INFORMATION, ANALYSIS
AND ADVICE FOR THE PARLIAMENT

INFORMATION AND RESEARCH SERVICES

Bills Digest
No. 45 2003–04

Spam Bill 2003

DEPARTMENT OF THE PARLIAMENTARY LIBRARY

ISSN 1328-8091

Inquiries

Members, Senators and Parliamentary staff can obtain further information from the Information and Research Services on (02) 6277 2646.

Information and Research Services publications are available on the ParlInfo database.
On the Internet the Department of the Parliamentary Library can be found at:
http://www.aph.gov.au/library/

Published by the Department of the Parliamentary Library, 2003

INFORMATION AND RESEARCH SERVICES

Bills Digest
No. 45 2003–04

Spam Bill 2003

Brendan Bailey
Law and Bills Digest Group
7 October 2003

Contents

Spam Bill 2003

Date Introduced: 18 September 2003

House: House of Representatives

Portfolio: Communications, Information Technology and the Arts

Commencement: Royal Assent or, where specified, 120 days after Royal Assent. (The 120 day deferred commencement period applies to penalty provisions to enable businesses time to align business practices with the legislative requirements.)

Purpose

The purpose of the Bill is to regulate unsolicited and unwanted commercial electronic junk mail (spam).

Background

The Government's Policy Commitment

On 23 July 2003, the Minister for Communications, Information Technology and the Arts, Senator the Hon Richard Alston announced that the Australian Government was to ban commercial electronic junk mail (spam). The media release stated:

> The Australian Government is committed to taking a strong stand against spam and has moved quickly to respond to the report by the National Office for the Information Economy *The spam problem and how it can be countered* released in April this year. This report provided a blueprint to take action against the problem to provide the maximum possible protection against spam.[1]

The proposed anti-spam measures will see national legislation, to be enforced by the Australian Communications Authority (ACA), banning the sending of commercial spam without the prior consent of the recipient. Commercial electronic messages will be required to include accurate identification details of the sender, and the distribution and use of list–generating software (and address lists) will be banned. The Government has stated that it will work closely with industry and liaise with international organisations to

combat the problem of spam while still allowing industry in Australia to maintain a workable regime for legitimate business practices.

The Bill provides a definition of an 'Australian link' in **Clause 7** to define when commercial spam falls within the regulation and penalty provisions of the legislation. Basically, the Bill is directed at Australian originated spam or where the overseas sender is represented in Australia or maintains a server in Australia. Spam is delivered electronically over the Internet and the legislation will not directly affect (in a practical sense) the bulk of e–mail from overseas sources but the initiative taken in Australia may help create a move towards an international enforcement regime. Clause 7 includes a provision that will cover any spam accessed by a computer in Australia but if the sender is overseas they need to come within Australian jurisdiction to satisfy the 'Australian link' provision. Spam filters and blockers will still have to be used to counter most overseas generated junk mail.

The Internet

The main drivers of the Internet today are commercial computer firms and a host of Internet Service Providers (ISPs) but the Internet grew out of an advanced research project for an electronic communications network undertaken for the United States Department of Defense. As early as 1969, a network called ARPANET was designed and developed to provide a 'network of networks' to link universities, military and defence contractors for the purpose of sharing research information and to study the potential of computer-based command and control systems.[2]

In 1983, ARPANET was split into MILNET (for military communications) and ARPANET (which continued to be used for research into networking) which eventually became absorbed into the broader Internet.[3]

Initially, it was proposed that ARPANET access be confined to researchers but the concept began to be adapted for the development of other networks and it became readily apparent that it was a valuable and new method for more widespread communications usage. The Internet still reveals its military origins in one sense in that it is designed to avoid a major catastrophe if a destructive strike was directed at 'headquarters'—the Internet has no 'headquarters'.[4] It is an interlinked web of networks that move electronic traffic through connecting gateways. Each network system joining the Internet is responsible for its own administration. There is no single service provider.

Electronic mail (e–mail) is the most elementary service on the Internet. E–mail in its simplest form is a carrier of digital messages between two people, or through a mailing list to a group. Initially, it was considered to be an insignificant aspect of network capabilities.[5] Today it is a worldwide form of electronic communication and it has become a core Internet application offering fast, convenient and, in some cases, an addictive form of mail transmission. The problem of distance is irrelevant on the Internet.

