Electronic Frontiers Australia

PO Box 382
North Adelaide SA 5006
Email: mail@efa.org.au
Phone: 02 9255 7969
Fax: 02 9255 7736
http://www.efa.org.au

The Secretary
House of Representatives Standing Committee
on Legal and Constitutional Affairs
Parliament House
CANBERRA ACT 2600
Via email: laca.reps@aph.gov.au

Dear Sir/Madam,

Inquiry into Privacy Amendment (Private Sector) Bill 2000

Electronic Frontiers Australia Inc (EFA) hereby submits our response to the Committee's Inquiry into the Privacy Amendment (Private Sector) Bill 2000.

EFA appreciates the opportunity to make a submission, and requests that we be granted permission to publish this submission online.

If the Committee decides to conduct public hearings, we would appreciate the opportunity to expand on our submission in person. We can provide representatives in any Australian capital city including Canberra.

Yours faithfully

Irene Graham
Executive Director
Electronic Frontiers Australia Inc

ELECTRONIC FRONTIERS AUSTRALIA

Submission to House of Representatives Standing Committee on Legal and Constitutional Affairs

Inquiry into Privacy Amendment (Private Sector) Bill 2000

INDEX

1. Executive Summary

EFA supports in principle the introduction of a co-regulatory scheme to provide privacy protection for Australians in relation to the activities of the private sector.

EFA is unable to support the Bill in its current form, because the Bill contains too many exemptions and exceptions and fails to come to grips with consumer privacy needs in the 21st century.

The exception to the Privacy Principles in relation to direct marketing is contrary to international developments and effectively legitimizes the practice of "spamming" (the

sending of unsolicited E-mail advertising) on the Internet.

The exemption for small business is unjustified and will introduce a confusing and complex regulatory environment that fails to protect consumers from privacy invasive practices. The confusion that will result from this exemption will hamper attempts by E-commerce vendors to attract overseas customers.

The exemptions for media organisations and political parties are far too broad and have not been justified. The definition of *media organisation* could well include almost every existing website.

The exemption for pre-existing data is unacceptable. A transition period should be provided for existing data uses to comply with the new legislation.

Enforcement provisions in the legislation are inadequate.

Instead of empowering individuals to exercise their right to privacy of personal data, the Bill confers on certain business interests the right to invade individual privacy.

In summary, the Bill is at best a token attempt to introduce privacy legislation. It is complex, unwieldy, ineffective and an insult to the citizens of Australia. The Bill needs to be re-drafted, preferably as a replacement for, rather than an amendment to, the Privacy Act 1988.

2. Introduction

> *"Solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury....*
>
> *The common law has always recognized a man's house as his castle, impregnable, often even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?"*
>
> *The Right to Privacy*. Samuel Warren and Louis D. Brandeis
>
> Harvard Law Review **4** 193 (1890)

Electronic Frontiers Australia Inc. ("EFA") is a non-profit national organisation formed to protect and promote the civil liberties of users and operators of computer based communications systems. EFA was formed in January 1994 and incorporated under South Australian law in May 1994.

Our major goals are to advocate the amendment of laws and regulations in Australia and elsewhere (both current and proposed) which restrict free speech and unfettered access to information and to educate the community at large about the social, political and civil liberties issues involved in the use of computer based communications systems. EFA is independent of government and commerce and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties.

EFA is primarily interested in privacy protection for Internet users and our comments on the proposed legislation will therefore largely focus on matters that may impact in the online area. However, we recognise that privacy issues pervade many other aspects of life, and we will therefore briefly comment on other aspects of the proposals.

EFA generally believes that government regulation should be a measure of last resort, particularly when it comes to regulation of new technologies such as the Internet. We are of the view that existing law can be applied to most problems that arise in the new information economy. We put this view particularly strongly in opposing the government's move to censor the Internet through the Broadcasting Services Act amendment of 1999. The government failed to listen and the result was a bizarre piece of legislation that is all but unenforceable, that has failed to meet its objectives, and that has embarrassed Australia internationally. If the current Privacy Bill is allowed to pass without major amendment, Australia may as well give up any hope of being a leading player in the information economy.

