

# Unsolicited Electronic Messages Act

Fiona Campbell, Wigley & Co, Wellington  
exposes problems in the new anti-spam legislation

New Zealand has just got its own anti-spam legislation, the Unsolicited Electronic Messages Act 2007, bringing it into line with the UK, US, Australia and Canada. The wide ambit of the Act means all organisations need to understand its requirements. It is not just aimed at offshore emails peddling fake watches and suspicious pills; it catches all New Zealand internet, email and text commercial messages too.

This article focuses on some of the key points of the Act, but does not cover every issue. At the time of writing no regulations have been made. The Act is well intentioned but has problems. After presenting an overview of how the legislation works, the last section of this article focuses on two of the Select Committee's changes that are particularly awkward.

## OVERVIEW OF THE ACT

The thrust of the Act is that commercial electronic messages (other than faxes and voice calls) are not to be sent without the consent of the recipient or without containing accurate information about the sender and a functional unsubscribe facility.

### Who's affected?

With limited exceptions (for example, for some public sector messages), the new law will impact all organisations that use email, text messages, instant messages, or similar accounts to promote goods and services. The legislation is concerned also with the legitimate promotion and marketing of land, interests in land, and business opportunities as well as the illegitimate fraudulent scams. There is no minimum number of messages required before the Act kicks in. Consequently a wide range of messages are captured from bulk mailouts to one-off emails. Pretty well all organisations are caught one way or another.

### Types of messages caught

The definition of "message" is very broad; it means information in the form of text or writing; data; speech, music, or other sounds; visual images; or any other form. An electronic message is a message sent using a telecommunications service to an electronic address. The legislation specifically refers to the addresses of email, text message, and instant messaging accounts, but it provides for messages sent to "similar accounts" too. So, a post to a MySpace page is likely to be caught as well.

Fax and voice calls are expressly excluded from the ambit of the legislation. This makes sense because, for the most part, the cost of making such transmissions undermines the business model upon which traditional email spam is based. Voice calls made using voice over internet protocol (VOIP),

eg Skype, are also excluded. Given that the business case for spam-by-VOIP must surely be close to that for spam-by-email, it is odd that the Act rules these out.

Commercial electronic messages are ones that:

- market or promote goods, services, land, interests in land, or business or investment opportunities;
- assist or enable the obtaining of a dishonest financial advantage or gain from another person; or
- provide a link or directs a recipient to a message that does anything listed above.

The sting is in the third provision, but more about that in the last section of this article.

Eight types of messages that might otherwise be categorised as commercial electronic messages have been specifically excluded from the definition of commercial electronic message:

- quotes and estimates;
- messages that confirm a transaction already entered into; and
- messages that provide information about goods or services offered or supplied by a government body.

The latter does not extend to local government.

From this point onwards commercial electronic messages will be referred to simply as "commercial messages".

## Three requirements for commercial messages

### (1) The consent requirement

You must have the consent of the recipient before sending any commercial messages. Consent comes in three flavours: express, inferred, and deemed. Express consent is straightforward, but be wary of hiding the consent provision in the fine print.

Consent may be inferred on the basis of the conduct and the business and other relationships of the persons concerned. Many organisations will look longingly at this category of consent but they have got to be able to point to conduct of the recipient or an actual relationship before they can rely on this. For those with existing mailing lists, the mere fact that a recipient has not availed itself of an unsubscribe function will not be sufficient basis to infer consent after the Act comes into force.

Persons are deemed to have given consent to receive messages related to their business or official capacities when they publish addresses without a statement saying they do not want to receive commercial messages. For example, an IT manager who hands over a business card at a networking event can expect to get emails promoting computer systems but not cat food.

### (2) *The accurate information requirement*

Every commercial message must now include accurate information that identifies the sender and that allows the recipient to contact the sender. This is easily achieved with emails. The requirement is more problematic in the context of text messages and instant messaging. In the case of text messages, space is at a premium so it will be a stretch to get all the information in. In the case of instant messaging, it mandates the use of an accurate username (eg "KilbirnieRenovationsLtd" not "crazyfrog23"), unless the full name is put into the body of the message.

There is no provision under the Act to contract out of this requirement. For most businesses who want to promote their corporate identity and contact details this will not be a problem.

### (3) *The functional unsubscribe requirement*

Every commercial message must contain a functional unsubscribe facility, expressed in a clear and conspicuous manner.

This requirement calls for at least an explicit reference to unsubscribing, for example, "Reply to the email with 'unsubscribe' in the subject line if you no longer wish to receive emails from us." It will not be enough to rely on the fact that a recipient could choose to hit reply and ask to be removed.

The UK Advertising Standards Authority has already addressed this issue in the February 2007 decision against World Networks Ltd. World Networks sent a text to Orange customers offering them a new phone and finished the message with the words "Opt-out available". Employing a similar standard to the New Zealand legislation, the ASA held that the words failed to meet the requirements for an unsubscribe function.

### **When does it take effect?**

There is a six-month transition period from the date of royal assent, so the Act will come into force in early September 2007. The challenge for many organisations will be to make their current and future mailing lists compliant with the new regime in time.

