

# **'Information Wants to be Free'**

**by Richard Hemsworth**

**Area of Interest: Digital Communities Law and Policy**

## **Introduction**

The development of information technology and the internet has dramatically increased the quantity of information available in digital form. This has resulted in a proliferation of uses of personal information. While data-mining and data-matching of existing information may allow individuals to be provided with goods and services that save them time and effort, some of the uses of personal data have major implications for the privacy of individuals.

The inherent limitations of paper-based systems provide a certain level of privacy protection. (Lessig, 1999, p151) The migration of records of personal information to IT systems has made possible a far greater range of uses of personal information and has made it easy to transfer information. The internet has made the solicitation and collection of information easier, and indiscriminate. (Australian Privacy Commissioner, 2001)

It has been argued that internet privacy polices should be national (or preferably international in scope), thus avoiding a patchwork of state and local jurisdictional mandates. A uniform framework that promotes the growth of interstate and international e-commerce, minimizing compliance burdens, sustaining a national marketplace and making it easier for consumers to protect their privacy. The quagmire of social, ethical and legal issues surrounding business and trade through a digital medium are yet to be resolved and are only now coming to the forefront of sensible public scrutiny. (Clarke, 2000)

## **Scope**

This paper recognises the increasing public sensitivity to privacy on the internet (including other digital communication systems). It initially specifies the mechanisms for the annulment of peoples' expected rite to privacy, delivers examples of digital community practice, explores the policy issues around what can be done to address community privacy concerns, and then specifically details the Australian attempts to deal with these issues.

## **Data Surveillance and Privacy Threats on the Web**

Physical and electronically enhanced monitoring of individuals and groups is an expensive process. While older techniques like surveys, questionnaires and form-filling (even if for some reward or discount) are still extensively used (Dyson, 1998, p248), they are being replaced by sophisticated and automated measures that are not always obvious to the patron. (Clarke, 2000) The level of privacy that is required should be a choice that individuals make, rather than a secretive collection where the user has no control and no awareness of the invasion. (Australian Privacy Commissioner, 2001b)

Over 97% of all internet and email users are unaware of the methods that are used to automatically collect data on their transactions. (Roy Morgan, 1999) Some of those methods include:

- a. Cookies, that for most users (who access the internet through a public ISP) are essential to ensure that each request is linked to the previous request. Cookies allow web site operators to assign a unique permanent identifier to a computer which can be used to associate the requests made to the web site from that computer. Cookies indicate to a web site that a user has been there before and can be used to record what parts of a web site a user visits.

While cookies in themselves may not identify a user, in the way a name or address does, a cookie can potentially be linked with other identifying information. For example, if a user provides extra information about themselves to the web site by buying something online or subscribing to a free service, then the cookies can be used to build up a profile of the user's buying habits and what they are interested in.

The issue is so well recognised that privacy software exists to circumvent the problem. Products like 'Cookie Cutter' and 'Window Wiper' remove cookies and prevent new ones being added; the new versions of browsers allow the user to turn off the cookies, and 'Potato' allows users to protect their identity by creating false identities. (Smith, 2001)

- b. HTTP and Languages. Lessig (1999, p3) says that 'code is law', and he identifies that the code (architecture and programming languages) control what is permissible. When a user accesses a web page from a web site, the web site expects certain information so that it can provide the page requested. The HyperText transfer protocol (HTTP) is the set of rules that web sites and browsers follow in order to communicate.

One piece of information the web site will require is the Uniform Resource Locator (URL), that is the page the user wants to look at. Other information that may be sent whenever the user requests a web page includes the users e-mail address and the last web page viewed. Marketers can use this information to track individual buying habits and interests, and hence target unwanted advertising to the user. As an example, a user may not want his application for employment to be logged with a reference that she visits pornography sites - yet this data is automatically supplied. (Ho, 2001, p2)

Equally, Java Script has features that allow automatic on-forwarding of emails to the original sender, without notification to the user. Protection of Intellectual Property or even a user's own opinion becomes difficult when any response to an email is automatically sent to the originator. (Smith, 2001)

- c. The Browsers themselves have bugs (that are regularly fixed), but not before information about the user has been supplied to a collection agent. The browsers also automatically supply the libraries and capabilities the users have loaded to the web-pages being requested. While this allows the web service to display and send appropriate data, it also reports more than is necessary

allowing the accumulation of profiles on software usage and previous information collected by the user.