Some Limited Methods to Counter Spam

Adam C. Engst in his 1994 text, *Internet Starter Kit for Macintosh*, foreshadowed that problems would occur with the commercialisation of the Internet. He noted:

> However, we must remember the old attitudes about commercial use of the Internet. In the past, commercial use was often acceptable if it wasn't blatant, was appropriately directed, and was of significant value to the readers. In other words, I'll be as angry as the next person if I start receiving automatically generated junk mail every day, just as I receive junk mail via snail mail.[6]

Mr Engst suggested in 1994 that one response was to 'flame away' (i.e. send back an outrageously nasty message). The problem nowadays is the volume of spam that seems to arrive and the waste of time that would be involved in replying. Also, some spam is deliberately constructed to confirm a valid e–mail address when the recipient responds and the address is then on-sold to other spammers.

Block deletion by the person receiving the message is always available but most users are concerned that in haste and frustration they may inadvertently delete an important message.

Education programs, voluntary codes of conduct for using the Internet, blacklisting and filters have not successfully addressed the problem of determined spammers who switch e–mail addresses or servers to avoid detection. Spammers will also abuse the relay facility that is at the core of the Internet which allows a message to be relayed by one server to another. Internet relay servers are proliferating in a number of countries.

One of the more serious threats with spam is its use to perpetrate scams and fraud and to offer access to illicit pornography. A useful discussion on spam and computer crime can be found in the Parliamentary Library's *Research Note*, 'Computer Crime and Compromised Commerce′ by Matthew James and Brian Murray[7] and in the transcripts of the hearing of the Parliamentary Joint Committee on the Australian Crime Commission on its reference *Cybercrime* held on 21 July 2003.[8]

Another development is the spamming of chatroom users. Apart from financial scams, there is a growing concern about young users who may be vulnerable to predators. Major providers of these services are looking to close down their chatrooms because of the abuse of the facility.[9]

It is possible to purchase a disposable e–mail address service where the addresses are time limited or just used as an alias and deleted (and replaced with a random address) once the first address is plagued by spam.[10]

The Top Ten Spam Messages for 2002

The Computer Research and Technology (CR&T) website provides a list of the 'Spam top 10 hit list'.[11] The list, which is more directly applicable to users in the United States—but the items are still received by other users of the Internet, for 2002 is:

1) Free adult site passwords
2) Low price drugs (Viagra)
3) Refinance your mortgage
4) Nigerian confidential money transfer
5) Tiny remote control car
6) Best online casino
7) #1 Pasta pot
8) Get out of credit card debt
9) Meet singles in your area
10) Copy DVDs in one click

Because of the difficulty of penalising anyone outside Australian jurisdiction, the legislation is unlikely to counter the transmission of the spam items listed above.

CR&T estimates that spam now cost businesses worldwide about $9 billion per year to deal with and that one in twelve e–mails was identified as spam by companies using spam Internet filters.

Businesses (and private users) are also concerned about the more sinister side to spam which now includes 'brand spoofing' where personal and financial data is extracted by the spammer who disguises the e–mail to make it appear as if it is from a reputable business address. Brand spoofing can also be used for hoaxes. Recently, British schoolchildren were reportedly encouraged to consume packets of chips and to retain the empty packets to stack into a bundle weighing the equivalent of a disabled infant. This cruel hoax misled the children into believing that once the goal was achieved a reputable snack manufacturer would pay for the infant's treatment.[12]

The tidal wave of spam has the potential to overwhelm the Internet.

Interest Groups and Press Commentary

On 26 June 2003, the Internet Industry Association convened a *Spam Legislative Forum* at Parliament House in Canberra. The consensus of the forum was support for tough national legislation to counter spam. An article outlining the key issues to consider in any regulatory response appeared in the August 2003 edition of the *Internet Law Bulletin*. The

article was written by Peter Coroneos, Chief Executive of the Internet Industry Association. The article is available on *ParlInfo*.[13]

The CR&T web site contains an article that is supportive of the Bill and describes it as a 'step in the right direction' but makes the observation that it will not have much of an impact on spam that originates from overseas.[14]

A lobby group, Coalition Against Unsolicited Bulk E–mail, Australia (CAUBE.AU) has been formed to represent the views of those in Australia who are opposed to spam advertising practices. There are related lobby groups in other countries. The following news item has been extracted from the CAUBE.AU website:

> 1st June 2002
>
> Global Internet Community Applauds European Anti-Spam Vote
>
> The Coalition Against Unsolicited Commercial E-Mail (CAUCE), EuroCAUCE, CAUCE India, CAUCE Canada and the Coalition Against Unsolicited Bulk E-Mail, Australia (CAUBE.au) today applauded the decision by the European Parliament to protect European Internet users from the practice of unsolicited e-mail advertisements. Yesterday's vote will turn Europe into a virtual "spam-free zone" after the formal adoption of the directive, making it illegal to send unsolicited e-mail, text message or other similar advertisements to individuals with whom companies do not have a preexisting business relationship.[15]

The *Canberra Times* reported on 26 September 2003 that in the United States the Governor of the State of California had signed into law a legislative ban on spam e–mails with fines of up to $US1 million ($A1.48 million).[16]

Media coverage in Australia on the Bill is generally favourable but there is some debate over the proposed exemptions for government agencies, political parties, charities, religious organisations and educational institutions. One approach suggested is to allow the exemptions but to monitor any abuse of this concession by non–commercial mailers using the Internet.[17]

Pros and Cons

The lobby group CAUBE.AU has stated that its support for regulation of spam through a legislative response is a reversal of its previous view that the government should not regulate the Internet.[18] CAUBE.AU has recognised that spam presents a unique problem that is getting worse.

Spam is parasitic. It is cheap to send but it relies on Internet service providers (ISPs) bearing the increasing cost of carrying the flood of messages on their servers and taking up disk space. ISPs are adding additional servers just to cope with the load including setting up additional mail servers to filter spam so that it is not moved within the network to

individual mail boxes. Individual users are also faced with the task of clearing spam that gets past the anti-spam devices. Unless checked, spam will slow down the Internet to a point that it may loose its utility for global and domestic communication. The spam load is wasteful and inhibits, to an appreciable degree, expansion in the number of new users of the Internet.

Domestic legislation in Australia will not prevent spam arriving from overseas but if enough countries are active in countering the menace and coordinating their efforts then there is hope for the creation of international enforcement action against this abuse of a valuable communications system.

Privacy Act and Other Existing Legislation

There is no specific legislation in Australia, at present, that requires a sender of an electronic message to first obtain the permission of the recipient. The National Privacy Principles in the *Privacy Act 1998* address the collection of personal information and the use of that information for purposes other than that for which it was collected. The *Explanatory Memorandum* to the Bill explains that the *Privacy Act 1998* may not adequately address the problem where the spammer has collected the personal information directly (as opposed to indirectly) from the recipient. Even where the *Privacy Act 1998* could apply there is the difficulty of enforcement.[19]

The *Explanatory Memorandum* also provides a brief summary of other legislation which has some relevance to the problem of spam.[20] These laws include:

- *Interactive Gambling Act 2001* (which prohibits certain forms of online gambling);
- *Therapeutic Goods Act 1989* (but only dealing with Australian-based offers of therapeutic goods i.e. as to any misleading statement as to content of the product);
- *Broadcasting Services Act 1992* (limited application in the content of sites on the Internet but the law does not apply to ordinary e–mails);
- *Trade Practices Act 1974* (misleading and deceptive conduct); and
- *Crimes Act 1914* (menacing, offensive or harassing material).

Australian Labor Party's Policy Position

In a media statement issued on 18 September 2003, Senator Kate Lundy, the Shadow Minister for Information Technology supported the introduction of anti–spam legislation but noted that the Coalition Government could have responded earlier to combat the problem of spam. Senator Lundy said that the Labor Party has always endorsed strong measures to counter spam and that it will analyse the Government's legislation in detail.[21]

The Australian Democrats Policy Position

Senator Brian Grieg, the Australian Democrats spokesperson on Information Technology, has recognised the need for anti-spam legislation but urges the Government to ensure that Internet users know their rights and are also made aware of the use of blocking devices and other practical anti-spam options.[22]

Senator Grieg is reported as commenting that, while the Democrats supported penalties for repeat offenders and the provision in the Bill to allow people to accept spam, the exemptions for political parties during election campaigns and charities should be removed.[23]

Consequences of Failure to Pass the Bill

The Bill is likely to receive bipartisan support in the Parliament. Viewed overall, it is not controversial legislation but there may be some consideration of the proposed exemption of non-commercial organisations. If the Bill was rejected, the existing availability of the Internet would continue with current anti-spamming measures remaining the responsibility of the industry, business, ordinary users and, where relevant, crime authorities.

