked on a link to get more information. See *Commission of the European Communities on 'Spam'*, above n 11, 7 note 7; a survey conducted by the Federal Trade Commission found that 8 per cent of 1118 respondents had purchased a product from a spam e-mail. Federal Trade Commission "SpamCatcher Attitude Survey" (1 May 2003) Forum Release.

incentive behind spamming has the flow on effect that most spam is commercial in nature.[139] It follows that by targeting commercial e-mail, the legislation will be rationally connected to the objective of eliminating spam, albeit indirectly, as most spam is commercial. The difficulty is achieving the "balance between making spamming unprofitable yet protecting legitimate business communications channels."[140] This balance will be achieved by the legislative definition of "commercial e-mail".

"Commercial" means the exchange of goods, products, or property of any kind or the buying, selling, and exchanging of articles.[141] The broad and ambiguous scope of this definition makes it unsuitable for legislation. Recognising this, other jurisdictions have attempted to refine the definition of "commercial e-mail". The CAN-SPAM Act defines commercial e-mail as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."[142]

A similar definition is adopted in the Australian Spam Act 2003 which defines a commercial electronic message as one where the purpose, or one of the purposes, of the message is:[143]

(1) to offer to supply goods or services; or

(2) to advertise or promote goods or services; or

(3) to advertise or promote a supplier, or prospective supplier, of goods and services.

The key issue with these definitions is the difference between "advertising" and "promoting" a product. These terms must stand for different ideas, and courts will be disinclined to hold that the terms have the same meaning.

1 Advertise versus promote

The Advertising Standards Authority (ASA) states that "[t]he word 'advertisement' … includes advertising which promotes the interest of any person, product or service, imparts information, educates, or advocates an idea, belief, political viewpoint or opportunity."[144]

---

139 Harris, above n 48, 6.

140 Hon Richard Alston MP, Minister for Communications, Information Technology and the Arts, "Australia Slams The Door on Spam" (18 September 2003) Press Release.

141 *Anderson v Humble Oil and Refining Co* (1970) 174 SE 2d 415, 417 (SC GA).

142 CAN-SPAM Act, above n 105, s 3(2)(A).

143 Spam Act 2003 (Cth), s 6(1).

144 Advertising Standards Authority Inc "Interpretation" <http://www.asa.co.nz/intro.htm> (last accessed 19 June 2005).

A current legislative definition of advertisement is "any publication … used to promote the sale of [a product or service]."[145]

Note that both definitions use the term "promote" to define "advertisement".

Promote has been defined as: "[t]o contribute to growth, enlargement, or prosperity of; to forward; to further; to encourage; to advance."[146] This broad definition has lead to concern that "promote" will cover legitimate business-to-business and other e-mail messages that advance a business' interests but do not expressly advertise a product or service.[147]

For example, consider an (unsolicited) e-mail containing political comment sent to the opinion section of a local newspaper. Suppose further that the e-mail was sent from a business e-mail account, and a link to the company web-page along with the company slogan is appended to the bottom of the e-mail. The purpose of the appended information is clearly to forward, further or advance the company and yet few would call such an e-mail spam.

This issue can be resolved by realising that promotion and advertising are not disjunctive ideas. Rather, advertising is a subset of promotion. Given that the motivation for sending spam is to sell products, the definition of commercial e-mail should be limited to:

> [T]hose e-mails that advance the sale of a product or service, and not merely promote a company generally.

This would not be unduly harsh on direct marketers. They do not generally send unsolicited e-mail, and prefer an opt-in approach.[148] One reason being that spamming would probably lose more customers than it would gain.[149] Therefore, legislation that limits the sending of advertisement material will not affect our marketers, provided that consensual advertising material does not attract liability.

2 Direct marketing

In contrast, the United Kingdom legislates against direct marketing.[150] Although no definition of "direct marketing" is offered, it is clear from other European legislation that "direct marketing" is

---

145 Hazardous Substances and New Organisms Act 1996, s 2(1); Agricultural Compounds and Veterinary Medicines Act 1997, s 2(1). See also Fair Trading Act 1986, s 2(1).

