The Spam Bill - A precis

Spam

Spam has become costly, disruptive and a potential threat to IT systems. It constitutes an invasion of privacy and its volume has started degrading the infrastructure upon which the information economy relies.

Spam now accounts for half of all worldwide e-mail—with the proportion expected to grow even further. More than half of all spam is estimated to be illegal, misleading or offensive. Just wading through this unwanted and unsolicited flood of correspondence costs business dearly— some estimates put the cost at around $900 per employee per year.

The Australian Government is committed to taking a strong stand against spam and will be moving quickly to respond to ensure that all Australians have the strongest possible protection against spam.

Multi-layered approach

The anti-spam measures to be introduced by the Australian Government will include:

- National legislation, to be enforced by the ACA, banning the sending of commercial electronic messaging without the prior consent of recipients, for example where there is an existing customer-business relationship, or where the person has actively agreed to their address being used for communications (an opt-in regime);
- Civil sanctions for unlawful conduct including financial penalties, an infringement notice scheme and the ability to seek enforceable undertakings and injunctions;
- The requirement for all commercial electronic messaging to contain accurate details of the sender's identity and a functional 'unsubscribe' facility to enable people to opt-out;
- Banning the distribution and use of electronic address 'harvesting' or list-generating software for spamming,
- Banning the distribution and use of harvested address lists, and
- Working together with international organisations to develop global guidelines and cooperative mechanisms to combat the global spam problem.

Legislation and international negotiation are part of the Government's multi-layered approach to combating spam. There will also be an education campaign to raise awareness of the nature of spam and anti-spam measures and to inform individuals and business of their rights and responsibilities when it comes to spam. The development of industry codes of practice, and the pursuit of technical countermeasures will also be encouraged.

Intent of anti-Spam legislation

The Bill is intended to regulate and minimise unsolicited commercial electronic messaging (spam) that is sent from, or received in, Australia by implementing a civil penalties regime which:

- prohibits the sending of commercial electronic messages to end-users in Australia, or from Australia, without the prior consent of the recipient, for example where there is an existing business relationship;
- requires commercial electronic messages to contain accurate sender details;
- requires commercial electronic messages to contain a functional 'unsubscribe' facility; and
- prohibits the sale, supply or use of electronic address harvesting software and lists generated from these in respect of spamming.

Overview

The Spam Bill will define civil penalties for breaches. The legislation will cover electronic messages of a commercial nature that are sent from, or received within, Australia.

Requirements for commercial electronic messages

The requirements of the legislation will include:

- no commercial electronic messaging to be sent without the prior consent of the recipient, for example where there is an existing business relationship, an express agreement, or some other behaviour through which consent may be inferred;
- all commercial electronic messaging to contain, or have access to, accurate sender details; and
- all commercial electronic messaging to contain a functional "unsubscribe" facility which must be acted on within a reasonable timeframe (5 working days), where there is no requirement for ongoing electronic communication due to the nature of the continuing business relationship or a contractual requirement.

Address harvesting software and address lists

The legislation would also prohibit the supply, acquisition or use of software for the purpose of electronic address collection, list generation, or the use of lists generated thereby, for spamming purposes. This is sometimes referred to as "address harvesting" or "dictionary attacks".

Messages partly exempted from the requirements of the legislation (designated commercial electronic messages)

Particular messages, designated commercial electronic messages, will not be required to be sent with the consent of the recipient, or with an included unsubscribe facility. This exception will apply to protect currently accepted government, business and commercial practices, such as government to citizen messages, messages from charities and religious organisations are also excepted, as are messages from educational institutions directed to the households of past or attending students. To be covered by the exemption, the messages in question must be about goods or services directly provided by the body that authorises the sending of the message.

Messages which are of a purely factual nature are also covered by this exemption. The legislation makes it very clear that a factual message can only be accompanied with material that identifies the sender, authoriser or sponsor of the message. The factual component of the message needs to be of such a nature that it would not be considered a commercial electronic message. For example a message describing a particular drug may be simply factual, but if it also includes a link to where it can be bought, it would not be a commercial message and not exempt.

