MinterEllisonRuddWatts
LAWYERS

SPAM AND PRIVACY ISSUES

Spam for Breakfast, Lunch and Dinner:
What will the Unsolicited Electronic Messages Bill do for Privacy?

30 March 2006

Graeme Crombie
Senior Associate
Minter Ellison Rudd Watts

1. Introduction

1.1 Spam is a major problem for all technology users. While it is hard to pin down exactly what is spam, we all known it when we see it. The problem is how to stop spam.

1.2 This paper looks at what spam is, how the Privacy Act helps the fight against spam, its shortcomings and how the Unsolicited Electronic Messages Bill is going to impact the spam problem.

2. Spam

What is Spam?

2.1 Spam is a major annoyance to almost all email account holders. Spam is most frequently found in email inboxes, but can be sent via other electronic mediums such as SMS messages. While most people can identify what spam is when it arrives in their inbox, it is a difficult term to define.

2.2 In my view, the key to defining spam is to look at the common characteristics. Spam is:

(a) always unsolicited;

(b) usually of a commercial or promotional nature;

(c) typically sent to numerous addresses;

(d) generally such that it is impossible to identify who sent the message;

(e) often the same message received a number of times; and

(f) often characterised by fraudulent schemes or offensive information or offers.

2.3 Information Technology Minister, David Cunliffe, at the Unsolicited Electronic Messages Bill's first reading in Parliament on 15 December 2005, said that spam has gone from being a "minor nuisance to becoming a significant social and economic issue". He went on to say that "It is a drain on the business and personal productivity of New Zealanders".

2.4 He also referred to a recent (mid 2005) report by an anti-spam software company, which suggest that at least 65% of all emails received in New Zealand are spam, and over 90% of these originate from overseas spammers. In 2001 only 8% of emails were spam (see Ministry of Economic Development Legislating Against Spam Discussion Paper (Wellington, 2004)).

Some Problems Caused By Spam

2.5 Spam causes a number of problems, the first of which is annoyance. However other issues include offensive content, deceptive or fraudulent practices and breach of privacy. These problems turn the spam issue into a major national and international problem which needs to be addressed.

2.6 A major reason why the sending of unsolicited emails has become such a huge problem is due to the minimal cost of sending an email. While the cost of printing and distributing flyers through mail boxes can be expensive and time consuming, the cost of sending a bulk email to thousands of people is virtually nothing. The cost is almost solely borne by the recipient of the message by way of downloading time and computer space. A 2004 EU study estimated that the worldwide cost of spam to internet subscribers was in the vicinity of EUR 10b per year (NZ Herald 16/7/2004).

2.7 While spam can include unsolicited messages sent via SMS message, this is yet to be a major problem for New Zealanders due to the costs involved in sending an SMS message. However, it is possible that in the future, cell phones will also be targeted.

2.8 Spam sometimes involves attachments or large files containing images, which can overload a system causing it to crash. Worse still, the attachment or email itself may contain a virus. This can cause major problems by disrupting communications both privately and commercially.

2.9 Internet Service Providers (**ISP's**) have already put in place systems designed to stop spam getting through. The problem with these is that they are often not effective in stopping many spam emails. Frequently the spammer uses tricks to get their messages through, such as misleading subject lines and spelling mistakes. Furthermore these systems can also stop desired emails getting through. This is particularly a problem if the recipient is expecting an email in the form of a newsletter or company mail-out which is sent to numerous people.

2.10 A further problem with spam is the privacy issues it raises. Many people legitimately feel that their privacy has been invaded when they receive spam. For instance, sometimes the recipients of emails can see the email addresses of all other recipients. How privacy relates to spam is discussed further in this paper.

3. The Privacy Act 1993

Application of the Privacy Act

3.1 The Privacy Act was enacted to deal with situations where personal information (eg email addresses and cell phone numbers) is given or collected by an agency for a particular purpose. The Privacy Act is designed to ensure that information collected is not used for other purposes or disclosed to other people without the subject's consent. The Privacy Act sets out 12 Information Privacy Principles (**Privacy Principles**) which deal with the collection, holding, use and disclosure of personal information.

3.2 The relevant Privacy Principles are 2, 3, 4, 10 and 11. They provide as follows:

(a) Privacy Principle 2 requires an agency to collect information directly from the subject. In other words, an agency cannot collect information from other

agencies. However, an agency can collect information if it is publicly available, a point I shall return to later.

