The Need for Business Law Co-Ordination in the Global Marketplace

Maree Chetwin
Associate Professor, College of Business and Economics,
Department of Accountancy, Finance and Information Systems,
University of Canterbury, Private Bag 4800, Christchurch 8020, New Zealand
Tel: +64 3 364 2616; Fax: +64 3 364 2727
Email: maree.chetwin@canterbury.ac.nz

Abstract: E-mail is regarded by some companies as a mainstream marketing option. Legislation that prohibits unsolicited electronic messages of a marketing nature is a basis to stop the growth of spam. The ideal solution would be an international framework of legislation and law enforcement, but, legislation around the world has been diverse. New Zealand has taken a wait and see attitude to spam legislation. Its discussion paper "Legislating Against Spam," which was issued in May 2004, made considerable reference to the Australian approach. This paper considers the proposed New Zealand legislation in light of the Australian Spam Act 2003 and the New Zealand and Australian Memorandum of Understanding (MoU) on business law co-ordination. Does the proposed legislation go far enough? Legislation is a positive move. Without legislation, there is no basis from which New Zealand can address spam on a global basis. It is also a move to ensure sound business e-marketing practices which are essential as the Internet increases in importance for business communications. Spam is a global problem and reference is also included to the diverse approaches of the United Kingdom and the United States.

Introduction

E-mail is an important business tool as it is low cost and effective. Increasingly consumers use technology to access information. Related to this has been a significant growth in spam via the internet which threatens the growth of the internet and the information society as a whole.

On July 25, 2005, the New Zealand Commerce Minister, Pete Hodgson, announced that New Zealand and Australia would review their Memorandum of Understanding (MoU) on business law co-ordination. "Better co-ordination has been called for by the business community on both sides of the Tasman and we are interested in their views on the MoU and how it could be improved." Two days later, the Unsolicited Electronic Messages Bill was tabled in the New Zealand Parliament. The Australian Spam Act 2003 was the outcome of the review by the Australian National Office for the Information Economy (NOIE). New Zealand's discussion paper which was issued in May 2004, Legislating Against Spam, made considerable reference to the Australian approach.

Proceedings of the Fifth International Conference on Electronic Business, Hong Kong, December 5-9, 2005, pp. 719 - 724.

The Unsolicited Electronic Messages Bill

The explanatory note to the Unsolicited Electronic Messages Bill states that the legislation is part of a multi-tiered strategy to combat the growth of spam along with self-regulation in the form of industry codes of practice, education and awareness campaigns, improved technical measures, and international co-operation. Generally, it is a positive move as it will ensure that New Zealand is no longer a soft target for spammers. However, it should be noted that New Zealand has been slow to introduce legislation and its response is not innovative but rather a weak response to the problem.

Australian Spam Act 2003

The Australian Government website of the Department of Communications, Information Technology and the Arts outlines its "multi-layered strategy to address spam as recommended in the *Final Report of the National Office for the Information Economy (NOIE) review of the spam problem and how it can be countered*. This strategy involves the following elements designed to complement and reinforce each other:

- national legislation (the *Spam Act 2003* and the *Spam (Consequential Amendments) Act 2003*);
- international cooperation;
- information and awareness-raising;
- industry codes of practice; and
- technical solutions.

The Australian Spam Act 2003 and the Spam (Consequential Amendments) Act 2003 were passed by Parliament in December 2003 and both came into effect on 10 April 2004.

Is the Australian Spam Act the best model for New Zealand?