- d. Data already exists on most people and automatic 'worm' programs can scour the net for this data. Governments (through publicly accessible data, like ABNs), listings of Directors of companies, school and volunteer sites listing occupants of voluntary positions, telephone directories and electoral roles; all provide data that can be mined to provide a comprehensive view of an individual.

Much personal information, which is publicly available, has been collected and combined into databases by web-based companies that then sell this information to businesses or individuals. Comprehensive and sometimes inaccurate profiles of individuals can be derived by combining information from many sources. As there is little or no law anywhere in the world governing this sort of activity, there is very little an individual can do about it other than raise their level of awareness. (Clarke, 2000)

- e. Requests for downloads of shareware and freeware provide even more data on the interests of individuals, while search engines allow information about an individual's interests to be logged. Search engines also allow email addresses and names of individuals to be found in news groups and chat rooms.
- f. Buying a product from a commercial website usually entails the use of a credit card and although most sites use an encryption system, the data is then sometimes stored on accessible servers. Internet commerce exposed individuals to privacy risks in that they are required to provide more information than for a counter purchase. (EPIC, 1997)
- g. E-mail is more like a postcard than a letter; anyone can intercept it and read it. (Clarke, 2000) The 'Finger' utility allows email addresses to be searched and information found about the owner. In 1996, Standards Australia released a document titled 'Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia to attempt to ensure the security of email communication. (Australian Privacy Commissioner, 2001) Although the Government agreed to facilitate the creation of a new peak body to oversee the development of a national system for online authentication, there has been little progress, leaving consumers exposed or needing to employ their own encryption methods like Pretty Good Privacy (PGP). (Freehill, Hollingdale & Page, 2000)
- h. Spam invades users privacy and costs them money and time to download. This unwanted junk email is sometimes sent using randomly-generated addresses, but more commonly the lists come from NewsGroups or public sources. Sensitivity to Spam has increased with more aware advertisers offering to remove users from the list of recipients on request.

While net-users commonly believe that legislation is the only way to control this 'invasion of privacy' (Clarke, 2000), some users groups have formed to combat spamming by direct action against the perpetrators, jamming their web

sites or using virus-like software to incapacitate their Ebusiness offering. (Branscomb, 1995)

- i. Internet relay chats offer a great risk to privacy with, in extreme cases, assaults and rapes being reported from resulting relationships. While anonymity can be achieved, it is also possible for chat participants to falsely identify themselves leading netizens to cry: 'caveat emptor'. The architecture provides an ability to hide or make ambiguous who is being dealt with. As a related issue, 'trust' cannot readily be established. (OECD, 1999; EPIC, 1997)

The litany of possible infringements of privacy is significant and Lessig's four factors that mitigate behaviour (customs, laws, markets and architecture) each have a role to play in addressing these. The factors are not always mutually exclusive or independently applied, nor are they necessarily supporting of each other. Digital community practice applies a variable standard of ethics and acceptable behaviour depending on where the user is (in a geographical or jurisdictional sense) and who the user is (applying a corporate versus personal distinction).

### **Digital Community Practices**

In conducting business across the net, the same legal issues that plague bricks and mortar business operations are likely to occur. They are not necessarily more complex, just different. (Dyson, 1998, p126) Lessig (1999, p151) uses the issue of privacy to illustrate the similarities between data collection now and data collection before the internet. His distinction is primarily that data in the past was imprecise and had human recollection as its collection and storage agent. With modern monitoring, data is machine collected and archived for posterity. People's lives become an ever-increasing record.