When it comes to privacy legislation, EFA is of the view that this is a legislative backwater that has been ignored in Australia for too long. We support a co-regulatory approach to privacy legislation, with approved privacy codes backed up by legal sanctions.

However, we consider that the current Bill fails to meet the standards of international best practice that have been established by other countries that have already legislated in this area, such as New Zealand, Canada, the UK and Hong Kong. Furthermore, we are of the view that the Australian legislation in its current form will fail to meet the requirements of the European Union Directive on Data Protection and therefore threaten to prevent Australian industry from fully participating in the emerging information economy.

Privacy has been defined as the right to be left alone. Unfortunately this simple principle has been largely overlooked in the current Bill. Australians generally deplore being overwhelmed with junk mail, telemarketing calls, unsolicited E-mail and an arrogant and intrusive media. As citizens we are nervous about giving out information about ourselves lest it be used for purposes that we did not approve.

Privacy concerns are consistently raised as amongst the top reasons why Internet users are reluctant to make purchases on the Internet. If Australia is to be a successful E-commerce player, it will have to convince the rest of the world that privacy is taken seriously and that effective sanctions are in place against offenders. This Bill is unlikely to convince anyone.

3. Direct Marketing Exception and E-mail Spam

At 2.1(c) of Schedule 3 of the Bill (National Privacy Principles) an extraordinary exception for secondary use is permitted in respect of direct marketing. Although this exception existed in the original version of the NPPs, the version included in the Bill has been widened further. No justification has ever been provided for this quite unacceptable intrusion into individual privacy.

The exception to the Privacy Principles in relation to direct marketing is also contrary to international developments and effectively legitimizes the practice of "spamming" (the

sending of unsolicited E-mail advertising) on the Internet.

Personal information should only be used for marketing purposes with explicit consent, not by default with the blessing of the government. Unsolicited direct marketing, whether in the form of junk mail, telemarketing phone calls, or by E-mail is notoriously unpopular with consumers.

The rapid expansion of E-mail as a means of communication has made unsolicited advertising particularly obnoxious. Not only does the user have to put up with the nuisance value of the material, which in some cases can be quite offensive, but the user actually pays for delivery owing to the costing model for charging of bandwidth. Bandwidth charges are levied on the recipient of any data transfers. Although this cost is initially borne by the ISP, it is passed on to users in the form of usage charges.

EFA submits that the direct marketing exception should be replaced with an "opt-in" provision that permits the use of personal information for direct marketing purposes only by specific prior consent. Sanctions should be applied to breaches of this principle.

4. Other exceptions and problems with the Principles

EFA holds the view that Privacy Principles should consist of an easily understood and briefly stated set of rules that can be applied generally. Any exceptions should be justified on a case by case basis under approved Privacy Codes. When the National Privacy Principles were first promulgated by the Privacy Commissioner in 1998, the simple statement headings were qualified by large numbers of exceptions. The current Bill has taken this unfortunate situation a step further by adding more qualifications and further weakening the Principles. EFA believes it is wholly inappropriate to build such exceptions into legislation. The Canadian Act (referenced below) provides an excellent example of a more appropriate approach to legislative integration of privacy principles.

The qualifications placed on the application and enforcement of the Principles severely impair the effectiveness of the Principles in providing fair treatment of privacy. Changes to previous drafts and failure to define important terms require the Principles to be reviewed in full by process of community consultation.

Prior to the introduction of this Bill, the Principles were understood to represent a bona fide attempt to establish a series of basic protections for personal data and against undue intrusion. Eroded by exceptions, provisos and definitional deficiencies, the Principles no longer achieve a useful purpose, especially in an environment of self-regulation.

There are fundamental problems with the way this Bill treats the most sensitive of personal information in the health industry and in the workplace. Much work is needed to balance the rights of patients and employees with the sweeping exemptions gifted to the holders of personal data of particular sensitivity.