Cheng suggests that "[t]he 2003 [Australian] enactments should be seen as a major step on a long road, rather than arrival at a final destination." This is particularly the case when the Spam Act is considered in light of global developments, legislation in other jurisdictions, such as the United States and the European Directives. It was announced on 2 July 2004 that the Australian Competition & Consumer Commission (ACCC), and the Australian

Communications Authority (ACA) were signatories to a Memorandum of Understanding between the US Federal Trade Commission, the UK Department of Trade & Industry, the UK Information Commissioner and UK Office of Fair Trading for mutual assistance in the enforcement of spam laws. The UK Department of Trade and Industry website outlines the effect -

"It will mean for the first time that:

- Enforcement authorities in the UK, United States and Australia will work together to investigate spammers in those countries;
  * enforcement authorities across all three countries will take part in joint training initiatives to combat spam;
  * international solutions and strengthening capabilities will be developed to trace and convict spammers; and
  * cross border enforcement against spammers will take effect."

United Kingdom

UK spam is covered by a set of regulations. The Directive on Privacy and Electronic Communications (2002/58) was adopted by the European Commission and it was implemented in the United Kingdom via the Privacy and Electronic Communications (EC Directive) Regulations 2003 which came into force on December 11, 2003. The Regulations prohibit the sending of unsolicited emails for direct marketing purposes without the recipient's prior consent (opt-in) unless one of three exemptions applies:

(a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;
(b) the direct marketing is in respect of that person's similar products and services only; and
(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication. (Regulation 22(3))

The sender of all marketing messages must not conceal his or her identity and must provide a valid address for opt-out requests.

The Information Commissioner is responsible for enforcing the regulations, which is one of the major criticisms of the Act outlined by Munir as the Commissioner is "overworked and under-resourced." Munir also criticises the low £5,000 fine for breaking the Regulations and its application. Spam to private email addresses is prohibited but it is permissible to send spam to the employees of businesses. Regulation 22 (electronic mail) applies only to transmissions to individual subscribers (the term "individual" means "a living individual" and includes "an unincorporated body of such individuals"). Motion concludes his summary of the regulations: "A laudable effort all round on the part of the UK Government, but it is doubtful that any of this is going to make much difference in isolation."

United States

The United States "Controlling the Assault of Non-Solicited Pornography and Marketing Act," otherwise known as the CAN-SPAM Act 2004 took effect as from 1 Jan 2004 and only applies to spam messages which are commercial. Section 2 of the Act outlines twelve Congressional findings and policy, the first of which states: "Electronic mail has become an extremely important and popular means of communication, relied on by millions of Americans on a daily basis for personal and commercial purposes. Its low cost and global reach make it extremely convenient and efficient, and offer unique opportunities for the development and growth of frictionless commerce."

The Act defines "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." Excluded are "transactional or relationship messages," which facilitate existing commercial exchanges or provide information necessary to existing commercial relationships.

A major criticism of the Act is that it is an opt-out regime. The recipient must be told that he or she will receive messages unless advice is received they do not want them. Commercial messages must contain opt-out provisions and the sender's physical address. Some recipients would take the view that spammers include an opt-out to validate e-mail addresses which could mean more e-mails.

The Act prohibits the use of deceptive subject lines and false headers. In the case of unsolicited email, the marketer must label the email as an advertisement by ADV or other comparable identifier in the subject line. To amount to actionable spam there must be multiple unsolicited commercial emails that do not comply with the provisions of the Act.

The CAN-SPAM Act provides criminal penalties and unlike the UK Regulations the penalties are steep (fines up to 2 million). Zhang notes that some critics consider the possible penalties are disproportionate to the crime.

The CAN-SPAM Act does not allow a private right of action. Parker Baxter asserts that the theory behind allowing an individual private right of action against spammers in small claims court is that a rash of small lawsuits can create significant costs for the spammer that are normally shifted to the recipient of an unsolicited communication and can thereby cause a reduction in the amount of spam sent.

Subsection 12 of the Congressional findings and policy states: "Many States have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but these statutes impose different standards and requirements. As a result, they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail, in part because,

since an electronic mail address does not specify a geographic location, it can be extremely difficult for law-abiding businesses to know with which of these disparate statutes they are required to comply." Spam regulation has been removed from state regulation to the federal government and in some cases imposes a softer regime.