146 Henry C Black *Deluxe Black's Law Dictionary* (6 ed, West Publishing Co, Minnesota, 1990) 1214.

147 Kennedy and Lyon, above n 42, 1.

148 The New Zealand Marketing Association "Standards for Email Marketing" (Auckland, 2005) Guiding Principle One ["Standards for E-mail Marketing"].

149 Interview with Zak Bullen, Business Development Manager, Message Media (Todd Niall, Summer Report, National Radio, 7 January 2004) Transcript provided by Newztel News Agency Ltd.

150 The Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK), cl 22 (1) and (2).

different to e-mail for "promotional purposes".[151] In New Zealand, direct marketing has been defined as "[t]he process by which consumers are offered the opportunity to obtain or purchase goods or services".[152] Clearly the precise extent of "offered the opportunity" is uncertain.

Therefore, the best definition of unsolicited commercial e-mail is "an e-mail that advertises a product or service" where "advertise" means to advance the sale of a product or service.

3 Primary or secondary purpose

This narrower definition also resolves the "primary or secondary purpose issue". The CAN-SPAM Act requires that the advertisement or promotion of a product be the primary purpose of the e-mail.[153] Thus, spammers can circumvent the legislative intent by inserting other information into an e-mail, relegating the advertisement or promotion of a product to secondary importance.

The Spam Act takes a broader approach, covering e-mail where the purpose, or one of the purposes, of the message was to advertise or promote the sale of a good or service.[154] This definition is potentially too broad, given that a lot of e-mail sent from a commercial e-mail address will have some company referencing information automatically appended to that e-mail.[155] This extra information is clearly promoting the company, and may indirectly promote the products or services supplied by that company, bringing that e-mail within the scope of the legislation. This broad definition may have the effect of destroying e-mail as a business communications medium as businesses may decide not to use e-mail, for fear of being caught by the legislation.

The best option is to define commercial e-mail as "an e-mail, any purpose of which is to advertise (advancing the sale of) a good or service." This definition gives protection to e-mail sent from a business account, while capturing spammers who try to circumvent legislation by putting other information into the e-mail. Consider an e-mail that contains political opinion, and an Internet link to a web-page selling Viagra. Although the primary purpose of the e-mail may have been to spread political comment, one purpose of the e-mail was to advertise (advance the sale of) Viagra and therefore, the e-mail will be caught by the legislation.

Consider a similar e-mail from a company employee to a friend. At the bottom of the e-mail, the contact details of the company and the company slogan are appended. This e-mail will not be

---

151 Italian Personal Data Protection Code Legislative Decree No 196 (20 June 2003), ss 130(1) and 130(5).

152 The New Zealand Marketing Association "Code of Practice for Direct Marketing in New Zealand" (Auckland, 2000) 2.

153 CAN-SPAM Act, above n 105, s 3(2)(A).

154 Spam Act 2003 (Cth), s 6(1).

155 For example: a disclaimer, company contact details, company logo or motto, or link to the company web-site.

caught by the legislation. Although one of the purposes of the e-mail was to promote the company (and hence promote the goods and services provided by that company), it is difficult to argue that the e-mail actually advertised (advanced the sale of) a good or service.

4 Non-commercial speech

Unfortunately, it does not follow that spammers are driven solely by commercial incentives. People may spam for social, religious or political reasons as well, especially as e-mail is an inexpensive medium and can transcend political and geographical boundaries.[156] To define spam in purely commercial terms may dangerously limit the scope of the legislation. In Australia, for example, there was a strong body of opinion that called for the legislation to include both commercial and non-commercial e-mail.[157] However, it will be much more difficult to justify a limitation on non-commercial speech in terms of the BORA. A ban that potentially covers all e-mail is not specifically targeted enough to be an effective definition.

D Illegal E-mail

One response to the limited "commercial" focus of the legislation would be to extend the legislative scope to cover all e-mail that contains illegal material, such as false advertising, fraud, scams and objectionable material.[158] Although freedom of expression does cover illegal speech,[159] the government has a compelling objective in suppressing such speech. Therefore the legislation should ban all e-mail containing material that is in breach of any law of New Zealand. Clearly there is a rational connection between the limitation and the harm, and that limit is proportional to the government objective.

