

Main features of the Spam Bill 2003

Definition of spam

The *Spam Bill 2003* refers to spam as "unsolicited commercial electronic messaging".

- The legislation covers more than just e-mails: mobile text messaging and other electronic messaging is also covered.
 - Voice to voice telemarketing is not covered.
 - A key attribute of the messaging covered by the legislation is that it is commercial in nature - it either offers a commercial transaction, or directs the recipient to a location where a commercial transaction takes place.
 - To be considered spam, the message must have been sent without the recipient's consent. Consent may be expressly given, or may be inferred from the behaviour or business or other relationships of the recipient. In restricted circumstances consent can also be inferred by someone conspicuously publishing their electronic address.
 - There is no reference to bulk messaging - a single unsolicited commercial electronic message could be spam, although enforcement would be unlikely.
-

Spam prohibited

The *Spam Bill 2003* prohibits sending, or causing to be sent, unsolicited commercial electronic messages that have an Australian link. It is prohibited to send commercial electronic messages to a non-existent address that would have an Australian link if the address existed. It is prohibited to aid, abet or otherwise be party to a contravention of the legislation.

Australian link

The legislation is intended to prohibit:

- spam originating in Australia being sent to any destination;
 - spam originating overseas being sent to an address accessed in Australia.
-

Accurate information about message originator

The *Spam Bill 2003* requires that all commercial electronic messaging contain accurate information about the message's originator. This will be the person or organisation that authorised the sending of the message, regardless of whether they actually send the message, or arrange for someone to do it on their behalf. The information must be reasonably likely to remain correct for a period of 30 days after the sending of the message.

Functional unsubscribe facility

The *Spam Bill 2003* requires that all commercial electronic messaging contain a functional "unsubscribe" facility to allow people to opt out from receiving messages from that source in the future. The unsubscribe facility must be reasonably likely to be able to receive and act on unsubscribe messages for a period of 30 days after the sending of the message. A request to opt out must be honoured within five working days to avoid future breaches of the legislation. Acceptable examples of the unsubscribe facility will be specified by regulation and may vary between technologies.

Harvesting software, harvested lists

The *Spam Bill 2003* prohibits the supply, acquisition or use of software that "harvests" electronic addresses from the internet for the purpose of sending spam. Similarly, the provision, acquisition or use of address lists to send spam is prohibited.

Exclusions - Designated Commercial Electronic Messages

Exceptions apply to protect currently accepted government, business and commercial practices, such as:

- Government to citizen messages;
- Messages from registered political parties;
- Messages from charities;
- Messages from religious organisations;
- Messages from educational institutions directed to attending students, past students or members of their households;

where the message relates to goods or services, and the sending body is the supplier of the goods or services. The sender must still include accurate information about the message's originator, but may send unsolicited commercial electronic messages, and is not required to include an unsubscribe facility.

Industry Codes & Standards

The Australian Communications Authority (ACA) will also facilitate and support the development of Industry Codes that complement and are consistent with the legislation. Industry Codes would provide relevant and achievable standards and procedures to assist compliance with the legislation.

120 day sunrise provision

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.

Formal warnings

The ACA may choose to issue a formal warning, rather than issue an infringement notice or initiate a full court proceeding. This would typically be done where the ACA was satisfied that the contravention was largely inadvertent and would not be repeated, or in other cases where a warning would suffice to change the contravening behaviour.

Infringement Notices

The ACA may choose to issue infringement notices for contraventions of the legislation, instead of initiating a full court proceeding. A person who receives an infringement notice may refuse to pay, but would then be subject to a court action, where, if the contravention was proven, they could be penalised at a higher rate than the infringement notice.

Main features of the *Spam Bill 2003*

Infringement Notices and Penalties

The infringement notice penalties for sending spam are:

- \$440 per contravention for an individual, with a maximum penalty of \$22,000 set for all contraventions that occur on a single day.
- \$2,200 per contravention for a body corporate, with a maximum penalty of \$110,000 set for all contraventions that occur on a single day.