Australia

The underlying principle of consent was emphasised on the Second Reading by the Minister for Communications, Information Technology & the Arts -

"The Spam Bill 2003 has as its cornerstone the principle of consent. Has the recipient asked for this communication—which constitutes explicit consent—or is there implicit consent? Implicit consent would exist where there is an existing business or other relationship. Drafting the bill has been a delicate balancing act. We must balance the legitimate needs of business and the concerns of the community."

The Spam Act is divided into 6 Parts – five of which contain a section headed "simplified outline."

Part 1 Introduction s3: Simplified outline

It states: The following is a simplified outline of this Act:

> This Act sets up a scheme for regulating commercial e-mail and other types of commercial electronic messages.
>
> - Unsolicited commercial electronic messages must not be sent.
> - Commercial electronic messages must include information about the individual or organisation who authorised the sending of the message.
> - Commercial electronic messages must contain a functional unsubscribe facility.
> - Address-harvesting software must not be supplied, acquired or used.
> - An electronic address list produced using address-harvesting software must not be supplied, acquired or used.
> - The main remedies for breaches of this Act are civil penalties and injunctions.

The basic definition of spam is in S6. For the purposes of the Act, it is a commercial electronic message. The Australian Communications Authority (ACA, a government regulator of telecommunications and radiocommunications is responsible for enforcing the Act. Its website defines spam as "unsolicited commercial electronic messages regardless of their content". The provisions relating to consent, allow the sending of legitimate commercial messages. Bulk spamming is covered by penalty provisions rather than in definition.

An electronic message becomes a "commercial electronic message" when it is within one of the listed purposes which include an "offer to supply or sell goods or services, advertise or promote goods and services, or to advertise or promote a supplier or prospective supplier of goods and services."

A commercial electronic message that has an Australian link, is prohibited unless the "relevant electronic account holder" to whom the message was sent consented, or there is a mistake by the sender, or the message is a "designated commercial electronic message."

The Act is much wider in application than either the UK Regulations or the CAN-SPAM Act. It covers all forms of electronic messaging such as mobile text messaging (SMS), multimedia messaging service (MMS) and instant messaging. Fax and voice calls are not covered. The Australian Consumers' Association consider that the Act should cover unsolicited marketing phone calls.

The practical guide for business put out by the Government lists three key steps to provide a clear explanation of the legislation's requirements:

"1 Consent Only send commercial electronic messages with the addressee's consent – either express or inferred consent."

2 Identity Include clear and accurate information about the person or business that is responsible for sending the commercial electronic message.

3 Unsubscribe Ensure that a functional facility is included in all your commercial electronic messages. Deal with unsubscribe requests promptly."

There are a number of exceptions for "designated commercial electronic messages" as defined in Sch.1. They must comply with s.17 and include information about the institution or organisation which authorised the sending of the message. Schedule 1, cll.2 and 3 outline the range of messages and list a number of bodies that are authorised such as government agencies, registered political parties, religious organisations, charities and educational institutions. Also excluded from the operation of the Act are purely factual messages but the sender must include accurate contact details of the message's originator (Sch.1, cl.2). Likewise if the relevant electronic account-holder consented to the sending of the message (Sch.2).

"Consent" means express consent; or consent that can reasonably be inferred from the conduct, and the business and other relationships, of the individual or organisation concerned.

The range of penalties is wide and it will depend on the history of the offender and whether or nor it is a body corporate or an individual as to the penalty imposed. ACA can issue infringement notices or penalties can be imposed by the courts. Under the former regime, the ACA may choose to issue a formal warning if a person contravenes a

civil penalty provision. Schedule 3 covers infringement notices, the object being to set up a system of infringement notices for contraventions of civil penalty provisions as an alternative to the institution of proceedings in the Federal Court.

Civil penalties are covered in Pt 4. The maximum penalties are substantial and are calculated on an increased scale for repeat offenders. If a business is found to be in breach of the Spam Act a penalty of up to $220,000 for a single day's contraventions may be imposed. If, subsequently, the business contravenes the same provision, the possible penalty is up to $1.1 million. For an individual first time offender the maximum is $44,000 per day and for a repeat offender $220,000 per day.