5. Exception for Existing Data

Division 3 Clause 16C(3) (Approved privacy codes and the National Privacy Principles)

provides:

> *(1) National Privacy Principles 1, 3 (so far as it relates to collection of personal information) and 10 apply only in relation to the collection of personal information after the commencement of this section.*
> *(2) National Privacy Principles 3 (so far as it relates to personal information used or disclosed), 4, 5, 7 and 9 apply in relation to personal information held by an organisation regardless of whether the organisation holds the personal information as a result of collection occurring before or after the commencement of this section.*
> *(3) National Privacy Principles 2 and 6 apply only in relation to personal information collected after the commencement of this section.*
> *(4) National Privacy Principle 8 applies only to transactions entered into after the commencement of this section.*

The exemption from Principles 2 and 6 is unreasonable. Principle 2 (Use and Disclosure) and Principle 6 (Access and Correction) are important privacy principles that apply irrespective of whether the data is in existence prior to the commencement of the legislation. It is recognised that some organisations may require time to organise their procedures to take privacy rights into account. However, this should be accommodated by allowing a transition period of say, 12 months, rather than a blanket exemption.

6. Small Business Exemption

No justification has been provided for exempting small business operators from compliance with this legislation. (Schedule 1, 6C,6D,6E)

Privacy rights do not disappear just because a consumer happens to be dealing with a small company. The responsibility upon commercial organisations to recognise the privacy rights of consumers does not magically become apparent when an organisation's revenue base exceeds some arbitrary figure.

All organisations, large and small, need to take consumer privacy obligations seriously. No other countries of significant standing in this field have found it necessary to exempt small business and EFA questions whether business organisations in Australia have even raised this issue as a major concern. It seems most unlikely that small businesses would incur any significant compliance costs if strong privacy legislation were to be introduced.

In conjunction with the *related body corporate* provision, this exemption could conceivably be used by large organisations with complex corporate structures to evade their responsibilities by transferring data collection activities to an smaller entity.

The small business exemption also poses a major problem in relation to global trading on the Internet. Both local and overseas customers will have no way of knowing what size organisation they are dealing with, and given that consumer confidence is vital in building good customer relationships, Australian traders are likely to be bypassed in favour of suppliers from countries that have introduced good privacy law. This will affect all Australian E-commerce traders, since customers will assume the worst once they learn of Australia's half-baked approach to privacy.

EFA therefore strongly recommends that this exemption be dropped.

7. Media Exemption

As a strong supporter of the principles of freedom of speech and freedom of the press, EFA recognises the need for consideration to be given to the effects of privacy legislation on news media. However, the definitions of the terms *media* and *journalism* in the draft Bill are far too broad, and the blanket exemption is considered unacceptable.

The definitions in the Bill (Schedule 1,18-19) are:

> ***journalism*** *means the practice of collecting, preparing for dissemination or disseminating the following material for the purpose of making it available to the public:*
> *(a) material having the character of news, current affairs, information or a documentary;*
> *(b) material consisting of commentary or opinion on, or analysis of, news, current affairs, information or a documentary.*
>
> ***media organisation*** *means an organisation whose activities consist of or include the collection, preparation for dissemination or dissemination of the following material for the purpose of making it available to the public:*
> *(a) material having the character of news, current affairs, information or a documentary;*
> *(b) material consisting of commentary or opinion on, or analysis of, news, current affairs, information or a documentary.*

At Division 1,42:

> *7B Exempt acts and exempt practices of organisations*
> *...*
> *(4) An act done, or practice engaged in, by a media organisation is exempt for the purposes of paragraph 7(1)(ee) if the act is done, or the practice is engaged in, by the organisation in the course of journalism.*

Under the proposed definition, almost any website on the Internet could be considered to qualify, given that almost all web site providers "disseminat[e] the following material for the purpose of making it available to the public: (a) material having the character of ...information...". The proposed media exemption thus appears to sanction a "media organisation" collecting and publishing personal information whether or not such publication is in the public interest.

EFA believes it is unlikely that the proposed definitions and exemption could be narrowed in a way that would not be likely to adversely affect freedom of the press. However, there is a need to provide protection for individuals whose privacy may be grossly infringed by unethical persons claiming the broad media exemption.

EFA therefore recommends that, in cases of complaint, "media organisations" should be required to demonstrate that publication of personal information was in the public interest. Such a test should represent no threat to ethical media organisations.