VII LEGISLATIVE REQUIREMENTS

Clearly legislators should focus on unsolicited e-mail sent for an illegal or commercial purpose. However, there are some other factors that should be considered, that is, other criteria that render a seemingly legitimate e-mail spam when drafting legislation.

---

156 E-mail could be sent in the volumes we are seeing now by groups determined to have their voices heard. Currently, the majority of (albeit commercial) spam originates from 200 individuals or groups. Spamhaus "ROKSO" <http://www.spamhaus.org> (last accessed 19 June 2005). Out of all the people who have Internet access, it is not unreasonable to think that 200 may have an opinion to push.

157 Australian Democrats *Inquiry into the Spam Bill 2003 and the Spam (Consequential Amendments) Bill 2003* (Senate Printing Unit, Canberra) 30; Australian Privacy Foundation *Submission to the Inquiry into the Spam Bill 2003 and Spam (Consequential Amendments) Bill 2003* (submission to the ECITA Legislation Committee, 2003) 3.

158 Within the meaning of the Films, Videos and Publications Classification Act 1993, s 3.

159 Rishworth and others, above n 108, 312.

A Accurate "From" Clause

Altering the sender information in an e-mail header is a technique often used by spammers to avoid detection. Thus all e-mail, regardless of content, should accurately identify the e-mail address from which the e-mail was sent.[160] The New Zealand business community endorses this sentiment.[161]

This requirement places no burden on e-mail senders because accurate sender information is the default position. Manipulating sender information requires some considerable skill (the use of open relays[162] or open proxies[163]) and effort. Additionally, there is no limitation on anonymous speech.[164] Individuals can still participate in anonymous communications in the traditional way – opening up a web-based e-mail account with an obscure address.[165] The sender remains anonymous, but the Internet community is able to respond to unsolicited e-mail.[166]

Unfortunately, spammers often open up a web-based e-mail account with false details to send unsolicited commercial e-mail.[167] Forcing people to sign up for e-mail accounts with accurate

---

160 This avoids the difficulty found in the American legislation. CAN-SPAM Act, above n 105, s 5(a)(1)(B) provides that the 'from' clause is not misleading if it accurately identifies the person who initiated the message. The section is silent on the inclusion of an e-mail address in the "from" clause and so could be interpreted to permit a spammer to identify themselves by name alone – this is not very useful when you are trying to contact them, or close down their e-mail address: Fingerman, above n 26, 11.

161 Survey data collected by author (Wellington, 2004).

162 "Open relays allow spammers to route their e-mail through servers of other organizations, thereby disguising the origin of the e-mail. Spammers identify and use other organizations' open relays to avoid detection by the filter systems that ISPs use to protect their customers from unwanted spam. Routing spam through open relays also makes it difficult for law enforcement agencies to track down senders of fraudulent or deceptive spam": *FTC Prepared Statement on Spam*, above n 31, 12, note 14.

163 "A proxy server runs software that allows it to be the one machine in a network that directly interacts with the Internet. This provides the network with greater security. But if a proxy is not configured properly (i.e. if it is an "open proxy"), it may also allow unauthorized users to pass through the site and connect to other hosts on the Internet. For example, a spammer can use an open proxy to connect to a mail server. If the server has an open mail relay, the spammer can send a large amount of spam and then disconnect – all anonymously": *FTC Prepared Statement on Spam*, above n 31, 12, note 15.

164 Anonymous speech is an important right and must be protected. See Dawn C Nunziato "Freedom of Expression Democratic Norms and Internet Governance" (2003) 52 Emory LJ 187, Part VI.

165 For example, "MrExample999@hotmail.com".

166 Although the person sending the e-mail remains anonymous, the e-mail account can be shut down, stopping further e-mail from being sent.

167 When signing up for a web-based e-mail account, the individual signing up must usually provide their name and contact details. For example, see Yahoo! <www.mail.yahoo.com> (last accessed 19 June 2005).

details could reduce this problem.[168] It is evident that there is a legitimate link between these requirements and the goal of reducing spam.