Main Provisions

Part 1—Introduction

(Part 1 commences on Royal Assent.)

Clause 3 provides a simplified outline for the legislation. The key features of the Bill are:

- the regulation of commercial e-mail, including a prohibition on sending unsolicited commercial electronic messages;
- a requirement to include information about who authorised the sending of the message;
- a facility for a recipient to unsubscribe to the commercial messages;
- a ban on address–harvesting and list producing software; and
- civil penalties and injunctions for breaches of the legislation.

The main regulatory framework for the administration of the legislation by the Australian Communications Authority (ACA) is found in the accompanying Bill, the Spam (Consequential Amendments) Bill 2003.

Clause 4 provides the definitions of words and expressions used in the legislation while **Clauses 5** to **6** provide specific extended definitions for standard and commercial 'electronic messages', respectively. (**Schedules 1** and **2** to the Bill provide detailed definitions for 'designated electronic message' and the meaning of 'consent' when used in relation to the sending of an electronic message, respectively.)

Clause 7 is a key provision in the Bill. It provides a definition for when a commercial electronic message has an Australian link. The regulation of commercial e–mails and the penalty provisions in the Bill are tied to e–mails that have an 'Australian link'. Broadly stated, the link is established if the commercial e–mail:

- originates in Australia;
- the sender (or person who authorised the e-mail) is located in Australia;
- the computer or server that accesses the message is located in Australia, or
- the electronic account holder is in Australia.

Clause 9 makes it clear that the carriage provider who simply provides a service for the transmission of e–mails does not breach the legislation unless the carriage provider actively advertises to provide services to spam senders.

Part 2—Rules about sending commercial electronic messages

(Part 2 commences 120 days after Royal Assent.)

Part 2 of the Bill sets out the civil penalty provisions for sending unsolicited commercial e–mail where there is an Australian link. Part 2 also specifies that commercial e–mails must contain identifiers and an unsubscribe facility.

Clause 16 is the primary provision that proscribes the sending of unsolicited commercial 'Australian link' e–mails unless there is prior consent. The penalty for an offence applies to the person who hits the send button, the author of the message and whoever may have authorised the message. The penalty applies to those actively involved in sending the message and not to the equipment i.e. to avoid a situation of penalising a person whose computer (or telephone) was hijacked or the computer is affected by a virus. Similarly, the penalty does not apply to innocent transmission by a carrier.

Exemptions

- government bodies;
- a registered political party;

- a religious organisation;
- a charity or charitable institution;
- educational institutions (but only for student or former student related matters);
- a message containing no more than factual information and;—that complies with the identification obligations under the legislation; or
- is identified in subsequent Regulations made under the legislation.

Specified defences to an offence

The defences (with the evidential burden on the sender) to an offence under the legislation are specified as:

- the relevant account–holder consented to the message;
- the sender could not reasonably have known that there was an Australian link (e.g. which may occur if the Australian recipient has an address that ends with '.com' rather than '.com.au'; and
- the message was sent by mistake (e.g. where the sender's computer is affected by a virus or if there is an incorrect misspelling of an e–mail address where the intended addressee has consented to receive the message).

Paragraph 16(1)(b) provides an exemption for e–mails that are 'designated commercial electronic messages' (see the list above and the definition in Schedule 1 to the Bill).

Subclause 16(6) covers the situation where the spammer sends e–mails in bulk by a 'dictionary method' i.e. by a random method such as a common surname in the address but prefixed by 'a', then 'b', then 'c' and so on (referred to in the Bill as non–existent electronic addresses).

Subclause 16(9) covers aiding, abetting, conspiracy and inducing the sending of spam by threats or promises.

Clause 17 requires commercial electronic e–mails to contain accurate identification details and **Clause 18** requires commercial e–mail messages to also contain an unsubscribe facility. An unsubscribe facility allows the recipient to opt-out of future contact. Penalties, specified defences, aiding and abetting provisions also apply (see Part 4—Civil penalties, below).

Part 3—Rules about address–harvesting software and harvested–address lists

(Part 3 commences 120 days after Royal Assent.)

Clauses 20 to **22** prohibit the offering of, supply, acquisition or use, respectively, of address–harvesting software and harvested–address lists. Some spammers collect addresses from web pages or newsgroups and also buy lists from other spammers or companies. They also use electronic *spambots* (the suffix 'bot' just means 'robot' software) to scour web pages and newsgroups. This type of software is also called a web crawler, spider, robot or worm. It has legitimate commercial applications, such as when used for tracing copyright infringement or sale of counterfeit products. Responsible commercial web crawlers will respect the industry–based *Robots Exclusion Protocol* and not examine sites that contain an electronic signal in their text that requests that the site not be crawled.

