Spam canned — new laws for Australia

David Vaile
UNSW FACULTY OF LAW

Spam now constitutes more than 50 per cent of all email, and poses a threat to the information economy which prompted new laws around the world in late 2003.[1]

In Australia the National Office of the Information Economy (NOIE) wrote a report recommending Australian laws[2] which saw the Spam Bill 2003 (Cth)[3] and Spam (Consequential Amendments) Bill 2003 (Cth)[4] introduced in September 2003. ALP and Democrat amendments in the Senate in November were rejected by the Coalition Government, and the Bills passed in their original form in early December.[5] The Acts will come into full operation 120 days after assent (late April 2004 at the earliest).

These new Acts mainly affect senders and distributors of electronic messages, not recipients.[6] An item in the 'Bytes' section of *Internet Law Bulletin*[7] entited 'Industry support for Anti-spam Bill' noted support from stakeholders in the former category, such as the Internet Industry Association and Australian Direct Marketing Association (ADMA), while the UNSW Baker & McKenzie Cyberspace Law and Policy Centre symposium[8] also confirmed support from stakeholders in the latter category for the core 'opt in' principle,[9] but significant concerns were raised about the details by Electronic Frontiers Australia (EFA), Australian Privacy Foundation (APF), Australian Consumers Association (ACA), Internet Society of Australia and others.

Main features

NOIE summarised the Acts as follows[10] (added comments are in square brackets).

- There is a prohibition on sending 'unsolicited commercial electronic messages' to or from Australian addresses, or being commissioned by people within Australia[11] [unless they are 'designated commercial electronic messages' (DCEM) below].[12] References are to the *Spam Act 2003* (Cth) unless otherwise noted.
- Commercial electronic messaging is to be sent on the basis of consent[13] [with options for explicit consent and various forms of implied consent, including existing business relationship and 'conspicuous publication' of an address].
- Commercial electronic messaging is to include accurate details of the message's authoriser [except certain DCEM].
- Commercial electronic messaging is to include a functional unsubscribe [except certain DCEM].
- Address harvesting software and harvested lists are prohibited in respect of spamming [except certain DCEM. Sending messages to non-existent addresses is prohibited — harvesting software may be supplied provided an undertaking is given by the purchaser to comply with the Act].
- Courts may order payment of civil penalties, compensation, recovery of financial gain, or grant injunctions. [Penalties vary greatly. They range from an infringement notice from the ACA for sending spam of $440 per contravention for an individual, with a maximum penalty of $22,000 for all contraventions on a single day, to a maximum penalty that a court may impose where a court has found the individual or organisation in contravention of the particular provision in the past and they have contravened subsequently; $55,000 per contravention for a body corporate, with a maximum penalty of $1.1 million for all contraventions on a single day.]
- The ACA may issue formal warnings, infringement notices, accept enforceable undertakings, gather evidence through warrant or consent based searches [though arguably in some cases without a warrant or consent] and the ACA may register industry codes.[14]
- Provision is made for limited exemptions [DCEM] in respect of commercial messages from government bodies, registered political parties, charities, religious organisations, educational institutions, and commercial messages conveying purely factual information.

Courts may order payment of civil penalties, compensation, recovery of financial gain, or grant injunctions.

'Opt in' principle and exceptions

The Acts are based on an 'opt in' principle. The required consent can be either explicit or implicit.

In addition to relatively uncontroversial 'existing business relationship' and 'previous conduct' cases,[15] 'implicit consent to receive messages relevant to a recipient's employment function can also be based the 'conspicuous publication' of an email address in a way that does not negate a willingness to accept such messages.[16] An address on a company site without a 'no commercial emails' note would permit unsolicited commercial emails relevant to the person's job role, which could arguably be considered

to be very wide in the case of a senior officer of a large, diverse corporation. Marketers will no doubt be tempted to push the boundary of this job role exemption, but it will be difficult to assess where the legal threshold falls.