(b) Privacy Principle 3 requires that the subject is aware that the information is being collected, the purpose of the collection, the intended recipients, the name and address of the agency collecting and holding the information and the subject's right to access and correct their personal information. This requirement is designed to ensure the subject knows for what purpose their information is to be used.

(c) Privacy Principle 4 provides that the agency collecting personal information must not collect information by any unlawful means, or means that are unfair or intrusive in the circumstances. This means the agency cannot trick a person into consenting to the use of their information for unrelated purposes.

(d) Privacy Principle 10 provides that personal information is not to be used for any other purpose other than that purpose for which it was collected, subject to a number of exceptions. This prohibits an agency sending messages to an email address for purposes which were not consented to at the time the address was collected, such as marketing or promotional reasons if these were not specifically agreed upon.

(e) Privacy Principle 11 controls the disclosure of personal information and prohibits this unless one of the exceptions is made out. This means that an agency cannot pass personal information on to any third party unless that is directly related to the purpose for which the information was originally obtained.

3.3 Quite clearly the Privacy Principles ensures that a legitimate business that has collected personal information will not be able to spam or be involved in spamming activities. If it did, a breach would be quite easy to establish and would likely present a serious publicity problem for the business.

3.4 Is the Privacy Act enough to stop spam by itself? In my view no, as spam is not something that typically comes from a legitimate business.

Limitations of the Privacy Act

3.5 There are three principal limitations on the effectiveness of the Privacy Act stopping spam. They are:

(a) scope of the Privacy Act;

(b) public availability of personal information;

(c) off-shore nature of spam;

(d) remedies available under the Privacy Act.

3.6 The first relates to the extent of coverage under the Privacy Act. The Privacy Act only applies to the personal information of natural persons. It does not apply to the information (eg email addresses) of a company or a corporation. Thus, an email address like info@corporation.co.nz can be used by spammers without any consequences under the Privacy Act.

3.7 The second concerns the availability of individual's email addresses. If an individual's email address is publicly available, eg by being on a company's website, then a spammer can collect that information without needing to collect it directly from the individual (see exception 2(2)(a) to Privacy Principle 2). The spammer can also use

that information for any purpose and disclose it to anyone else as it sees fit (see exception (a) to Privacy Principles 10 and 11). Again, spamming in this instance does not breach the Privacy Act.

3.8 Related to this point is the fact that spammers also have techniques to guess email addresses. If an email address is guessed no information has been collected from anywhere and so the Privacy Act has no application. If the recipient of the spam then does something to validate the email address (ie replies, so that the spammer knows it is correct) any collection of information will be for the purposes of further spamming and so permitted by the Privacy Act!

3.9 The third is the international nature of spam. As already mentioned, over 90% of spam is estimated to have originated overseas. While the Privacy Act does apply to information held overseas, this is of little consequence if the spammer has no presence in New Zealand. The Privacy Act is effective only at dealing with breaches of privacy which occur in New Zealand.

3.10 The final limitation relates to the remedies available for a breach of privacy. If an individual feels their privacy has been interfered with, that person can lay a complaint to the Privacy Commissioner.

3.11 However, in order to make a complaint it must be shown that the agency breached a Privacy Principle and the Privacy Commissioner is satisfied that this breach has resulted in the complainant:

(a) suffering loss, detriment, damage or injury;

(b) being adversely affected in relation to their rights, benefits, privileges, obligations or interests; or

(c) suffering significant humiliation, loss of dignity, or injury to feelings.

3.12 It is this latter requirement which causes problems when complaining to the Privacy Commissioner about spam. As mentioned earlier, one of the problems with spam is the cost it places on the recipient of the email, the cost to the economy nationally and internationally is huge. However, the individual costs are not so great - while being a nuisance to delete the messages from ones inbox, the damage the recipient suffers is not usually significant. Therefore it is likely to be very difficult to show that an individual has suffered damage. Proceeding via a complaint to the Privacy Commissioner may therefore be ineffective.

4. The Unsolicited Electronic Messages Bill

Main Aims of the Bill

4.1 The Unsolicited Electronic Messages Bill is currently before the Select Committee. Submissions on the Bill close on 31 March 2006.

4.2 The Bill has the main aim of promoting the responsible use of electronic messages. It is also designed to put New Zealand in line with other overseas efforts at regulating spam.