The Australia Card was quashed as an invasion of privacy, yet ten years later databases have been established to track every visit to any doctor or any use of the medical system. Albeit a trial in New South Wales, if successful: all pharmacists, doctors, health clinics, hospitals, and child welfare agencies will be added to the system. Other government and private agencies 'may be added' in the future. (Department of Health Media Statement, February, 2001) Community consultation did not occur and legislative control for the introduction of this type of mass data accumulation does not exist. (Clarke, 2000)

While the government's life mission could arguably be to collect data, private industry is not far behind. 92% of commercial websites collect personal data from Web users. If the contention that privacy is about the ability to control data about oneself, is accepted, and if an individual has no control over the retention of data about himself or herself, then perhaps there is no privacy. (Privacy Exchange Archives, 2001)

Ho (2001, p1) describes the appointment of Chief Privacy Officers in corporations in response to the Federal Government's new privacy laws as 'installing a human firewall'. The compliance issue is strictly in response to new laws, dampening the idea that self-regulation of communities is likely to be an effective control mechanism. All 500 members of the Direct Marketing Association are appointing compliance officers to ensure that privacy of client data records is maintained.

Similarly, Toysmart which has TRUSTe licensing and guarantees customer privacy, listed its 190,000 person database as an asset in Bankruptcy hearings. It then offered the list for sale. Toysmart withdrew the list from sale after public and media derision citing that 'no reasonable offers were made'. The State Attorneys in 43 US states also threatened to sue to protect public privacy. This begs the question: what use is self-regulation, if third-party sureties (like TRUSTe) are ignored? (New York Times, 2000)

The profit motive and commercial interests have had significant impact in the United States recently with the US Bush administration sending a letter to the European Commission protested against model contract terms agreed by the EU for the transfer of personal data. (Financial Times, March 29, 2001) At least this is consistent with Bush's greenhouse gas back-down. As 60% of all internet traffic is based within the United States, an argument could be mounted that it would be difficult to enforce privacy rules when the main player rejects the rules.

In assignment 1 for Law521, insurance companies were reviewed in terms of visitor data collected by their website. The top 20 (by market capitalisation) all retain an automatic table of web identifiers of people who had visited their site. They claim this was for security reasons. They all also asked for details about the visitor, but only if the individual was interested in a product offering. None of the sites moved to an encrypted or otherwise secure environment to transfer this data except where they asked for payment using a credit card or Bpay facility. Of direct relevance, in the United States, District Judge Naomi Reice Buchwald of the US District Court dismissed a class action suit against DoubleClick Inc saying that 'the placing of 'cookies' on a computer user's hard drive by an Internet advertising agency was not an invasion of privacy', thereby legitimising the automatic data collection for internet advertising purposes. (DoubleClick Inc. Privacy Litigation, 00 Civ. 0641 (NRB) New York Southern District) (Ricardi, 2001)

The inconsistencies in digital community practices; either trans-border, across related areas or reversals over time, are likely to result in a rising level of suspicion from the general public and an increasing level of mistrust.

As a further inconsistency, the US House of Representatives Commerce committee unanimously approved an amended version of HR 718, the Unsolicited Commercial Electronic Mail Act of 2001, this week. (Tech Law Journal, March 2001) The bill allows individuals to opt-out from unsolicited commercial e-mail. This anti-spam legislation still does not stop spamming, it just provides legislative muscle for individuals who want to be removed from mailing lists.

The architecture also inconsistently applies practices, with Microsoft's new Internet Explorer 6 defaulting to allow cookies and personal data transmission to commercial information gathering websites while Netscape is implementing P3P with defaults set to provide absolute privacy. Given the level of understanding in the general community about cookies and the permissions that can be given regarding information flow, it is unlikely that most individuals will be able to make informed choices. (Junkbusters, 2001)

**Privacy Versus Freedom - Policy Issues** (Free Speech or Cyber Censorship)

Establishing limitations on the collection and distribution of data, some would argue, imposes a significant burden on the rights of people to free speech. While a number of countries have embedded free speech within the governing laws and constitutions, there are few who have embedded the right to privacy. Defamation, censorship to protect minors, copyright, libel and false promise laws (including trade practices legislation) act to prevent incorrect, previously owned or morally offensive information from being distributed. None act to guarantee the privacy of the individual as an inalienable right. (Clarke, 2000)

In many ways, the privacy lobby is at odds with groups demanding fully open systems involving freedom of information and freedom of speech. Information broadcast in the public interest often defies an individual's claim to privacy for what is said to be the public good. Libertarian supporters of this argument often cite Aristotle's ethical position that this unauthorised release of information forsakes the 'good' of the individual. Utilitarian interests say they have an interest in the body corporate and are prepared to allow interference with others to promote the greatest good for the greatest number of people, even though individuals can end up worse off. (Shaw and Barry, p103)

Sun's CEO Scott McNeely's gave a speech to the Computers, Freedom and Privacy Conference (1999) entitled: 'There is no privacy: get over it' and came under vitriolic attack for his 'casualness with other people's privacy'. (Davies, 1999) Moral and ethical positions are greatly varied, allowing arguments to fester and legislators and esystem participants to sway in their support for particular behaviours.