Withdrawal of consent must be honoured within five working days,[17] except for certain DCEM (so it may be hard to get charities, churches, political parties or governments to stop sending you DCEM).

The Acts cover 'electronic messages'.[18] Email messages are the main target but other media are covered, such as SMS (short text messages sent from or to a mobile phone) and instant messaging (messages exchanged in real time by networked computers using compatible instant messaging software clients). These are potential growth areas for targeted marketing.

The Acts cover only 'commercial' electronic messages,[19] the definition of which focuses on a purpose to offer, advertise or promote goods, services, land or business opportunities, or a supplier thereof, and includes dishonestly obtaining benefits, and other purposes in regulations. Other messages are not regulated and some commercial messages are exempt (below). Unsolicited bulk emails are permitted if they are not 'commercial'. Some supposedly 'purely factual' messages (such as certain newsletters) from commercial sources with a promotional purpose among other purposes will be permitted if they are DCEM.

Only messages with an 'Australian link' are covered, such as the sender, authoriser or recipient being in Australia, or having business or message access devices in Australia. It has been suggested that a foreign sender might argue that avoiding email address domains ending in '.au' is enough to raise a defence that they have tried not to send messages to recipients in Australia.[20]

Exemptions

Electronic messages which are not 'commercial' in nature within the terms of the Acts (they do not promote or offer goods and services and so on) are outside the scope of the legislation by definition, so political speech (which is also specifically exempt), religious, advocacy, educational and other messages are not regulated. As a matter of policy choice, and potential legal and constitutional difficulties with broader free speech issues, the Acts do not regulate mass messaging for these purposes.

Only messages with an 'Australian link' are covered, such as the sender, authoriser or recipient being in Australia, or having business or message access devices in Australia.

Bodies

There are explicit exemptions for 'designated commercial electronic messages' permitting certain bodies[21] (registered political parties, local or foreign governments, religious and charitable organisations, and educational institutions in respect of students and their families) to send commercial messages about their own goods and services.

'Factual' messages

DCEM includes messages characterised as 'factual' (as compared to 'commercial') that include logo and address of sender, provided they would not have been a commercial electronic message but for the presence of the logo and so on.[22] While apparently aimed at newsletters, it potentially permits a broad category of unsolicited bulk email from commercial senders.[23] Determining the primary intent of the message may depend on whether links in the message take the reader to a point of purchase or just a general web page. The distinction between a designated commercial electronic message containing factual information and a commercial electronic message will be hard to draw precisely.

Single message

There is no volume test, so a single message can be considered spam. While

this makes it easier to obtain evidence to prosecute,[24] it offers a wide scope for the ACA's discretion, apparently assuming it will turn a blind eye to potential small scale or technical breaches. The ACA seems likely to focus on education and encouragement of voluntary industry improvement efforts, rather than investigation or enforcement — so targeting single messages seems unlikely. However, this will complicate compliance and liability assessments.

Internet service providers

Internet service providers (ISPs) will not be liable merely by supplying a carriage service which enables spam to be sent.[25] However, ancillary provisions mean that an ISP who is aware that an account user is using the carriage service to distribute spam may arguably be deemed to be encouraging the user, and hence at risk of breaching the prohibitions against aiding, abetting, counselling, procuring, inducing by threats or otherwise, being in any way directly or indirectly knowingly concerned in or party to, or conspiring to effect a contravention of ss 16-18.[26] Drawing a line between mere supply of carriage service and these latter cases may be difficult in practice, making liability uncertain and dependent on the ISP's knowledge and subjective attitude.

Requirements

No address harvesting

Supplying, acquiring or using address harvesting software and lists created therefrom, where the supplier or user has an Australian link, is prohibited.[27] EFA suggests government agencies, senders of non-commercial messages and senders of DCEM are exempt.