Injunctions may be granted in relation to contraventions of civil penalty provisions. The ACA is presently taking action against Clarity1 Pty Ltd of East Perth and its managing director, Mr Wayne Mansfield, and are seeking an interim injunction against the parties to be in force until the hearing because of the scale of the alleged breaches. It is alleged that the parties sent out at least 56 million commercial emails in twelve months after the Spam Act 2003 commenced in April 2004. Clarity1, which also uses the trading names Business Seminars Australia and the Maverick Partnership harvested some of the email addresses to which emails have been sent.

The ACA has been successful against a car company that advertised using text messages. Carsales.com .au was fined $6600.

The ACA has been active in enforcing the Act by educating Australian businesses and consumers and it has been involved in joint action internationally in combating spam. Not only has it signed the M of U noted above with the USA and the UK to counter spam but it has also signed a joint statement with the Thai government on telecommunications and information technology.

On 1 December 2004 , the Acting ACA Chairman, Allan Horsley, in a media release advised the anti-spam initiative with Pacific Internet and the software development company Spammatters. They are conducting a “world first” spam reporting system which enables Pacific Internet customers to report spam they receive via a number of methods including a plug-in to Microsoft Outlook and a web interface.

"When they receive spam, these customers will be able to use the software to forward it directly to the ACA's forensics database system for collection, research, analysis and action," Mr Horsley said. "The database system automatically extracts relevant information from the spam that may help the ACA to track down spammers. This information can be used as evidence in court because the database also saves the spam message with the header and body intact. This enhances its usefulness as legal proof. "

"The database system reduces the need for manual spam investigations and is able to process and analyse very large amounts of spam."

Summary of the NZ Unsolicited Electronic Messages Bill compared to the Australian Spam Act 2003.

Clause 3 sets out that the purposes of the Act are to –

(a) prohibit commercial electronic messages with a New Zealand link from being sent to people who have not given their prior consent to receiving those messages; and

(b) prohibit promotional electronic messages with a New Zealand link from being sent to a person who has withdrawn consent to receiving those messages; and

(c) require all commercial and promotional electronic messages to include accurate information about the person who authorised the sending of the message; and

(d) require all commercial and promotional electronic messages to contain a functional unsubscribe facility; and

(e) prohibit address-harvesting software and any electronic address list produced using that software from being supplied or acquired for use, or being used, in connection with sending unsolicited commercial electronic messages, or promotional electronic messages, in contravention of the Act.

The proposed Act will apply to marketing and promotional electronic messages whereas the Australian Act covers all commercial messages relating to an offer of goods or services, for example, quotes and invoices.

Clause 6 defines commercial electronic message. It means an electronic message that has, as its primary purpose,-

(i) marketing or promoting-
- (A) goods; or
- (B) services; or
- (C) land; or
- (D) an interest in land; or
- (E) a business or investment opportunity; or

(ii) assisting or enabling a person to obtain dishonestly a financial advantage or gain from another person; but…the section then lists (i) – (viii) what an electronic message does not include – such as, a quote or estimate for the supply of goods or services. (viii) is a mopping up subsection. It does not include an electronic message that has any other purpose set out in the regulations.

A promotional electronic message means an electronic message-

(a) that is not a commercial electronic message; and

(b) that has, as its primary purpose, the promotion of marketing of an organisation, or its aims or ideals.

The Bill follows the Australian approach with regard to bulk spamming. It is not included in the definition but is relevant in terms of penalties.