While the community vacillates and legislators are moved by influential lobbyists, there are other alternatives to privacy legislation.

George Vradenburg of AOL asserts that self-regulation works, through mechanisms such as the Privacy Alliance and TRUSTe. His focus is on freedoms, rather than on privacy and regulation. Both Microsoft and AOL have been significantly impacted by the voices documenting and attacking privacy-abusive practices. Supporters argue that market pressures are real, and that regulatory regimes of the past are not the only approach needed. (Clarke, 2000)

There are still those that are promoting regulatory practices. US Congressman Ed Markey (Electronic Bill of Rights Act) introduced a private member's Bill into the House in March 1999 to address medical privacy. As at 28 February 2000, President Bush put this legislation on hold stating that more general legislation needed to be enacted. (Wall Street Journal, 2001) It has the following rules:

1. Written consent is generally required before using a person's health information (but marketing exemptions will exist).
2. There are provisions to prohibit the coercion of consent by unfairly conditioning benefits on it.
3. The rule applies equally to electronic, paper, and oral information.
4. People will have the right to access their own medical files and to request amendments or corrections.
5. Employers who administer their own health care plan must not use medical information for anything other than health care. (Known as purpose specificity in privacy law.)
6. States may pass stricter laws if they wish.

7. People have right to a 'disclosure history', detailing the entities that received their personal data. (Junkbusters, 2001)

Regardless of the Markey's success or failure with the Electronic Bill of Rights, legislative measures have been inconsistent across jurisdictions, with German Federal judges unwilling to attempt to enforce pornography or copyright infringements outside their territory. On the other hand, US Federal Courts (based on the precedent of child sex abuse cases) are prepared to prosecute US citizens once they return to US territory, even if the offence occurred outside the territorial limits of the US. This inconsistency promotes unease in the internet community and has stakeholders looking for alternatives.

A multifaceted approach using privacy-enhancing technologies such as P3P, as well as statutory intervention to ensure privacy protection in the private and public sector seems likely. (Clarke, 2000)

With regard to self-regulatory measures such as TRUSTe 'certified' privacy statements, some authors query the value of privacy statements that are difficult to find, difficult to read, and/or difficult to understand. More fundamentally, privacy statements can be likened to a note left by a burglar explaining what he will and will not do with the goods he has stolen. (Jacobus, 2000)

Self-regulation can come in a number of forms: professional responsibility being another of them. From the LAW521 forum comes an example of misuse of professional responsibility that was not upheld by the law. In the Andersen Consulting LLP v. UOP and Bickel & Brewer, Case No. 97 C 5501 (D. Ill. Jan. 23, 1998), the plaintiff was hired to perform a systems integration project for the defendant UOP. The plaintiff was given access to, and utilized, defendant UOP's internal e-mail system to complete the work. After a dispute arose between the parties over plaintiff's performance of this assignment, defendants sent e-mail authored by plaintiff to a newspaper, which published the same. The plaintiff commenced suit, arguing that such unauthorized transmission of its e-mail constituted a violation of the Electronic Communications Privacy Act, 18 U.S.C. Section 2701 et seq. The court disagreed, and dismissed plaintiff's complaint. (Law521 Forum, 2001)

While the case may have been lost, there is an argument that users have a professional responsibility and should act to do the right thing. Only 'custom' would now seem to oblige the defendant to protect the privacy of his corporate client.

### **Australia's Privacy Issues**

The Privacy Act was passed by Federal Parliament at the end of 1988. The Act gave effect to Australia's agreement to implement guidelines adopted in 1980 by the Organisation for Economic Cooperation and Development (OECD) for the protection of privacy and transborder flows of personal data, as well as to its obligations under Article 17 of the International Covenant on Civil and Political Rights.