'Unsubscribe' facility

Many messages require a 'functional unsubscribe facility'.[28] Where there is no requirement for ongoing communication due to a continuing business or contract relationship, it is prudent to include this on emails based on an existing relationship, and to comply with requests within five days. DCEM are exempt.

Accurate sender information

Messages, even DCEM, must include accurate information on the sender or authoriser.[29]

Enforcement

The ACA has been given wide powers of search and seizure but limited extra resources. Ambiguities in the definitions mean a range of messages may arguably be prohibited, but ACA may have to exercise its wide discretion to ignore or warn most detected alleged offenders.

The potential prison term for failure to provide passwords or decryption keys will no doubt concern system operators wary of compromising security.

Fines and injunctions will be the main legal means for acting against known spammers, with enforceable undertakings an option.[30]

No private right of action

Reports of spam to the ACA will probably not be treated on a case by case basis. Recipients and others must rely on the ACA to litigate.

In view of the ambiguities in some of the significant distinctions noted above, it will be interesting to see how the Act's provisions will be enforced in practice. Indications are that ACA does not see itself primarily as a 'spam police' unit, but it may be a challenge to assess the precise level of potential legal liability risk that can be tolerated by ISPs and marketers. ●

David Vaile, Executive Director, Baker & McKenzie Cyberspace Law and Policy Centre, UNSW Faculty of Law.[31]

Endnotes

1. EU Directive 2002/58/EC <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf>; *Controlling the Assault of Non-Solicited Pornography and Marketing Act 2003 (CAN-SPAM Act)* (US) <http://thomas.loc.gov/cgi-bin/query/ z?c108:S.877:>; California's *Business And Professions Code* s 17529 <www.spamlaws.com/state/ca1.html>

2. <www.noie.gov.au/publications/NOIE/spam/final_report/>.

3. <http://scaleplus.law.gov.au/html/bills/0/2003/0/2003091906.htm>.

4. <http://scaleplus.law.gov.au/html/bills/0/2003/0/2003091905.htm>.

5. <www.aph.gov.au/senate/committee/ecita_ctte/spam/report/>.

6. Recipients are subject to search and seizure of their computers (although ACA and NOIE suggest this is unlikely to occur without an invitation). Recipients can inform the ACA of a spam incident, but this will not be treated as a complaint, and thus there is unlikely to be any report back about progress or outcomes of any investigation.

7. (2003) 6(7) INTLB 86.

8. <www.bakercyberlawcentre.org/spam/spam_bill.htm> has useful references.

9. As opposed to the dubious 'opt out' principle in the US *CAN-SPAM Act*.

10. Submission 14 to Senate committee, October 2003 p 5, <www.aph.gov.au/senate/committee/ecita_ctte/spam/submissions/sub14.doc>.

11. Sections 5 and 6.

12. Section 16(1)(b).

13. Section 16(2).

14. *Telecommunications Act 1997* (Cth) Pt 6.

15. See the *Explanatory Memorandum, Spam Act 2003* (Cth) for examples.

16. *Spam Act 2003* Sch 2 Cl 4(2).

17. Section 6 of Schedule 2.

18. Section 5.

19. Section 6.

20. Sections 7 and 16(3)(b).

21. Schedule 1 Cl 3 and 4.

22. Schedule 1 Cl 2, esp 2(1)(b).

23. See Explanatory Memorandum.

24. *Spam (Consequential Amendments) Act 2003.*

25. *Spam Act 2003* s 9, 16(10), 17(6) and 18(7).

26. Sections 16(9), 17(5) and 18(6)

27. Part 3.

28. Section 18.

29. Section 17.

30. Parts 4 and 5.

31. The author draws on commentary and submissions from Patrick Fair and Nathan Shepherd of Baker & McKenzie, Jodie Sangster of ADMA, Lindsay Barton of NOIE, John Haydon of ACA, Irene Graham of EFA, Nigel Waters of APF, Philip Argy of ISOC-AU and Jason Catlett of Junkbusters, but the opinions and errors are of course his alone.