The Australian Spam Act 2003 seems to have been the model for the drafters of the New Zealand legislation. Despite the departures that our regime takes from that model, advisers will get useful assistance from the materials developed for Australian businesses. See the "Spam Act 2003: A practical guide for business", Australian Communications and Media Authority, [www.acma.gov.au/webwr/consumer\\_info/frequently\\_asked\\_questions/spam\\_business\\_practical\\_guide.pdf](http://www.acma.gov.au/webwr/consumer_info/frequently_asked_questions/spam_business_practical_guide.pdf).

### **What are the penalties?**

The Act employs a civil liability regime. The Department of Internal Affairs has an array of enforcement options available to it. It can take action itself using formal warnings, civil infringement notices (that may specify fines up to \$2000), or by taking enforceable undertakings. Alternatively, DIA can go through the Courts to seek injunctions, and apply for

pecuniary penalties, compensation or damages. The first set of options anticipates that there will be a number of first offenders who merely warrant a slap on the wrist with a wet bus ticket.

Any person affected by a breach of the Act may seek an injunction, compensation or damages. Individual recipients, employers, and ISPs will all be in a position to take advantage of this provision.

### **SELECT COMMITTEE CHANGES CAUSE PROBLEMS**

The Select Committee recommended a number of changes be made to the Bill:

- ISPs no longer play a role under the legislation. Complaints may be made directly to DIA.
- The use of the unsubscribe facility must be at no cost. This may be a headache for text-

marketing campaigns.

- "Promotional messages", with their "opt-out" regime, have gone. The bifurcated approach to commercial and promotional messages was rightly considered too confusing.
- The "primary purpose" qualifier has been deleted.
- The definition of "commercial electronic message" has been extended.

The combined effect of these last two changes makes the scope of the legislation exceptionally wide. Many non-commercial (in the normal sense) emails will unwittingly be caught.

### **Two changes cause one big problem**

In an effort to simplify the legislation, the Select Committee recommended that the primary purpose qualifier be deleted from the Bill. Previously, the definition of commercial electronic message had read: "... commercial electronic message means an electronic message that has as its primary purpose marketing or promoting goods or services ..." This was thought to introduce unnecessary confusion into the regime.

We recommend removing from clause 6 the requirement that marketing or promoting goods or services must be the primary purpose of the message. We are concerned that the requirement as introduced could lead to debate over exactly what constitutes the primary purpose of a message, and could inadvertently exempt some messages that are commercial in nature but can be interpreted as having another primary purpose. We consider the bill should catch all messages that seek to market or promote goods and services, and that our amendment provides clarity on the matter. (Select Committee report, p 4)

While the simplification of the legislation is a laudable aim, it creates a very odd result when considered against another of the Select Committee's changes: that "commercial electronic messages" should include non-commercial messages that contain a link to a commercial message.

*Continued on page 134*

---

## **The challenge for many organisations will be to make their current and future mailing lists compliant with the new regime in time.**

---

Old Beijing Twister". However, foreign franchisors must balance this strategy by also marketing the distinctiveness of their product when entering China.

calculated risk assessment based on a franchisor's financial resource. On the other hand, franchisors that delay entering China face the risk of being left behind. □

*Continued from page 131*

We recommend amending the definition of "commercial electronic message" in clause 6 to capture messages that seek to market goods or services merely by providing links to other websites or messages. We consider it could be open to debate whether or not such messages have marketing or promoting as their purpose, and therefore whether or not they are included in the definition as introduced. We consider this amendment necessary to ensure the bill's provisions extend to messages of this nature. (Select Committee report, p 3)

The Select Committee's reasoning is strong here. Emails we commonly think of as spam may provide nothing more than a passage of gobbledygook accompanied by a link to a website where the real promotion or fraud lies. Such emails should be within the ambit of the legislation.

The problem posed by the combination of these two changes is that, without a primary purpose qualifier, any such link renders a message "commercial". A vast number of corporate emails are sent every day with a link to the company website at the bottom of the email. The company website will invariably market and promote that company's goods and services, and thus the ordinary email is rendered commercial under the Act. Links to company websites elevate the most mundane emails to the status of commercial messages.

#### **Can it be fixed?**

It is unlikely that the Select Committee intended this result, but it can be remedied fairly easily. The Act provides for

certain electronic messages to be excluded from the ambit of the Act through the making of regulations. Regulations could fix this problem by adopting the US approach just in relation to links within otherwise non-commercial messages. The equivalent US legislation states:

The inclusion of a reference to a commercial entity or a link to the website of a commercial entity in an electronic mail message does not, by itself, cause such message to be treated as a commercial electronic mail message for purposes of this Act if the contents or circumstances of the message indicate a primary purpose other than commercial advertisement or promotion of a commercial product or service. (15 USC § 7702(2)(D))

Such an approach would not overly frustrate the Select Committee's purposes in removing the qualifier in the first place. However, given the very wide ambit of the legislation, and the fact that most "true" spam comes from offshore anyway, perhaps Parliament should re-introduce the qualifier for all messages.

#### **CONCLUSION**

Start transitioning your organisation's practices and existing databases to the new regime now! Keep an eye out for any regulations that are made; these may make life a lot simpler for message senders. Finally, remember that the Privacy Act 1993 still applies. □