The Act had a two-pronged objective: the protection of personal information in the possession of Federal government departments and agencies and safeguards for the collection and use of tax file numbers (the latter connected with the up-grading of the tax file number system following the demise of the 'Australia Card' proposal).

In 1991, two major additions were made in the areas of credit reporting and data matching. The credit reporting jurisdiction was the first major extension of the Act to a private sector area of activity and generated significant involvement with the private sector in the development of legally-binding rules for the handling of credit information. The data-matching jurisdiction led to the creation of a separate unit within the Privacy Commissioner's office dedicated to the oversight of the Commissioner's responsibilities under the Data-matching Program (Assistance and Tax) Act 1990.

The Privacy Commissioner acquired additional functions under amendments to the National Health Act (passed in 1991) in relation to guidelines for the operation of the eligibility checking system between pharmacists and the Health Insurance Commission. That system is now undergoing trials for delivery through the internet. (Australian Privacy Commissioner, 2001)

The Privacy Commissioner again increased his Jurisdiction with changes to the Telecommunications Act 1997 in relation to records made by telecommunications carriers, carriage service providers and others of their disclosures of customer information. The Act also provides for industry codes and standards of conduct in a range of consumer protection areas including privacy, for which the Privacy Commissioner must be consulted. The codes are voluntary in the first instance, but breaches can be enforceable by the Australian Communications Authority. (Australian Privacy Commissioner, 2001)

In comparing Australia to the United States; Australia has made significantly more progress than the US towards protecting computerized personal data. Australia already has a law covering the government's collection and use of personal information; and January 2001 saw the Privacy Amendment (Private Sector) Act passed to cover private corporations as well. (Freehill, Hollingdale & Page, 2001) (Kennedy, SMH, 20Feb2001) In contrast, the United States Congress lacks a single bill addressing general issues in privacy, although a few existing and proposed laws cover isolated types of data. (Oram, 1998) Why is this the case?

Perhaps the difference is that privacy advocates are better organised in Australia. There has been a loosely organised privacy lobby in Australia for over twenty years, which has become more focused recently. The threat of a national ID card in 1987 generated 'the largest public protests since the Vietnam War' (Oram, 1998) and continued high profile lobbying by people like Greenleaf and Clarke has had an impact on the Australian debate and policy. (Greenleaf, 1998) (Freehill, Hollingdale & Page, 2000)

Clarke (1997) is of the view that 'purely self-regulatory schemes have been given their opportunity, and have failed to deliver.' The Federal and State governments appear to agree, with extensive legislation already in place and further changes likely. (Ho, 2001)

Australian views vary greatly, but the independence of the Australian psyche is likely to want the level of privacy to be a choice made by the individual. (Oram, 1998) This independence concept seems to be being supported by US legislation as well (for example the US opt-out provisions for commercial email), new software like Internet Explorer 6, commercial market sensitivity with the appointment of Privacy Officers, and architectural reinforcements like P3P.

## **Conclusion**

The early part of this paper listed a litany of ways that individual privacy can be invaded; how choice can be removed from the hands of the individual and how thoughtless technology can be used to compromise what some people believe should be an undeniable rite to control information about oneself. It also described the ways that techno-savvy individuals were able to mobilise public and political support to set standards independent of legislation.

Later came the consideration of privacy versus freedom, including a fatalist premise that 'privacy is already gone and therefore individuals shouldn't worry about it' (put forward by Sun Microsystem's CEO). While this contemptuous parent-child transaction can be dismissed as a one-sided technologist's view, it does point out the significant momentum that Lessig's architecture has in defining the standards of acceptable behaviour.

'Digital law' (the statutes and regulations) are always going to be responsive rather than proactive because of their nature; and the market (lead by its representatives, as exemplified in George W. Bush's response to the EU privacy data exchange protocol) will lobby for maximum profit and maximum advantage to the commercial constituents, leaving individuals running a slow second.

That then only leaves the 'Customs' expressed through 'netiquette' norms to ensure a balance in the privacy debate. And while consistency has not been well evidenced, particularly through geographical jurisdictions, it does provide a counterpoint to the march of personal privacy invasion.

The Chinese language has no words for privacy, yet Hong Kong introduced the Hong Kong Data Protection Law that protects individual privacy. They needed a descriptor and so now have a composite word: 'self-hide'. Perhaps this composite word defines the locus of control for privacy where it should be: with the individual.