Summary of the Bill

4.3 The Bill is designed to operate a mixed opt-in and opt-out regime. Messages with a primary purpose of marketing and/or promoting goods or services operate on an opt-in basis. These messages are referred to as “commercial electronic messages” and must not be sent to an email address unless that person has specifically consented to

receiving such emails (clause 9). However, if the primary purpose of the message is to promote or market an organisation the opt-out regime applies. These messages are known as "promotional electronic messages" and may be sent until a person notifies the sender that they no longer wish to receive such messages (clause 10).

4.4 The Bill only applies to messages which are sent with a New Zealand link. These emails are required to identify the sender, provide contact details and have an effective unsubscribe function (clauses 11 and 12).

4.5 The Bill also prohibits the use of software which is designed to harvest email addresses and prohibits the use of such address lists.

Key Concepts

4.6 Three key concepts are the definitions of *commercial* and *promotional* electronic messages, *New Zealand links* and what constitutes *consent*.

4.7 *A commercial electronic message* is an electronic message that has, as its primary purpose:

(a) marketing or promoting goods, services, land (including an interest in land) or a business or investment opportunity; or

(b) assisting or enabling a person to obtain dishonestly a financial advantage or gain from another person.

4.8 There are a large number of exclusions to the requirement that a recipient must 'opt in' to receive the message - where it could be considered that consent has been given (for example, where a quote for some work was requested by the recipient). Messages from government agencies or courts are also excluded.

4.9 A *promotional electronic message,* on the other hand, is an electronic message that has, as its primary purpose, the promotion or marketing of an organisation, its aims or ideals. Permitting this type of message has been criticised as legitimising spam (see Electronic Frontiers Australia Inc's submission on the Review of the Australian Spam Act 2003 - EFA is a non-profit national member-based organisation representing Internet users concerned with on-line rights and freedoms).

4.10 Together, these definitions broadly mirror the *commercial electronic message* concept in the Australian *Spam Act 2003*. However, the split between the two types of message is different to that Act. The reason for the split is a compromise between the 'opt in' and the 'opt out' proponents. Messages that are trying to sell something or defraud the recipient have the higher 'opt in' standard to pass. In contrast, general marketing messages that simply promote an organisation can be sent until consent is withdrawn.

4.11 It is important to bear in mind that a single electronic message can be caught by these prohibitions, not just the bulk emails sent by a "typical" spammer.

4.12 For a message to be prohibited under the Bill, the message must have *a New Zealand link*. This is defined widely so that, in essence, if any party to the message has a connection with New Zealand, the message will be seen as having a New Zealand link.

4.13 Consent can be:

(a) given expressly;

(b) inferred from the conduct and the business and other relationships of the sender and recipient (and any other circumstances that may be specified in regulations);

(c) deemed to have been given where the recipient's electronic address is published conspicuously in a business or official capacity without a statement that the person does not want to receive unsolicited electronic messages *and* the message sent is relevant to the business, role, functions, or duties of the person in a business or official capacity.

4.14 Last year an Australian case looked at what was needed for consent in relation to spam by SMS (the New Zealand Bill would also extend to SMS). In the case Carsales.com sent SMS messages to the cellphone numbers of people advertising cars in the newspaper. The company was prosecuted under the Spam Act. The court held that consent could not be inferred merely because people had published their mobile phone numbers and Carsales.com was fined A$6,600.

4.15 As this case demonstrates, it will be important to consider the circumstances carefully before inferring consent. For example, a one-off transaction is unlikely to make the relationship sufficiently close that consent can be inferred. However, the provision of ongoing advice to clients is probably enough - so sending newsletters to our clients is unlikely to be caught by the Bill.

Obligations when sending electronic messages

4.16 Where commercial and promotional electronic messages are permitted under the Bill, they must comply with a number of criteria. Each message must:

(a) clearly and accurately identify the person who authorised it to be sent;

(b) include accurate information about how the recipient can readily contact the person who authorised the message; and

(c) have a functional unsubscribe facility that allows the recipient to instruct the person who authorised the message that he or she does not wish to receive any further messages.

4.17 These requirements will be easy to comply with as long as companies (and their staff) are aware of them. Companies should also consider building these features into email templates.

Address Harvesting

4.18 The use or acquisition of address harvesting software or lists created by such software is prohibited under the Bill, except where the use or acquisition is not in connection with sending spam. Again, this is in line with the Australian approach.