Spammers also join a mailing list then gather the e-mail addresses of other members. Spammers also deceive random addressees by falsely including a message to reply to 'remove' the address. A reply simply confirms a legitimate address and that there is no anti–spam device operating at the address.

Again, under these provisions there must be an Australian link and there is a defence that the supplier had no reason to believe that the software or list would be used for spamming. Aiding and abetting is also covered. Civil penalties apply.

Part 4—Civil penalties

(Part 4 commences 120 days after Royal Assent.)

Clauses 23 to **30** provide the details of the application of the series of civil penalties that are payable for contraventions of the legislation. The penalties escalate for repeat offences. Proceedings for the recovery of penalties are instituted in the Federal Court of Australia. Ancillary orders for compensation to a victim and for payment to the Commonwealth of the amount of any financial benefit obtained by the spammer are covered in this Part.

The unit rate for a penalty is currently set at $110 per penalty unit. The summary of current maximum penalty amounts is provided in the *Explanatory Memorandum* at pages 93 to 96 and they range for an individual from $1,100 to $220,000 (repeat offender) and for a corporation from $5,500 to $1.1 million (repeat offender).

(A summary of the maximum penalty amounts is provided in the *Explanatory Memorandum* at pages 93 to 96.)

Clause 30 provides a link to **Schedule 3** to the Bill which sets up a system of infringement notices as an alternative to proceedings in the Federal Court.

The ACA is empowered by **Clause 26** to initiate proceedings in the Federal Court and to issue infringement notices (**Schedule 3**).

Part 5—Injunctions

(Part 5 commences 120 days after Royal Assent.)

Clauses 31 to **36** authorise the Federal Court to issue a range of injunctions for contraventions of the legislation. These injunctions include orders to restrain conduct and to compel a person 'to do something'. The ACA is empowered to apply to the court for injunctions.

Part 6—Enforceable undertakings

(Part 6 commences 120 days after Royal Assent.)

Clauses 37 to **40** authorise the ACA to receive formal administrative undertakings that are court enforceable from a person, in connection with a matter relating to commercial e–mails and address–harvesting software. A breach of an undertaking can give rise to court–ordered compensation (**Clause 40**).

Part 7—Miscellaneous

(Clause 41 commences 120 days after Royal Assent. **Clause 42** commences on Royal Assent. **Clauses 43** to **46** commence 120 days after Royal Assent. **Clause 47** commences on Royal Assent.)

Clause 41 empowers the ACA to issue formal warnings if a person contravenes the legislation and if the matter is assessed as a minor infringement.

Clause 42 provides additional functions for the ACA in spam–related matters, including:

- community education programs;
- research; and
- conducting liaison with other regulatory bodies in Australia and overseas.

Clause 43 allows the concurrent operation of any State or Territory laws that are capable of applying together with the provisions of this Bill.

Clause 44 prevents the Bill applying to the extent that it would infringe the freedom of political communication as implied from the Constitution.[24]

Clause 45 authorises the making of Regulations that would give effect to an international convention that deals with combating spam and address–harvesting software. This Clause foreshadows that Australia is looking at the possibility of concluding agreements with other countries to deal with the global impact of spam. Regulations are subject to a tabling and disallowance procedure in the Parliament.

Clause 46 specifies that the operation of the legislation will be reviewed 2 years after the commencement of the legislation (in this section commence is 120 days after Royal Assent). A report of the review must be tabled in Parliament by the Minister.

Concluding Comments

It is noted that **Clause 44** in the Bill addresses the implied freedom of *political* communication as recognised by the High Court (see endnote 23, below). The Bill does, however, limit any general doctrine of the freedom of speech but that erosion of freedom in the case of spam appears to be supported by the majority of users, business, industry, the media, government and other political groups. There may be some debate on the exemptions for specified non–commercial senders of e–mails.

Endnotes

1 Senator the Hon Richard Alston, Minister for Communications, Information Technology and the Arts, *Media Release* No. 122/03, 'Australian Government to ban spam', 23 July 2003 at: http://www.dcita.gov.au/Article/0,,0_4-2_4008-4_115938,00.html and the report by the National Office for the Information Economy (NOIE), *The spam problem and how it can be countered* (April 2003) can be located at: http://www.noie.gov.au/publications/NOIE/spam/final_report/index.htm.