## Bibliography

- Australian Law Reform Commission. (2000). *Annual Report 2000: R90*. Government Printer: Canberra.
- Australian Privacy Commissioner. (2001). *Australia's privacy laws*.  
[http://www.privacy.gov.au/issues/p7\\_1.html](http://www.privacy.gov.au/issues/p7_1.html)
- Australian Privacy Commissioner. (2001b). *National Principles for the Fair Handling of Personal Information*.  
<http://www.privacy.gov.au/publications/npps01.doc>
- Australian Taxation Office. (1997). *Electronic Commerce Project: 1 August 1997*. Government Printer: Canberra. [http://www.ato.gov.au/content.asp?doc=/content/business/ecommerce\\_Ecp.htm](http://www.ato.gov.au/content.asp?doc=/content/business/ecommerce_Ecp.htm)
- Bolman, Lee G. and Deal, Terrence E. (1997). *Reframing organisations: artistry, choice and leadership*. Jossey-Bass: San Francisco.
- Brailov, Marc. (2001). *Trade association releases guidelines for preemption legislation*. Business Wire, 18 January 2001.  
[http://www.aeanet.org/aeenet/PressRoom/pradet0000\\_privacyprinciples011801.htm](http://www.aeanet.org/aeenet/PressRoom/pradet0000_privacyprinciples011801.htm)
- Branscomb, Anne Wells. (May 1995). Anonymity, autonomy and accountability: challenges to the first amendment in cyberspaces. *Yale Law Journal: symposium*. Vol. 104, No 7.
- British Home Office. (1998). *UK Data Protection Act 1998*.  
<http://www.hmsso.gov.uk/acts/acts1998/19980029.htm>
- Burnes, B. (1994). Change management: approaches and techniques, in *Managing Change*. Pitman Publishing: London, pp. 149-179.
- CCH Australia Limited (Elizabeth Lovel, ed). (2000). *Master Tax Guide*. CCH Australia Limited Publishing: Sydney.
- Centre for Democracy and Technology. (June, 1997). *Communications Privacy in the Digital Age*. [http://www.cdt.org/digi\\_tele/9706rpt.html](http://www.cdt.org/digi_tele/9706rpt.html)
- Clarke, Roger. (1997). *Privacy advocates and the privacy commissioner's discussion paper of August 1997 regarding (self-)regulation of the private sector*. Version of 10 October 1997. Xamax Consultancy Pty Ltd, Canberra
- Clarke, Roger. (2000). Data surveillance and information privacy: notes from the Computer, Freedom and Privacy Conference 1999.  
<http://www.anu.edu.au/people/Roger.Clarke/DV/>
- Corporate Executive Board. (2000). *Innovation and agility: building the entrepreneurial enterprise*. Corporate Leadership Council: Washington.

- Council of Europe. (2000). *European Treaties concerning Data Protection* (summaries). <http://www.coe.fr/eng/legaltxt/abstracts/epublic.htm>. Summaries and links to treaties.
- Council of Europe. (1999). *Council of Europe Convention concerning automatic processing of personal data*. <http://www.coe.fr/eng/legaltxt/108e.htm>. Convention 108/81.
- Council of Europe. (1999). *Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data*. <http://europa.eu.int/comm/dg15/en/media/dataprot/inter/con10881.htm>
- Cunningham, Michael J. (2000). *B2B: how to build a profitable e-commerce strategy*. Allen and Urwin: New York.
- Davies, Simon. (1999). *Privacy International Directors Review of CFP Conference 1999*. <http://www.cfp99.org>.
- Despeignes, Peronet and Hargreaves, Deborah. (2001). EU-US clash over personal data: private right or commercial opportunity? *Financial Times*, Mar 29, 2001. London.
- Dyson, Esther. (1998). *Release 2.1: a design for living in the digital age*. Penguin Books: London.
- EPIC. (1997). *Surfer Beware: Personal Privacy and the Internet*. <http://www2.epic.org/reports/surfer-beware.html>
- Fites, Philip E. and Kratz, B. (1993). *Information systems security: a practitioners guide*. Van Nostrand Reinhold: New York.
- Freehill, Hollingdale & Page. (2000) *Internet Privacy Survey Report 2000*. <http://www.freehills.com.au/>.
- Greene, Thomas C. (2000). How Carnivore works: sniffing by the FBI. *The Register*, 19 December 2000. <http://www.anonymizer.com/news/index.shtml>.
- Greenleaf., Graham. (1998). *A Proposed Privacy Code for Asia-Pacific Cyberlaw*. <http://207.201.161.120/jcmc/vol2/issue1/asiapac.html>.
- Halsall, Fred. (1992). *Data communication computer networks and open systems*. Addison-Wesley: New York.
- Ho, Christina. (2001). The human firewall, privacy on the internet. *Sydney Morning Herald*, 20 February, 2001; IT News, pp 1-2. John Fairfax Publications Pty Ltd: Sydney.
- Kennedy, Dorothy. (2001). New code for net campaigns. *Sydney Morning Herald*. 20 February, 2001; IT News: p 3. John Fairfax Publications Pty Ltd: Sydney.