B Unsubscribe Function

A recipient must be given the opportunity to revoke consent to receive future e-mails, even where consent was initially granted. Thus, every commercial e-mail should provide an opt-out mechanism. This mechanism does not need to be electronic, as is the case in the United States,[169] but must not place any extra financial burden on the recipient to use.[170] Potential legislative uncertainty can be reduced by providing that if an e-mail has been sent on behalf of more than one sender, then an opt-out request should apply to all those senders. [171]

VIII DEFENCES

The current definition of spam may be considered too wide by those who still wish to send unsolicited commercial e-mail. In these limited situations, a legislative defence should render legitimate what is prima facie spam.

Clearly an individual should be able to receive whatever e-mail they wish, provided they have given their consent (opted-in), unless the e-mail content is illegal.[172] By consenting, a recipient has made a decision to bear the burden (financial or social) of that receipt. The defence of consent allows commercial e-mail to be sent, limiting the intrusion onto the freedom of expression.

When a person consents, it is important that they are aware as to what exactly they are consenting to. The scope of the consent, which may range from the broad (you may send me any marketing material) to the narrow (you may send me specific adult content) must be determined on the facts. Further, a legislative presumption that any consent will be read narrowly should be included. This will help provide legislative certainty, and will help to protect consumers from unwanted e-mail.

---

168 This clearly removes the right of anonymous speech, but may be justified given that commercial speech receives a lower threshold of protection. Such a requirement for all speech would be difficult to justify. Enforcement would also pose difficulties, especially for web-based e-mail. Many of the more effective mechanisms (such as requiring people to set up such an account via their ISP, who could verify their details) impose compliance costs on innocent parties.

169 CAN-SPAM Act, above n 105, s 5(a)(3). Thus an 0800 telephone number should be sufficient in New Zealand.

170 For example, the costs of sending an e-mail or making a regular telephone call are examples of satisfactory costs for an individual to bear when they submit an opt-out request. Spam Regulations 2004 Statutory Rules 54 (Cth) reg 3.4.

171 Joshua Baer, UnsubCentral Inc "The CAN-SPAM Act" (Privacy Futures Symposium, San Francisco, 9-11 June 2004).

172 See Part VI D Illegal E-mail.

A Actual Consent

Actual consent may only be given by an informed individual through overt action.[173] This means that submitting an application via an Internet form that contains a pre-checked "you may send me any marketing material" box would not be considered to be actual consent.

B Implied Consent

A further defence is necessary to cover circumstances where actual consent has not been granted, but the e-mail sender reasonably inferred that the recipient would consent to receiving the e-mail. In Australia, a defence where consent can be reasonably inferred from the conduct and the business and other relationships of the individual or organisation concerned has been provided.[174] However, the extent of this defence is ambiguous, and has been criticised for creating legislative uncertainty.[175]

Nonetheless, compare that defence to the exception for "transactional relationship messages" adopted in the United States.[176] This very narrow exception covers only unsolicited e-mail sent to customers regarding a current commercial transaction.[177] This exception would not cover the situation where a company sends details of a special product offer to a customer who purchases that product on a weekly basis. Additionally, inferring consent on the basis of an established business relationship is common practice for many New Zealand companies.[178] Therefore, the Australian option is preferable to the American.

By providing factors that judges should consider when deciding whether consent can be inferred, legislative uncertainty can be minimised. The courts should look at:

- The duration of the relationship, and the types of transactions undertaken in the context of that relationship. If a legal or natural person has always purchased a particular product from a company, that company could reasonably infer consent for an e-mail relating to the previously purchased product;
- the content of the e-mail. If the content is directly related to a previous business transaction, then it will be easier to infer consent;

---

173 See CAN-SPAM Act, above n 105, s 3(1)(A); Spam Act 2003 (Cth), sch 2, cl 2(a).

174 Spam Act 2003 (Cth), sch 2, cl 2(b).

175 Microsoft Australia "Submission on the Spam Bill 2003 and Spam (Consequential Amendments) Bill 2003" to the Senate Environment, Communications, Information Technology and the Arts Legislation Committee, 2.