It is permitted to send commercial messages to conspicuously published addresses where the subject is specifically related to the addressees' employment function, but the message must contain an unsubscribe facility.

Enforcing agencies

The Australian Communications Authority (ACA) will have the power to investigate, issue infringement notices and institute proceedings. In some cases they may identify and refer content that could be the subject of other regulatory regimes to other relevant agencies. This could include, for example, child pornography, fraudulent and/or misleading content and "health" related content.

Coverage of the legislation (Australian link)

The regime will address locally originated spam and overseas originated spam directed in-country including, where appropriate, notification and enforcement measures. Investigations will be instigated both on the basis of intelligence developed by the enforcing agency or from public referrals.

Civil sanctions (penalties; infringement notices; injunctions; enforceable undertakings; and formal warnings; compensation; recovery of financial benefit)

Civil sanctions for unlawful conduct will include pecuniary penalties, an infringement notice scheme and the ability to seek enforceable undertakings and injunctions to restrain unlawful conduct. The inclusion of an infringement notice scheme will enable most matters to be dealt with expeditiously and efficiently.

Implementation - 120 days after Royal Assent

To ensure the smooth introduction of the regime, it will be implemented in concert with a significant information program both for industry and the general public before the legislation takes effect. Most provisions of the Act will commence 120 days after the legislation receives Royal Assent. This will ensure that persons or companies that currently unknowingly send spam will be able to correct their behaviour without penalty.

NOIE will coordinate a broad-based educational program focusing on both business and user communities utilising, for example, NetAlert, the IIA, the AIIA and others. This will promote the strategies and technical measures available to individuals and organisations to limit spam exposure including filtering products and "spam interception" services. It will target user communities, focussing on spam-reduction and avoidance strategies, and business communities, focussing on legitimate online marketing.

Industry Codes

The enforcing agency will also facilitate and support the development of Industry Codes that complement and are consistent with the legislation. Codes may include (where relevant) features such as:

(a) requiring ISPs to make available to retail clients filtering options from an approved schedule of spam filters;

(b) encouraging members to publicise spam filtering options and products and participate in their evaluation;

(c) requiring code members to ensure their servers are configured appropriately and to take action to close down open relay servers; and

(d) requiring code members to take due care to prevent their facilities being used for the purposes of sending spam.

Code compliance would not prevent spammers from being subject to the penalty provisions of the legislation but could progressively improve public perception of, and confidence in, the sector. Industry associations would be encouraged to deal with infringements by association members arising under their respective codes to the extent that they can.

Future plans - international moves against spam

Although anti-spam legislation will, of itself, have a limited initial impact on spam, it is an important element of the overall multi-layered strategy. By removing Australia as a source of spam, we will be able to promote, facilitate and participate credibly in international efforts on spam.

The initial focus from an enforcement perspective will be on locally sourced spam. Enforcement of the penalties relating to overseas sourced spam will be problematic until international arrangements are in place, but will meanwhile serve as a promotional and educational tool and discourage in-country spammers simply moving offshore. It will also ensure that there is an appropriate enforcement regime in place to deal with overseas spammers as soon as multilateral arrangements are in place.

Contents of the Spam Bill

Commencement [cl.2]
The prohibitions on spamming and attendant civil penalties will come into force 120 days after Royal Assent.

It is intended that the passage of the legislation will be accompanied by a significant information and educational program both for industry and the general public. Commencement of the penalty provisions 120 days after Royal Assent is intended to ensure that people or companies that currently unknowingly spam will be able to correct their behaviour without penalty.

Definitions: relevant electronic account-holder [cl.4]
The relevant electronic account holder is the individual or organisation who either owns, or is responsible for using, the email address, other electronic address or phone number that has sent or received a message.

Electronic messages [cl.5]
Electronic messages include:
- E-mails (electronic mail);
- Instant messaging;
- Text messaging to mobile phones;
- Video messaging to mobile phones; and
- Messages defined in the Regulations.