Both the opt-in and opt-out approaches are utilised. The opt-in approach applies to unsolicited commercial electronic messages that have a New Zealand link. The opt-in approach involves a higher standard. The messages can only be sent if the recipient has consented to receiving them. This can be express or inferred from the conduct and the business and other relationships of the person concerned and any other circumstances that may be specified in regulations. Consent is deemed to have been given when an electronic address has been conspicuously published by a person in a business or official capacity and it is not accompanied by a statement to the effect that the relevant address-holder does not want to receive unsolicited electronic messages. The message sent must be relevant to the business, role, functions or duties of the person in a business or official capacity. Opt-out applies to promotional electronic messages that have a New Zealand link. They are prohibited from being sent to any person who has opted out of receiving messages. It defines how a person opts out of receiving promotional electronic messages. Commercial electronic messages and promotional electronic messages that have a New Zealand link must clearly and accurately identify the person who authorised the sending of the message; and include accurate information about how the recipient of the message can readily contact the person who authorised the message to be sent. The explanatory note to the Bill states that "Regulations made under the Bill, when it is enacted, may specify further conditions about the information that must be included in commercial electronic messages and promotional electronic messages." In addition a functional unsubscribe facility must be included unless the parties agree otherwise. In line with the Australian Act that facility must be reasonably likely to be functional and valid for at least 30 days after the message is sent.

Covered are all messages generated within New Zealand and all messages sent to a New Zealand email address. This is also in line with the Spam Act as are the provisions relating to prohibiting the supply, acquisition, and the use of address- harvesting software and harvested-address lists in connection with the unlawful sending of messages.

Again only civil remedies apply but for New Zealand the maximum is $200,000 for individuals and $500,000 for bodies corporate.

The Bill provides two defences. They are applicable where the person sent the message by a reasonable mistake of fact or the message was sent without the person's knowledge.

Consumers and users are required to resolve any spam problems with the sender and their Service Provider who in turn is required to refer matters to the government enforcement agency. Individuals cannot complain directly as according to the explanatory note to the Bill this places higher cost on Government and does not resolve issues by ISPs who are best placed to take technical measures in relation to spam originating from overseas. This could be unduly onerous for the ISP provides and it restricts the individual's remedies. The Department of Internal Affairs is responsible for enforcing the new legislation, educating consumers, users and businesses and promoting compliance.

Has New Zealand emulated the Australian Spam Act?

The proposed New Zealand legislation is very similar to the Australian Spam Act. Is it better? The title differs as does the ordering of many sections. Likewise different words are used although essentially their purpose is the same, for example the Australian infringements are called contraventions. It is difficult to understand the reasoning behind some of the changes, particularly in view of the MoU and the frequent aspirations of a single economic market. A parallel development occurred with the New Zealand Commerce Act which was introduced after the Australian legislation but it is very similar. Some sections were reworded and the rewordings have proved to be detrimental. It is apparent that a lot of the changes in the Unsolicited Electronic Messages Bill are cosmetic only and seem to be of little benefit in the fight against spam.

The New Zealand Bill does include standard search and seizure provisions. Similar provisions were included in the Australian Telecommunications Act via the Spam (Consequential Amendments) Act 2003.

The New Zealand Government has had the benefit of a number of legislative models and their critics but has not taken advantage of the opportunity to make legislative innovations in the spam area.

Chetwin and Clarke suggest that a unique role for the law lies in requiring the deployment of technical defences against spam and in imposing heavy penalties not only for non-technical misdemeanours (such as buying and selling address lists) but also for operating email systems that lack these required technical defences. An example suggested is legislating that all mail-systems must implement technical barriers of a certain efficacy against spoofing.

Ryan Hamlin, the head of Microsoft's Technology Care and Safety Group has criticized the Bill as being "two broad" and feared for the future of email marketing. He advocates the American opt-out approach which New Zealand rejected as being too weak. In Hamlin's view, the Bill as it is could prevent businesses from sending out emails to people who had been customers. Labelling of advertising emails, for example by ADV in the subject line, would have the advantage that recipients could filter out the unwanted messages.

Conclusion

The Congressional Findings and policy in the CAN-SPAM Act summarised the problem with legislation which has been echoed in all other jurisdictions:

"(12) The problems associated with the rapid growth and abuse of unsolicited commercial electronic mail cannot be solved by Federal legislation alone. The development and adoption of technological approaches and the pursuit of

cooperative efforts with other countries will be necessary as well."