176 CAN-SPAM Act, above n 105, s 3(17)(A).

177 Kennedy and Lyon, above n 42, 3.

178 "Standards for E-mail Marketing", above n 148, Guiding Principle One.

- the importance of the e-mail. If the importance of the e-mail is such that it is almost inevitable that the recipient would consent to receive it, then this will be sufficient to be protected by the defence of inferred consent. For example, a product recall due to defects, or information showing how the product is a hazard to its user; and
- the frequency of previous business interaction. It is easier to infer consent for a person who has entered into a business transaction with the sender on numerous occasions.

The onus is on the sender to show that it was reasonable to infer consent. In balancing the factors, the content of the e-mail is of foremost importance. A car company sending a Viagra advertisement to an established, frequent customer would not attract protection from the defence.

C Conspicuous Publication

Finally, there are situations where there is no previous relationship from which consent can be inferred but where an individual still has an interest in receiving an unsolicited commercial e-mail. For example, a plumber would be interested in receiving offers of work and information about specialist tools. This situation is covered by the "conspicuous publication" defence which has been adopted in Australia.[179]

In order to infer consent from the conspicuous publication of an e-mail address, four criteria must be met:

(1) The e-mail address must allow the public, or a section thereof, to e-mail an individual in their employment capacity,[180] provided that it is reasonable to assume that the e-mail was published with the consent of that person;[181]

(2) the address must be conspicuously published,[182] that is, the address must be prominently displayed;[183]

(3) a statement having the effect of revoking any possible implied consent must not accompany the address;[184] and

(4) the content of any e-mail sent must be relevant to the functions, duties, office or position of the recipient.[185]

---

179 Spam Act 2003 (Cth), sch 2, cl 4(2).

180 Spam Act 2003 (Cth), sch 2, cl 4(2)(a).

181 Spam Act 2003 (Cth), sch 2, cl 4(2)(c).

182 Spam Act 2003 (Cth), sch 2, cl 4(2)(b).

183 National Office for the Information Economy *Spam Act 2003: A Practical Guide for Business* (Canberra, 2004) 19.

184 Spam Act 2003 (Cth), sch 2, cl 4(2)(d).

Essentially, when an individual publishes their e-mail address in the yellow pages, newspapers, journals or on web-sites, they are inviting communications in respect of their particular work related function.[186]

However, this defence adds uncertainty to the Australian legislation. First, it may be difficult (and potentially expensive) to establish whether an e-mail address has been published in a business or personal context. This distinction can not always be deciphered by looking at the actual e-mail address.[187] Secondly, the legislation is silent on the situation where the sender reasonably believed the e-mail content to relate to the functions, duties, office or position of the recipient.[188] Thirdly, the defence does not cover commercial e-mail sent to individuals who are not acting in an employment or organisational function. Thus, those e-mails will not be sent to private individuals who may have an interest in receiving them.[189] Fourthly, this defence allows a broad range of vendors to e-mail those individuals who have a wide interest in a business or organisation.[190] Finally, there is a danger that spammers will develop sophisticated databases of names that link e-mail addresses to job titles or position, meaning only e-mails that fall within the defence are sent.[191]

Notwithstanding these difficulties, a conspicuous publication defence is necessary to ensure that business communications are not overly disrupted by anti-spam legislation. However, the impact of these issues must be reduced. First, the defence should be extended to cover e-mail sent to private individuals, provided the content of the e-mail was directly related to an activity undertaken by the

---

185 Spam Act 2003 (Cth), 2nd sch, cl 4(2)(e)-(g).

186 Australian National Office for the Information Economy *NOIE Submission to the Senate Environment, Communications, Information Technology and the Arts Committee* (submission to ECITA Legislation Committee, 2003) 7.

187 For example, consider a plumber who uses the (fictional) e-mail address of "bob@xtra.co.nz".

188 Spam Act 2003 (Cth), 2nd sch, cl 4(2)(e)-(g).

189 Consider an avid gardener who has a personal web-site discussing their passion for gardening. They would have an interest in receiving e-mails about special deals on gardening products, or new gardening tools. The conspicuous publication defence should cover these people as well.