8. Political Parties

No justification has been provided in the Explanatory Memorandum for an exemption from the Act for political parties (Schedule 1,42). Given the cynicism and low esteem with which the public currently regards politicians and political parties, this exemption will be regarded as yet another case of favouritism, privilege, and abuse of power. Political parties should be treated no differently from any other organisation in respecting the privacy rights of Australian citizens. To do so is to send a message that the Privacy Act is only a token gesture, to be evaded when it happens to suit particular vested interests with the political clout to get their own way.

The exemption for political parties is likely to be exploited in several ways:
(a) Bogus political parties being formed by commercial marketing interests;
(b) Abuse of personal data gathered by political parties;
(c) Laundering of data obtained by and destined for commercial marketing interests by political parties.

Again, no other country which has introduced adequate privacy law has seen fit to provide such an exemption, yet their political systems manage to comply with the law. EFA therefore strongly objects to the inclusion of this exemption in the Bill.

9. Enforcement Issues

EFA finds the enforcement provisions in the Bill confusing and unclear, like much of the rest of the document. One is invited to question whether Members of Parliament can adequately research and exercise their democratic responsibilities when legislative drafting borders on the incomprehensible. Thanks to the Internet, the law of the nation is no longer the exclusive preserve of lawmakers, lawyers and the courts. It therefore behoves the drafters of new legislation to strive for ease of comprehension by those who are subject to the law.

Given that the Bill purports to encourage self-regulation by industry, presenting a Bill that requires industry to seek legal interpretation and development of compliance strategies adds to the impression that the law is only intended to bind big business.

The Bill should contain enforcement procedures that persuade compliance from both big business and small business, notwithstanding that it is in the direct financial interests of industry to market data to the limits of the law.

What is needed is a clear statement of the responsibilities of the Privacy Commissioner or his/her delegate to approve codes, hear complaints, issue directives, make determinations, undertake privacy audits and take legal action.

Unfortunately the Office of the Commissioner has been inadequately resourced to undertake such functions even if the legislation accorded the necessary powers. Furthermore, recent incumbents in the position have been disinclined to act as independent public interest watchdogs but have instead acted as career public servants accountable to the government of the day rather than the Parliament.

Another weakness in the Act is that there are no requirements for organisations subject to the Act to provide a complaints mechanism. Such a mechanism should also be part

of any approved privacy codes.

Without adequate complaints handling procedures, backed up ultimately by strong legal sanctions, the Bill will be a totally ineffective and token piece of legislation.

10. Lessons from other countries

EFA strongly urges the Committee to compare the provisions of the Australian Bill with privacy legislation enacted in other jurisdictions, especially New Zealand, Hong Kong, the U.K. and Canada.

For example, the Canadian *Personal Information Protection and Electronic Documents Act* (Bill C-6), received Royal Assent on April 13, 2000 and comes into force on January 1, 2001. The Act contains no exemptions for small business, political parties or direct marketing, although there is an exemption that applies to an organisation that collects data for "a journalistic, artistic or literary purpose".

The Bill applies to any commercial activity within the legislative authority of the Canadian Parliament, covering any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership of other fundraising lists.

On January 1, 2004, the law will extend to every organization that collects, uses or discloses personal information in the course of a commercial activity within a province, whether or not the organization is a federally-regulated business or not. However, the federal government may exempt organizations and/or activities in provinces that have adopted privacy legislation that is similar to the federal law.

In February 2000, Senator Alston released the Australia-Canada Joint Statement on Global E-Commerce, saying "The statement records a joint commitment to improving the international protections for intellectual property, personal privacy and consumer rights."

The joint statement included the following:

> *Australia and Canada will work together and through international organizations to develop a global environment which facilitates the growth of global electronic commerce by:*
>
> *1. Building trust for users and consumers - ensuring that frameworks and safeguards provide confidence in the digital marketplace by addressing such issues as privacy, security, and consumer protection.*
> *...*

Key priorities for joint work over the next year include:

> *d. Privacy - Ensuring effective protection with regard to the processing of personal data on global information networks begins with domestic regimes for the protection of privacy and personal information. Canada and Australia have committed domestically to a 'light' legislative regime, based on standards developed from the OECD Privacy Guidelines, in an effort to augment self-regulatory efforts, such as voluntary codes, with independent oversight and legal redress for consumers.*

Canada and Australia agree to conclude agreements on the harmonization of their respective legislative frameworks as those frameworks proceed.