The infringement notice penalties for sending commercial messages without an unsubscribe facility or inaccurate sender information, or for a contravention of the harvesting provisions are:

- \$220 per contravention for an individual, with a maximum penalty of \$11,000 set for all contraventions that occur on a single day.
 - \$1,100 per contravention for a body corporate, with a maximum penalty of \$55,000 set for all contraventions that occur on a single day.
-

Court Action

The ACA may initiate a court action in respect of a contravention of the legislation. If a contravention is found to have occurred, the ACA may apply to the court to order the person or organisation involved to pay a penalty (listed below), and additionally, to surrender any financial benefit they gained in the course of their contravening activity. Any person who has suffered loss or damages from someone else contravening the *Spam Bill 2003*, or the ACA on their behalf, may apply to the court to make an order for compensation.

Court imposed penalties for spamming

The main penalty provisions of the *Spam Bill 2003* are:

- Sending unsolicited commercial electronic messaging;
- Sending commercial electronic messages to a non-existent address;
- Aiding, abetting or otherwise being a party to such a contravention.

The maximum penalties that a court may impose for sending spam are:

- \$2,200 per contravention for an individual, with a maximum penalty of \$44,000 set for all contraventions that occur on a single day.
- \$11,000 per contravention for a body corporate, with a maximum penalty of \$220,000 set for all contraventions that occur on a single day.

Where the individual or organisation has a prior record - a court has found them in contravention of the particular provision in the past - and they have contravened subsequent to the court finding, then a higher schedule of penalties applies:

- \$11,000 per contravention for an individual, with a maximum penalty of \$220,000 set for all contraventions that occur on a single day.
 - \$55,000 per contravention for a body corporate, with a maximum penalty of \$1.1 million set for all contraventions that occur on a single day.
-

Main features of the *Spam Bill 2003*

Penalty amounts for other offences

Additional penalty provisions in the *Spam Bill 2003* are:

- Failure to include accurate sender information;
- Failure to include a functional unsubscribe capability;
- Address harvesting software and harvested lists – supply, acquisition, use;
- Aiding, abetting or otherwise being a party to such a contravention.

The maximum penalties that a court may impose for sending commercial messages without an unsubscribe facility or inaccurate sender information, or for a contravention of the harvesting provisions are:

- \$1,100 per contravention for an individual, with a maximum penalty of \$22,000 set for all contraventions that occur on a single day.
- \$5,500 per contravention for a body corporate, with a maximum penalty of \$110,000 set for all contraventions that occur on a single day.

Where the individual or organisation has a prior record - a court has found them in contravention of the particular provision in the past - and they have contravened subsequent to the court finding, then a higher schedule of penalties applies:

- \$5,500 per contravention for an individual, with a maximum penalty of \$110,000 set for all contraventions that occur on a single day.
- \$27,500 per contravention for a body corporate, with a maximum penalty of \$550,000 set for all contraventions that occur on a single day.

International activity

The legislation includes provisions that anticipate Australia's entry into multilateral arrangements with other countries concerned about the regulation of spam. This will enable regulations to be made giving effect to these agreements once in place. Enforcement of the penalties relating to overseas sourced spam will be problematic until international arrangements are in place, but the legislation ensures that there is an appropriate enforcement regime in place to deal with overseas spammers as soon as multilateral arrangements are in place.

Other streams of Australian anti-spam activity

Educational programmes

NOIE will coordinate a broad-based educational program focusing on both business and user communities in partnership with such groups as NetAlert, the IIA, the AIIA and others. It will target user communities, focussing on spam-reduction and avoidance strategies, and business communities, focussing on legitimate online marketing.

Technological measures

NOIE, the ACA and concerned industry bodies will promote the development and use of technological measures designed to reduce or eliminate spam. The closing of open relays, used as a conduit for spam, and the utilisation of spam filters and "spam interception" services will be important strategies.