190 For example, consider a small business operator who has several staff, two vans and a computer. Because of their wide range of involvement in the business, e-mail relating to computer hardware/software, new tools, staff training, management techniques, company law reform, vehicle maintenance and commercial advertising all relate to their business position. Any company promoting these products may reasonably send unsolicited e-mail to this business owner.

191 See Electronic Frontiers Australia "Spam Bill 2003 and Spam (Consequential Amendments) Bill 2003" submission to the Senate Environment, Communications, Information Technology and the Arts Legislation Committee (20 October 2003) 6-14.

individual, and the individual had made it known what particular activities they are interested in.[192] Secondly, the defence should be available to e-mail senders who reasonably believed the content of the e-mail related to the recipient's employment, organisational involvement or interest. It would be difficult for a spammer, sending out great volumes of e-mail, to show that they reasonably believed (after making an informed, objective evaluation) the content of each e-mail had the nexus of relevance for each recipient. Finally, in considering whether an e-mail does have the necessary nexus of relevance, the courts should consider:

- Whether the sender reasonably believed that the recipient was interested in receiving the e-mail; and
- whether the precise role of the recipient was made clear when the e-mail address was published. The more ambiguous the role, the more difficult it is to show that the address was conspicuously published.

The inclusion of this defence in the legislative scheme will soften the strictness of an opt-in regime in its raw form. Therefore, there will be a level of protection granted to legitimate companies that should not be afforded to those who engage in spamming. This defence also reduces the impact on the freedom of expression, ensuring consistency with the BORA.

IX CONCLUSION

There are many considerations to be taken into account when drafting anti-spam legislation. This paper has considered the specific harms of spam, and analysed a range of legislative options in relation to those harms. It is clear that some options, such as legislating against "bulk" e-mail, or developing an "opt-out" regime are ineffective at stopping spam. This is because a savvy spammer can easily circumvent the legislation.

It is also clear that a pure "opt-in" regime would be too harsh, and potentially inconsistent with BORA protections. For that reason, the legislative defences of consent and conspicuous publication should be available. The rationale for this being that not all unsolicited e-mail is classed as spam.

Although the major focus is on unsolicited commercial e-mail, it is important to make anti-spam legislation equally applicable to e-mail containing either illegal content, or inaccurate sender information. These are common features of spam, and breach the societal norms of the Internet community.

X DRAFT LEGISLATION

Taking all these factors into account, a model legislative definition of spam is submitted as follows:

---

192 Therefore it would not be legitimate to send an e-mail about cleaning products to the gardener, as this does not specifically relate to their publicly stated interest.

Section 2 - Interpretation

"Advertise" means to advance the sale of any good or service or any interest in any good or service.

"Sender" means any legal or natural person who sent or caused to be sent an electronic mail message.

Section 3 - Definition of commercial e-mail

For the purposes of this Act, "commercial e-mail" means any electronic mail message, any purpose of which is to advertise any product or service.

Section 4 - Offences

(1) it is an offence for any legal or natural person to send or cause to be sent:

(a) any commercial e-mail;

(b) any electronic mail message, the content of which is illegal under any other New Zealand statute, regulation, code, or the common law of New Zealand;

(c) any electronic mail message such that when the message reaches the recipient, the sender information no longer accurately identifies the electronic mail address from which the electronic mail message was sent.

(2) it is an offence for any legal or natural person to sign up for or otherwise acquire an e-mail account by using false, misleading or fraudulent information, if the e-mail account will be used to send the type of e-mail described in subsection (1) paragraph (a) above.

Section 5 - Defence of consent

(1) It shall be a defence to any charge under section (4) subsection (1) paragraph (a), or section (4) subsection (1) paragraph (c) of this Act for the sender of the electronic mail message to show that either:

(a) the recipient of the electronic mail message consented for that message to be sent.

(i) subsection (1) will only apply when the consent was fully informed and given by a positive action by the recipient;

(ii) the scope of that consent is to be given the most narrow interpretation.

or:

(a) it was in all the circumstances reasonable for the sender of the electronic mail message to infer consent based on:

(i) the conduct; and

(ii) the business and other relationships;

of the individual or organisation concerned.