- OECD. (1999). Ministerial Declaration on the Protection of Privacy on Global Networks. 18 December 1999.  
[http://appli1.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg\(98\)10-final](http://appli1.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)10-final).
- OECD. (1997). *Guidelines for Cryptography Policy*, including background report on guidelines. <http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.htm>.
- OECD. (1992). *Guidelines for the Security of Information Systems*. including explanatory memoranda.  
[http://www.oecd.org/dsti/sti/it/secur/prod/e\\_secur.htm](http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm).
- Jacobus, Patricia. (2000) *Privacy heats up but doesn't boil over*. CNET News.com, 22 December 2000. <http://news.cnet.com/news/0-1005-200-4238135.html?tag=prntfr>
- Junkbusters. (2001). Microsoft announces P3P implementation, criticized over Hailstorm. *What's news at Junkbusters*: 30 March 2001.  
<http://www.junkbusters.com/new.html>
- Kennedy, Dorothy. (2001). New code for net campaigns: privacy guidelines for direct marketing. *Sydney Morning Herald*, 20 February, 2001; News, p 3. John Fairfax Publications Pty Ltd: Sydney.
- Krol, Ed. (1997). *The Whole Internet*. O'Reilly and Associates: California.
- Kirby, Justice. (1999). Privacy in Cyberspace. University of NSW Law Journal, 20 December 1999.  
<http://www.law.unsw.edu.au/unswlj/e-commerce/Kirby.html>.
- Lawrence, E. Corbitt, B. Tidwell, A. Fisher, J. and Lawrence, J. (1998). *Internet commerce: digital models for business*. John Wiley & Sons Australia Limited: Sydney.
- Levine, John R. and Baroudi, C. (1993). *Internet for Dummies*. IDG Books: San Mateo California.
- Lessig, Lawrence. (1999). *Code and other laws of cyberspace*. Perseus Book Group: New York.
- Luttwak, Edward. (1999). *Turbo Capitalism: winners and losers in the global economy*. Orion Business Books: London.
- National Competition Council. (1999). *National Competition Policy: First Assessment State and Territory Annual Reports, June 1999*. Australian Government Printer: Canberra.
- New York Times. (2000). Judge Overturns Deal on Sale of Online Customer Database. New York Times Publishing, 18 August 2000.

<http://www.nytimes.com/library/tech/00/08/biztech/articles/18toys.html>.

New Zealand Government Printer. (1993). The New Zealand Privacy Act 1993.  
<http://www.knowledge-basket.co.nz/privacy/legislation/1993028/toc.html>

Oram, Andy. (1998). Australian battle: privacy advocates won't back away. *American Reporter*, 10 March 1998. <http://www.american-reporter.com/>.

Peach, Randall J. (2000). U.S. Courts Ask, Does the Internet Make Court Records Too Public? *New Jersey Law Journal*, 22 Nov 2000.  
<http://www.privacyexchange.org/news/archives/usn/usnews0101.html>

Poulsen, Kevin. (2000). Federal judiciary seeks comments on internet access to court documents. *The Register*, 12 January 2000, London.  
<http://www.theregister.co.uk/content/6/15182.html>

*Privacy Act 1988*. (Commonwealth Act No. 119 of 1988). Government Printer: Canberra.