4.19 It is interesting that this is not a complete prohibition. So the use of address harvesting software will not be illegal unless it is used for sending spam. Legitimate uses of this software may include the collection of email addresses and phone numbers for purely statistical purposes.

Defences

4.20 The Bill contains two defences. These can be relied upon where:

(a) the person sent the message by a reasonable mistake of fact; or

(b) the message was sent without the person's knowledge.

4.21 The second of these will assist the unwary organisation whose servers are being used to send spam (for example, because a hacker has accessed the system or a virus or worm is spreading the email). However, once the organisation knows of that use, it will have to act instantly to shut down the security breach which enabled the spam to be sent.

4.22 The Bill also provides that a service provider does not send a message merely by providing the telecommunications service that enables electronic messages to be sent. This protects ISPs from being deemed to be spammers.

Remedies and enforcement

4.23 The Bill provides a wide range of remedies where a breach occurs. Primary enforcement obligations are expected to be given to the Department of Internal Affairs but the victims of spam and service providers are also specifically given rights to pursue spammers.

4.24 The policy is that ISPs will be the front line for customer complaints with the DIA as an overseer and backstop if need be. The Minister, David Cunliffe, has suggested that this approach will provide incentives for ISPs to obtain and implement the best filtering software to minimise the amount of spam going through their servers.

4.25 The Bill provides for civil, rather than criminal, penalties for breach. The maximum penalty that the High Court may impose is $200,000 for an individual and $500,000 for an organisation. Because it is a civil regime, the standard of proof is the 'balance of probability' rather than the criminal 'beyond reasonable doubt' standard – making enforcement in this difficult area easier.

4.26 The Bill also allows the DIA or the police to apply for a search warrant to search a place or thing.

4.27 The regime ultimately enacted may differ from that in the Bill. The Minister was quoted in the Dominion Post on 22 August 2005 as saying that the issue of enforcement may be revisited at select committee stage, to determine the best approach.

5. Problems with not having Legislation

5.1 While the overwhelming majority of spam originates overseas, there are still advantages to the implementation of national legislation to regulate spam. Some of these advantages include:

(a) Allowing New Zealand spammers to be effectively dealt with under New Zealand laws and not being subject to the requirement that a Privacy Principle must have been breached.

(b) Reducing the likelihood of overseas spammers relocating to New Zealand in the hope it is a "safe-haven" for spammers.

(c) The need for New Zealand to keep in line with other countries which are developing laws designed to deal with Spam. Some of the overseas initiatives include:

(i) The Spam Act 2003 – Australia;

(ii) Controlling the Assault of Non-Solicited Pornographic and Marketing Act 2003 – United States of America;

(iii) Privacy and Electronic Communications Regulations 2003 – United Kingdom.

(d) Enabling a Government agency to work with overseas counterparts to trace major spammers who send their spam to New Zealand.

5.2 The Unsolicited Electronic Messages Bill is designed to be one part of a multi-pronged attack on spam. It is believed that the legislation will be an effective tool alongside other initiatives such as:

(a) Codes of practice;

(b) Industry guidelines;

(c) Technical measures such as spam filters run privately or through ISP's; and

(d) Education campaigns.

5.3 Does anti-spam legislation work? This is often debated. In my view, the results suggest that it does. For instance in Australia, between April 2004 and October 2005, the Australian Communications and Media Authority warned more than 350 Australian business to comply with the Australian legislation, issued fines and infringement notices to 5 and is prosecuting one business (see Department of Communications Information Technology and the Arts Spam Act 2003 Review Issues Paper).

6. Conclusion

6.1 Generally businesses whose email practices abide by the Privacy Act will largely already comply with the provisions of the Unsolicited Electronic Messages Bill.

6.2 The Privacy Act provides some means of redress for those who receive spam messages via a breach of a Privacy Principle. It also acts as a deterrent to businesses and other agencies that collect personal information, from dealing with it in a manner that would breach the Privacy Act. However, by itself it is not effective in dealing with the spam problem.

6.3 The proposed Unsolicited Electronic Messages Bill will however go further than the Privacy Act currently does, and provide another layer of protection and a step closer towards removing spam altogether.

6.4 Ultimately though, protecting your privacy is in your own hands. Some tips:

(a) Make sure you check the privacy policy of any organisation before registering or providing your email address.

(b) Do not display your email address on your website or make it available in publicly available places.

(c) Do not reply to spam – it just validates the email address.