It is difficult to understand how Australia and Canada can hope to harmonize their laws in this area when Canada has strong privacy legislation with no real exemptions while Australia is planning to introduce a weak set of privacy principles and to allow massive exemptions for direct marketing, small business, and other interests.

It is also questionable whether Canada will allow commercial data transfers to Australia once the weaknesses in the Australian legislation are made known internationally.

11. E-commerce implications

Survey after survey has indicated that privacy and security concerns are the main reason for reluctance of Internet users to engage in online transactions.

In February 2000, the Australian law firm Freehill Hollingdale & Page released a report outlining this problem. While 41% of Australian adults have accessed the Internet, only 5% have used it for online shopping. The report found that privacy concerns for Internet users involve:

- *concerns about the security of sensitive personal information*
- *uncertainty about how personally identifiable information will be used or disclosed by the recipient organisation*
- *the desire to avoid unsolicited advertising material and other intrusions into an individual's personal cyberspace*

Although there were some encouraging findings about adoption of privacy practices by website operators, only 12% of respondents' websites carried privacy statements.

Other surveys (see References section) that have researched similar issues have included:

- IBM Multi-National Consumer Privacy Study, November 1999, which reported "a study from more than 3,000 who responded in the United States, the United Kingdom and Germany shows a universal consumer interest in online privacy protection." 78% of users refused to provide personal data online.
- A Roy Morgan survey, published in August 1999, found that "the majority of Australians (56 percent) are worried about invasion of privacy issues created by new information technologies."
- Internet.com's E-Commerce Guide, August 16, 1999 reported:
  "The No. 1 reason among online users who have yet to make an e-commerce purchase: lack of trust. In a new survey, a staggering 69.4 percent of reluctant e-shoppers cited fear that personal information would not be kept private by e-tailers as the major reason they shy away from purchasing via the Internet."
- in 1998, Australian Business Advisers Privacy Survey *Which Australian web sites*

care about your privacy? reported:
"Amazingly, only 6% of the 129 web sites surveyed by Australian Business Advisers promised not to disclose your personal information. Eighty eight percent of sites did not mention anything about what they would do with any information collected from users. And disturbingly, 5% of web sites stated that any and all information collected was deemed to be non-confidential and can be used in any way they chose, including disclosure to others 'without limitation'."

- A survey carried out by Boston Consulting Group (BCG) in 1998 confirmed that privacy and security fears do inhibit the take-up of electronic commerce on the Internet. The survey concluded that as much as 6 billion US dollars would be lost between now and the Year 2000 in potential electronic commerce revenue if privacy concerns were not addressed.

In view of these concerns, it is quite astounding that Australia proposes to introduce such weak Privacy legislation, especially as it encourages secondary use of personal data for direct marketing, despite massive user concern about such practices.

If Australia wants to be a serious player in the global information economy, it will have to adopt international best practice. The current Bill is far below the standard required and indeed adopted by other countries. Even the proposed "safe harbor" concept being put forward by the USA provides stronger protection than the Australian Bill.

12. Conclusions

While EFA supports in principle the introduction of a co-regulatory scheme, the proposed Bill is a totally inadequate response to the protection of privacy that is out of step with world's best practice.

The major deficiencies are:

- the Bill contains too many exemptions and exceptions and totally fails to come to grips with consumer privacy needs in the 21st century.
- The exception to the Privacy Principles in relation to direct marketing is contrary to international developments and effectively legitimizes the practice of "spamming" (the sending of unsolicited E-mail advertising) on the Internet.
- The exemption for small business is unjustified
- The Bill will cause Australia to have a poor international reputation in privacy protection that will hamper attempts by E-commerce vendors to attract overseas customers.
- The exemptions for the media are too broad and could include almost every existing website. A public interest test should be applied in response to privacy complaints.
- The exemption for political parties is unjustified will lead to unintended consequences.
- The broad exemption for pre-existing data is unacceptable. A transition period

should be provided for existing data uses to comply with the all Principles

- Enforcement provisions in the legislation are inadequate.
- Instead of empowering individuals to exercise their right to privacy of personal data, the Bill confers on certain business interests the right to invade individual privacy.