Electronic messages exclude:
- Voice to voice mobile phone messages;
- Voice to voice landline messages;
- Television broadcasts;
- Radio broadcasts;
- Film; and
- Messages defined in the Regulations.

It is currently planned for the Regulations to exclude Facsimile messages, although if fax spams do become a problem in the future, they could potentially be included in the future.

Commercial electronic messages [cl.6]
A commercial message is a message that is designed to promote the sale of or demand for goods, services, land or financial opportunity whether or not it invites or solicits a response from the recipient. The definition of "commercial electronic message" is quite extensive, in order to cover the variety of commercial activities covered by spam now and in the likely future.

It is intended to include in the legislation a power to specify additional variants of message in the regulations, in case it becomes necessary to clarify the coverage of this section.

There will also be a power to specify kinds of messages that would be considered not to be commercial electronic messages, in case it becomes necessary to clarify the coverage of this section.

Both these powers are intended to be used as a reserve power, used only to:
- ensure that future technologies and variants are covered, and
- remove uncertainties in interpretation.

Designated commercial electronic messages [Schedule 1]
Certain types of commercial messages may be sent regardless of whether or not the recipient has consented to receive them, and may not be required to contain an "unsubscribe" link.

These messages include:
- purely factual information with no element or link suggesting a commercial purpose;
- message, *in respect of goods or services that the originating organisation is supplying,* from:
  - government bodies;
  - registered political parties;
  - religious organisations; and
  - charities.
- a message from an educational institution to a student or a student's household.

Australian link [cl.7]
The legislation is intended to prohibit:
- spam originating in Australia being sent to any destination
- spam originating overseas being sent to persons in Australia

It is intended that the legislation will cover all persons in Australia and its territories - it will be illicit to send spam to them, whatever the spam's point of origin, they shall be prohibited from sending spam, or causing spam to be sent, whatever its destination.

It is intended that all legal persons created by Australian law shall similarly be covered.

Unsolicited commercial electronic messages must not be sent [cl.16]
The legislation will prohibit the sending or commissioning of unsolicited commercial electronic messages. To be covered by the legislation the message must:
- have an Australian link;
- have been sent without the consent of the recipient; and
- not be a designated commercial electronic message.

People or companies that breach this provision will be liable for a civil penalty.

Consent [Schedule 2]
"Consent" involves situations where the recipient of the message may reasonably expect to receive messages of a commercial nature from the sender. These include the following scenarios:

- The recipient has subscribed to or otherwise overtly indicated a desire to receive the commercial message and have knowingly and directly provided an electronic address to the sender (a case of express consent);
- The recipient has knowingly and directly provided an electronic address to the sender of the commercial message in the knowledge that a commercial message is likely to be sent to the address (an implicit consent in a case where communication is likely)
- The recipient is in an existing business relationship with the sender and as part of that relationship have knowingly and directly provided an electronic address to the sender, and have not subsequently indicated that they do not wish to receive commercial messages (a case of implicit consent);
- The recipient has published their electronic address and job title in a manner that they would expect to receive communications about their job function (a case of implicit consent).

It is possible for consent to be withdrawn, except where there is a continuing contractual requirement for messages to be sent (eg in some forms of online billing/banking, where the customer has nominated to utilise online transactions in return for a financial advantage.)

Accurate sender information [cl.17]
Any commercial electronic message with an Australian link, whether solicited or unsolicited, must contain information that clearly and accurately identifies the individual or company that authorised the sending of the message.

Unsubscribe facility [cl.18]
All commercial electronic messages with an Australian link (except designated commercial electronic messages) must contain a functional unsubscribe facility, so that recipients can opt out of future communications. The unsubscribe facility needs to be active for at least 30 days after the message was sent, and any unsubscribe request must be honoured within 5 days.

Harvesting software, harvested lists [cl.20-22]
Software that automatically scans for and collates electronic addresses from internet pages are forbidden to be bought, sold or used for spamming purposes in Australia. Lists that have been created by such software may not be bought, sold or used for spamming purposes in Australia.