*Privacy Amendment (Private Sector) Act 2000*. (Commonwealth Act No. 155 of 2000). Government Printer: Canberra.

Privacy Exchange Archives. (2001). *Global privacy developments*.  
<http://www.privacyexchange.org/news/archives/archives.html>

Phillips, Heather. (2001). Junk mobile mail fears spark action. *Sydney Morning Herald*, 20 February, 2001; IT News, p 2. John Fairfax Publications Pty Ltd: Sydney.

Riccardi, Michael A. (2001). DoubleClick Can Keep Hand in Cookie Jar, Federal Judge Rules. *New York Law Journal*: 30 March 2001.  
<http://www.law.com/cgi-bin/nwlink.cgi?ACG=ZZZJ4CT8XKC>

Richardson, Louise. (ed). (2000). Australian Netguide. *All wapped out: the internet is everywhere*. 3 March 2000, pp 60-64. Australian Netguide Pty Ltd: Sydney.

Roy Morgan Research. (1999). Big Brother Bothers Most Australians. Finding No. 3221. Published in *The Bulletin*; cover date August 30, 1999.  
<http://www.roymorgan.com/polls/1999/3221/>

Scott, Brendan. (1999). *An Essential Guide To Internet Censorship In Australia*.  
<http://www.gtlaw.com.au/people/bscott.html>, 30 November, 1999. Gilbert & Tobin: Sydney.

Scott, Brendan. (2000). *Internet censorship: Judgment day for the ABA*.  
<http://www.gtlaw.com.au/people/bscott.html>, 15 February, 2000. Gilbert & Tobin: Sydney.

- Shaw, W.H. and Barry, V. (1998). *Moral issues in business (7th edition)*. Wadsworth Publishing Company: San Francisco.
- Smith, Richard M. (2001). *Email Wiretapping: advisory notice*. Privacy Foundation. 5 February 2001. <http://www.privacyfoundation.org/advisories/>
- Strassman, Paul A. (1997). *The squandered computer: evaluating the business alignment of information technologies*. Information Economics Press: San Francisco.
- Stone, Martin. (2001). *Canada privacy law impacts foreign firms*. Newsbytes, 5 January 2001. <http://www.newsbytes.com/news/01/160095.html>
- Tanenbaum, Andrew S. (1989). *Computer Networks(2nd Ed.)*, Prentice Hall international: Amsterdam.
- United Nations. (1990). *Guidelines Concerning Computerised Personal Data Files*, adopted by the General Assembly on 14 December 1990. <http://europa.eu.int/comm/dg15/en/media/dataprot/inter/un.htm>
- Wall Street Journal. (2001). *Clinton administration medical-privacy rules changed not abandoned*. 28 February 2001. [http://www.nj.com/newsflash/index.ssf?cgi-free/getstory\\_ssf.cgi?a0426\\_BC\\_Thompson&&news&newsflash-washington](http://www.nj.com/newsflash/index.ssf?cgi-free/getstory_ssf.cgi?a0426_BC_Thompson&&news&newsflash-washington).
- Walker, David. (2001). *Packaging your way to profit*. Sydney Morning Herald, IT Section, p5. John Fairfax Publishing: Sydney.
- Willcocks, Leslie and Sauer, Christopher. (2000). *Moving to e-business: the ultimate practical guide to effective e-business*. Random House Business Books: London.

### Site References

- 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](http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6TOCE.html)
- International Safe Harbour Privacy Principles 2000*. <http://www.ita.doc.gov/td/ecom/shprin.html>
- Australian Privacy Foundation*. <http://www.privacy.org.au/>
- The Australian Privacy Charter*. <http://www.apcc.org.au/>
- NSW Privacy Committee*. <http://www.attgendept.nsw.gov.au/privacy.html>
- Victorian Data Protection Advisory Council*. <http://www.vicnet.net.au/~victorp/dataref.htm>

*Options for Promoting Privacy on the National Information Infrastructure - Draft for Public Comment from the National Information Infrastructure Task Force, USA. April 1997. <http://www.iitf.nist.gov/ipc/privacy.htm>.*

*The Canadian Standards Association Press Release, March 1997, on the new Canadian Privacy Model Standard. <http://www.csa.ca/031196-g.htm>.*