(2) In deciding whether it was reasonable in all the circumstances to infer consent under subsection (1) paragraph (b) of this section, the court must consider:

(a) the duration of the relationship between the sender and the recipient;

(b) the nature of the transactions undertaken in the context of that relationship;

(c) the frequency of interaction between the sender and the recipient; and

(d) the importance of the content of that electronic mail message.

Section 6 – Defence of Conspicuous Publication[193]

(1) It shall be a defence to any charge under section (4) subsection (1) paragraph (a) of this Act for the sender of the electronic mail message to show that a particular electronic mail address has been published such that it allows the public, or a section of the public, to send an electronic mail message to:

(a) any employee, director, or partner of a business, company or partnership; or

(b) any member of an organisation, or individual holding public office; or

(c) any individual in a private capacity, provided that:

(2) The electronic mail address had been conspicuously published; and

(3) It would be reasonable to assume that the publication occurred with the consent of the individual who uses the electronic mail address so conspicuously published; and

(4) The sender of the electronic mail message reasonably believes that content of the sent electronic mail message is directly relevant to:

(a) if subsection (1)(a) or subsection (1)(b) applies, the function, duties, office, position, or role concerned; or

(b) if subsection (1)(c) applies, the specific interest or activities undertaken by that individual which were publicly stated along with the electronic mail address;

(5) In considering whether the content of an electronic mail message is directly relevant, the court must take the following into account:

(a) whether the sender reasonably believed that the recipient was interested in receiving the electronic mail message; and

---

193 This section is modeled heavily on the Australian Act: see Spam Act 2003 (Cth), sch 2, cl 4(2).

(b) whether the precise role of the recipient was made clear when the e-mail address was published.

(6) This defence will not apply when the published electronic mail address is accompanied by a statement to the effect that the relevant holder of the address does not wish to receive any commercial e-mail.

It is submitted that this definition is more effective than those found in other jurisdictions. By limiting an opt-in regime to unsolicited commercial e-mail, capturing all e-mail that breaches key societal norms and providing legislative defences for legitimate unsolicited commercial e-mail, it is submitted that this definition balances the requirements of the BORA with the desire to be rid of spam.

XI POSTSCRIPT

Since the time of writing, the Government has introduced the Unsolicited Electronic Messages Bill 2005.[194] The Bill operates a mixed opt-in/opt-out regime. Messages that have the primary purpose of marketing or promoting goods and services (commercial electronic messages) operate under an opt-in regime.[195] However if the primary purpose is simply to promote or market an organisation (promotional electronic message), an opt-out regime applies.[196]

There are several difficulties with this approach. First, the legislation creates a distinction between the primary and secondary purpose. This has been criticised in other jurisdictions, as discussed above. The model legislation does not draw such a distinction. Secondly, it may be difficult to determine the difference between promoting the sale of a good, and promoting the organisation generally. For example, consider the "Coke™" logo. The model legislation attempts to avoid this difficulty by looking for "advertising of a good or service" and not the mere promotion of an organisation.

There are several other points of distinction between the model legislation and the Bill. The Bill provides a defence of conspicuous publication, but fails to provide a list of relevant criteria with which to judge whether a publication has been conspicuous.[197]

Additionally, the Bill requires that the person who authorised the sending be identified by the message.[198] This goes beyond the requirements of the model legislation where only the sending address need be identified. However, the Bill's requirements only apply to commercial and

---

[194] Unsolicited Electronic Messages Bill 2005, no 281-1.

[195] Unsolicited Electronic Messages Bill 2005, no 281-1, cls 2, 6 and 9.

[196] Unsolicited Electronic Messages Bill 2005, no 281-1, cls 2 and 10.

[197] Unsolicited Electronic Messages Bill 2005, no 281-1, cl 2.

[198] Unsolicited Electronic Messages Bill 2005, no 281-1, cl 11.

promotional messages. The model legislation would impose its more limited requirement on all messages.

Further research as to the differences between the model legislation and the Bill is required. Each piece of legislation is a balancing act – making some elements wider, and others narrower. The Bill and the legislation proposed in this article have chosen to widen and narrow different parts of the overall "anti-spam" framework. The passage of this legislation will be watched with interest.