Regardless of the jurisdiction discussed there are critics of the legislation in force or the proposed legislation. There is no easy answer. The Memorandum of Understanding on 2 July 2004 between the US Federal Trade Commission, the UK Department of Trade & Industry, the UK Information Commissioner and UK Office of Fair Trading and the Australian Competition & Consumer Commission (ACCC), the Australian Communications Authority (ACA) for mutual assistance in the enforcement of spam laws is a major step in the right direction. The ACA Acting Chairman acknowledged that on its own it will not solve the problem but it is an important start.

It is essential that New Zealand move quickly to pass legislation so that it can participate in any future international agreements and that spammers do not see it as a safe haven for transmitting spam. New Zealand has utilised the Australian Act as a model. The question remains why the minor unimportant changes which seem to be of little benefit? An international framework of legislation and law enforcement is required.

References

[1] Alongi, E.A. "Has the US Canned Spam?" 46 *Ariz L Rev*, 2004, 263.

[2] Australian Department of Communications, Information Technology and the Arts website:http://www.dcita.gov.au/ie/spam_home (last visited 12 Aug 2005)

[3] Caslon Analytics profile: Australian & NZ spam regulation website: http://www.caslon.com.au/anzspamprofile.htm (last visited 12 Aug. 2005)

[4] Cheng , T.S.L. "Recent international attempts to can Spam," .*C.L. S.R.* 2004, 20(6), 472-9.

[5] Chetwin, M. & Clarke, B. "The relative effectiveness of technology v legislation in curtailing spam," *C.T.L.R.* 2004, 10 (8), 192-197.

[6] Davidson, S. & Griffin, M.K. "The US tackles spam," *C.T.L.R.* 2005, 11(1) 1-3.

[7] Fritzemeyer, W. & Law, A. "The CAN-SPAM Act– analysed from a European perspective," *C.T.L.R.* 2005, 11(3), 81-90.

[8] Hamel, A. "Will the CAN-SPAM Act of 2003 finally put a lid on unsolicited-e-mail," 39 *New. Eng. L. Rev*. 961-1001.

[9] Krotz, J.L. "The 11th commandment :thou shalt not spam," at http://www.microsoft.com/smallbusiness/resources/marketing/online_marketing/the_11th_commandment_thou_shall_not_spam.mspx (last visited 12 Aug 2005)

[10] Motion, P. "Spam Banned," *C.T.L.R.*, 2004, 77-79.

[11] Munir, A.B. "Unsolicited Commercial Email Implementing the EU Directive," *CTLR* 2004, 10(5), 105-110.

[12] New Zealand link to media release and copy of the Unsolicited Electronic Messages Bill http://www.beehive.govt.nz/Minister.aspx?MinisterID=70 (last visited 12 Aug 2005)

[13] Parker Baxter, W. "Has spam been canned? Consumers, Marketers and the making of the CAN-SPAM Act of 2003," 8 *N.Y.U.J. Legis & Pub. Pol'y*. 163.

[14] Pullar-Strecker, T. "Microsoft find spam bill hard to swallow," Dominion Post, 22 August 2005.

[15] Sorkin, D.E. - Sorkin's website – contains legislation from various countries and it includes references to over 100 American articles and notes. http://www.spamlaws.com/ (last visited 12 Aug 2005)

[16] Sorkin, D.E. "Spam legislation in the United States," 22 J. Marshall J. Computer & Info. L. 3 (2003).

[17] UK Department of Trade and Industry website http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html (last visited 12 Aug 2005)

[18] UK Information Commissioner's Office website: http://www.informationcommissioner.gov.uk/eventual.aspx?id=5801 (last visited 12 Aug 2005)

[19] Zhang, L. "The CAN-SPAM Act: an insufficient response to the growing spam problem," 20 *Berkeley Tech LJ*, 301-328.