



The New "Anti Spam" Law – Is your Business Ready?

Sean Lynch, IT/Telecommunications partner at Hesketh Henry, provides an overview of this new law as well as a preparatory compliance checklist.

Introduction

The Unsolicited Electronic Messages Act 2007 ("Act") comes into force on 5 September 2007. Although not restricted to businesses engaged in direct marketing to electronic addresses, such businesses are likely to be most affected by this new law. These businesses must now prepare for, and learn how to best 'live with', the Act or risk incurring substantial financial or other penalties for breach.

The Act is the government's answer to combating spam. Spam is not only a nuisance (as most of us know), it is also a sizeable cost not only to our economy but to other economies world wide. As most spam originates from off-shore, the Act is unlikely to be the antidote many of us would like, but the government believes it will assist with international efforts to combat spam. There is a risk though that in attempting to stem the tide of unwanted sex and drug related emails, ordinary New Zealand businesses who are trying to get ahead will be penalised.

What is covered by the Act?

The Act primarily targets and restricts the sending of "*commercial electronic messages*". "*Electronic message*" is broadly defined to capture any message sent using a telecommunications service to an electronic address (i.e. email address, phone account, instant messaging account etc). Standard voice calls and faxed messages are excluded from the Act.

An "*electronic message*" becomes a "*commercial electronic message*" if it "*markets or promotes goods, services, land or a business opportunity*" (as the main limb to a three part definition). The Act contains a list of certain well defined exceptions but these will only assist in specific factual contexts (e.g. providing a quote or estimate for the supply of goods or services if that quote or estimate was requested by the recipient). The definition of "*commercial electronic message*" is somewhat problematic and is yet to be tested by the courts and refined. For example, would it cover an email that said "*to learn more about [XYZ brand], click the link below...*". The assumption at this stage is that it would be caught by the Act if the effect of the message is that it is indirectly promoting goods or services.

The Act also:

- requires that each "*commercial electronic message*" contains a "*functional unsubscribe facility*" and also clearly identifies the person or organisation who authorised the sending of the message, and includes accurate information about how the recipient can readily contact that person; and
- prohibits the use of address harvesting software, being software which is capable of searching the internet for electronic addresses, and collecting and organising those addresses.

Section 9 of the Act prohibits the sending of "*commercial electronic messages*" to any person who has not consented to receiving that message. So, what constitutes consent?

What amounts to recipient consent?

The consent of a recipient to receiving a "*commercial electronic message*" can either be:

- **Express** – that is, actually communicated by the recipient e.g. by written or electronic means;
- **Inferred** – from, say, a course of dealing with the recipient; or
- **Deemed** – from the conspicuous publication of an electronic address for business purposes without stating that unsolicited messages are not to be sent.

What should your Business do to comply with the Act?

The key issue is whether you can produce satisfactory evidence, if required (and the onus will be on you), which confirms that the consent of each recipient was obtained *before* the relevant "*commercial electronic message*" was sent.

You may say that "*consent must be inferred because we have been sending out emails to our customer database for 3+ years now...*" - but what about your new customers? or the customers you engaged with once 2 years ago? And what if you do have express terms of trade with your customers but these fail to cover this particular issue? Might it then be inferred that you do not have the required consent at all?

The preferred form of consent by far is express consent. This is because the position is then clear beyond doubt. For many businesses, the best way to obtain express consent will be through their terms of trade with their customers. These terms should contain appropriate provisions aimed at ensuring compliance as far as possible with the Act as well as other laws as required. However, terms of trade are only put in place with your customers, and the "consent" of any other recipient of a "*commercial electronic message*" will still need to be obtained. Depending on the 'channels to market' for your business, there may be a number of ways in which recipient consent can be obtained which satisfies the Act.

The above points are relevant for your new and potential customers – but what about your existing customer database? You will need to dissect your current database to see if each person falls within one of the categories of consent listed above. If in doubt, the prudent step is to take the opportunity now to update your terms of trade to include "express consent" wording along with any other updated legal requirements (of which there are likely to be a few in any event).

What are the Penalties for Non Compliance?

If found to be in breach, the penalty could range from a formal warning through to a \$200,000 fine for individuals or a \$500,000 fine for organisations, or an injunction.

A Checklist for Consideration

Below is a basic checklist to consider:

Do you have a customer database? If so, then...

Do you send electronic communications to contacts in your database? If so, then...

What is the purpose or effect of these communications? (i.e. to market or promote your goods and services?)? If so, then...

Do you have the consent (express, inferred or deemed as described above) of each contact in your database to the ongoing receipt of such messages? If not, then you are likely to be in breach of the Act if you send "*commercial electronic messages*" to these people;

Have your terms of trade been reviewed to ensure that express consent has been obtained with regard to "*commercial electronic messages*" being sent to your new customer contacts?;

Do your "*commercial electronic messages*" contain:

clear and accurate details of the identity and contact details of the sender; and

a functional unsubscribe facility for the recipient to 'opt out' of further emails unless the parties agree otherwise?

Are you confident that address-harvesting software has not been used to compile your 'contacts' database?

Please note that the above is a basic checklist only. Your particular business or set of facts may warrant the consideration of other issues. You should seek advice from a specialist IT lawyer.

Conclusion

Businesses and other organisations involved in email or other 'electronic' direct marketing activities need to understand the requirements of the Act and ensure that they are compliant before 5 September 2007 or risk being in breach of the Act. You should seek advice from a specialist IT lawyer as to what actions are most appropriate for your business or organisation to take.

If you would like to discuss any aspect of this article further, please contact Sean Lynch on (09) 375 8722 or at sean.lynch@heskethhenry.co.nz. This article is for general awareness purposes only and is not intended as legal advice.