2 Paul Gilster, *The New Internet Navigator*, John Wiley & Sons, New York, 1995, 21.

3 ibid., p. 23.

4 See Heinz Tschabitscher, 'Spam', *Email.About.com*, at: http://email.about.com/library/weekly/aa100697.htm .

5 Paul Gilster, *The New Internet Navigator*, John Wiley & Sons, New York, 1995, p.31.

6 Adam C. Engst, *Internet Starter Kit for Macintosh*, 2nd Edition, Hayden Books, Indianapolis, 1994, p. 53.

7 Matthew L. James and Brian E. Murray, 'Computer Crime and Compromised Commerce', *Research Note* No. 6 2003–04, Department of the Parliamentary Library, 11 August 2003 at: http://www.aph.gov.au/library/pubs/rn/2003-04/04rn06.htm.

8 See the evidence to the Parliamentary Joint Committee on the Australian Crime Commission, Reference: Cybercrime, *Hansard*, 21 July 2003: pp. 4, 37–38, 47, 52, 60 and 81at: http://parlinfoweb.parl.net/parlinfo/Repository/Commttee/Commjnt/Linked/2679-2.PDF

9 Diana Thorp and Stuart Kennedy, 'Net tightens on chat', *Australian*, 25 September 2003; p. 9.

10 See the review by Heinz Tschabitscher, 'Emailias', in *Email.About.com,* at:

http://email.about.com/cs/dispaddrrevs/gr/emailias.htm.

11 Computer Research and Technology, *eTopics,* at: http://www.crt.net.au/etopics/irritatingspam.htm.

12 'Modern Life', *Sydney Morning Herald*, 25 September 2003, p. 20.

13 Peter Coroneos, 'Perceptions of spam', *Internet Law Bulletin*, Vol 6 No 5, August 2003: 54–56 at: http://parlinfoweb.parl.net/parlinfo/Repository1/Library/Jrnart/YE9A61.pdf.

14 Computer Research and Technology, *eTopics*, 'Spam senders may face hefty fines', at: http://www.crt.net.au/etopics/spamfines.htm.

15 Coalition Against Unsolicited Bulk E–mail, Australia, (CAUBE.AU), *Latest News*, at: http://www.caube.org.au/latest.htm.

16 International, 'No junk mail please', *Canberra Times*, 26 September 2003, p. 12.

17 See Rachel Lebihan, 'Bill lets some spam slip through the net', *Australian Financial Review*, 19 September 2003: p. 13; E–mail, 'Anti–spam law wins applause', *Australian*, 23 September 2003, p. 29, 'New anti–spam laws to target junk e–mails', *Canberra Times*, 19 September 2003.

18 Coalition Against Unsolicited Bulk E–mail, Australia, (CAUBE.AU), at: http://www.caube.org.au/.

19 *Explanatory Memorandum*, Spam Bill 2003, p. 23.

20 ibid., p 24.

21 Senator Kate Lundy, Shadow Minister for Information Technology, 'Procrastination on spam costs Australians', Media Statement, 18 September 2003 at: http://www.alp.org.au/media/0903/20005753.html.

22 Senator Brian Grieg, Australian Democrats spokesperson for Information Technology, 'Democrats call for SPAM education', *Press Release*, 4 June 2003 at: http://www.democrats.org.au/news/index.htm?press_id=2716&display=1#.

23 See Rachel Lebihan, 'Bill lets some spam slip through the net', *Australian Financial Review*, 19 September 2003, p. 13.

24 Three High Court cases in the 1990s – *Australian Capital Television* (1992), *Nationwide News* (1992) and *Lange* (1997) established an implied constitutional right of political communication. The cases established that:

- limits on the Commonwealth's law making powers may be implied in and from the text of the Constitution;

- the key principle of the Constitution is representative democracy - expressed and constitutionally entrenched in sections 7 and 24;
- a necessary condition of representative democracy is the freedom to discuss and communicate information regarding political and economic matters; and
- this freedom extends beyond election periods to all political discussions generally.

A law cannot restrict freedom of political communication unless:

(i) it is enacted to fulfil a *legitimate purpose* (of Australia's constitutional system); and

(ii) the restriction is *appropriate* and *adapted* to fulfilment of that purpose.