Pecuniary penalties - Court action [cl.24-25]
Breaches of the legislation may be brought to court by the enforcing agency; each proven breach will be subject to a pecuniary penalty, although in most examples of minor or inadvertent braches it would be expected that the ACA would provide a formal warning

rather than impose a penalty. The size of the penalty varies from quite small amounts to amounts for minor infringements under an infringement notice scheme, to a maximum of $1.1m per day for court awarded damages in the most extreme recidivist cases.

ACA has power to bring civil action [cl.26]
The agency responsible for investigating breaches of the spam legislation, and initiating court procedures will be the ACA.

Compensation/damages [cl.28]
Where a person or company has suffered loss or damages due to a spammer's activity, they, or the ACA on their behalf, may apply to the Court on their behalf for compensation to be paid.

Recovery of finances gathered by spamming/harvesting [cl.29]
In addition to fines for breaching the legislation, the Court may order the spammer to surrender any money they have made from the illegal activity.

Infringement notices [Schedule 3]
Instead of instituting a prosecution, the ACA may choose to issue an infringement notice to the person who has breached the Act. The infringement notice would be for a lesser financial penalty than a full court action, and would be used in cases where more minor contraventions of the legislation have occurred. The ACA may also choose to issue a formal warning instead of imposing a penalty.

The person receiving the infringement notice may choose to have the matter considered in a court action rather than pay the infringement fine. If they do so, they may be liable for a larger penalty amount in the event of being found to be in breach of the legislation.

Evidence Gathering [Conseq Amends, Part 2]
The *Spam Bill* and the *Spam (Consequential Amendments) Bill* extend the existing search and seizure powers that the ACA currently possesses to include spam-related evidence. In terms of the ACA conducting a search of premises and seizure of pertinent evidence, the ACA would require:

- a warrant obtained from a magistrate, or
- the permission of the owner of the premises, or of an occupier of the premises.

In the absence of a warrant, permission to enter premises (whether or not a private residence) typically depends on the consent of a person that has a legitimate concern in those premises - the owner, or occupiers of the premises. Where consent is refused, then a warrant is required in order to gain entry. Warrants are typically served in respect of premises, not in respect of particular persons, or a particular person's possessions. This avoids substantial elements of evasion and confusion which could otherwise arise.

The ACA would typically target the originators of prohibited messages, rather than the recipients, when gathering evidence. It is not possible to expressly forbid serving

warrants on recipients of spam in the legislation, as spammers would then be able to protect themselves from investigation by sending spam messages to themselves.

Injunctions [cl.32-36]
The ACA may apply to the Federal Court for an injunction to be served on a person to either:

- Stop the person from undertaking an action or behaviour that contravenes the legislation; or
- Directing them to perform an action that will bring them into compliance with the legislation.

Enforceable undertakings [cl.38-40]
Rather than pursue a court prosecution or an infringement penalty, the ACA may choose to accept a written undertaking, for example, from a person who is thought to have breached the legislation. This enforceable undertaking would be a formal promise that the person would not in future undertake activities that contravene the legislation. A breach of this promise may be subject to substantial pecuniary penalties.

Formal warnings [cl.41]
The ACA may choose to issue a formal warning to someone who contravenes the legislation, rather than issue an infringement notice or undertake a civil prosecution. This provision is intended to cover small scale breaches where a simple warning would be sufficient to cause a change in behaviour.

Additional ACA functions [cl.42]
The legislation will give the ACA the powers to:

- conduct or coordinate public education/information programs about spam
- undertake or commission research into spam related issues
- liaise with overseas bodies about cooperative arrangements against spam

Free speech [cl.44]
The legislation will not limit freedom of political communication.

International agreements [cl.45]
If Australia takes part in an international convention against spam, or undertakes a treaty agreement with another country that includes spam provisions, then regulations may be created to give effect to provisions relating to commercial electronic messages or address harvesting

Review of operation of Act [cl.46]
Within 2 years of the commencement of the penalty provisions of the Spam Bill 2003, the operation of the legislation will be reviewed to ensure that it is having the desired effect, and to check that particular provisions of the legislation are not having unintended consequences.