In summary the Bill is at best a token attempt to introduce privacy legislation. It is complex, unwieldy, ineffective and an insult to the citizens of Australia. The Bill needs to be re-drafted, preferably as a replacement for, rather than an amendment to, the Privacy Act 1988.

13. Recommendations

EFA strongly recommends that the Bill should be re-written as a Bill for an Act replace the Privacy Act 1988, rather than attempting to amend the existing Act.

The following changes to the existing provisions should be incorporated:

- The Privacy Principles should be re-drafted to a simple statement of the principles, without the current raft of qualifying statements and exceptions.
- Any exceptions to the principles should be codified in industry privacy codes that are subject to public review and approval by the Privacy Commissioner.
- The Privacy Commissioner's office should be properly resourced and should report to the Parliament as a truly independent public interest watchdog.
- There should be no exemptions from the Act for special interest groups such as direct marketing, small business and political parties.
- Secondary use of personal data should only be permitted with the express consent of the individual concerned.
- *Media organisation* should be required demonstrate public interest where the Privacy Principles are infringed.
- Any exception for existing data should be subject to a transition period, and should not except Principle 2 (Use and Disclosure) and Principle 6 (Access and Correction).
- Enforcement provisions in the Act should be strengthened so as to place a clear responsibility on the Privacy Commissioner to resolve complaints, and to provide for comprehensive legal remedy for infringements of the Act or approved privacy codes.
- A study should be made of international responses to privacy in terms of legislation already enacted in Canada, New Zealand, Hong Kong and the U.K.
- The implications of the EU Directive on Data Protection in respect of Australian industry should be examined in more depth.

- More notice should be taken of the need for strong privacy protection to boost Australia's participation in global e-Commerce.

---

14. References

OECD Privacy Guidelines 1980
http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-en.HTM

Beyond the OECD Guidelines: Privacy Protection for the 21st Century - Roger Clarke, 2000
http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html

The European Union Directive 95/46/EC On the protection of individuals with regard to the processing of personal data and on the free movement of such data.
http://www.privacy.org/pi/intl_orgs/ec/final_EU_Data_Protection.html

National Principles for the Fair Handling of Personal Information - revised edition, January 1999
Australian Privacy Commissioner
http://www.privacy.gov.au/publications/index.html

Canada-Australia Joint Statement on Global Electronic Commerce Feb 2000.
http://www.noie.gov.au/projects/international/bilateral/canada.htm

Canadian Personal Information Protection and Electronic Documents Act, Bill C-6
http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6TOCE.html

Canadian Privacy Commissioner's page about the Personal Information Protection and Electronic Documents Act
http://www.privcom.gc.ca/english/02_06_e.htm

A Guide to Bill C-6 - An outline of Canada's Personal Information Protection and Electronic Documents Act as of April 15, 1999 (does not include all amendments) by privacy consultant Murray Long.
http://www.privcom.gc.ca/english/02_06_02b_e.htm

The New Zealand Privacy Act 1993
http://www.knowledge-basket.co.nz/privacy/legislation/1993028/toc.html

UK Data Protection Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

International Safe Harbor Privacy Principles
http://www.ita.doc.gov/td/ecom/shprin.html

Internet Privacy Survey Report 2000 - Freehill Hollingdale & Page
http://www.freehills.com.au/

E-Businesses Exhibiting Privacy Leadership Get the Sale IBM Multi-National Consumer Privacy Study, November 1999
http://www.ibm.com/security/library/wp_priv-survey.html

Big Brother Bothers Most Australians - Roy Morgan Research
(Finding No. 3221. Published exclusively in the Bulletin, cover date August 30, 1999)
http://www.roymorgan.com/polls/1999/3221/

Consumers to E-Tailers: Don't Kiss and Tell - from internet.com's E-Commerce Guide, August 16, 1999.
http://cyberatlas.internet.com/markets/retailing/print/0,1323,6061_183301,00.html

Which Australian web sites care about your privacy? Australian Business Advisers Privacy Survey 1998
http://www.abaconsulting.com.au/privacyart.htm

Electronic Commerce: Legal and Consumer Issues - Chris Connolly - reports on a survey carried out by Boston Consulting Group (BCG) in 1998
http://www2.austlii.edu.au/itlaw/articles/Connolly.html